AGID
Agenzia per l'Italia Digitale

Gestione servizi e piattaforme condivise

REM SERVICES – Criteri di adozione standard ETSI – Policy IT

Versione 2.0

Sommario

1 Prefazione

1.1 Scopo del Documento

Il decreto legge n. 135 del 14 dicembre 2018 prevede che con DPCM, sentita l'AGID e il Garante per la protezione dei dati personali, siano adottate le misure necessarie a garantire la conformità dei servizi di posta elettronica certificata (**PEC**), di cui agli articoli 29 e 48 del decreto legislativo n. 82 del 7 marzo 2005, al regolamento (UE) n. 910 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

A far data dall'entrata in vigore del suindicato DPCM, l'articolo 48 del decreto legislativo n. 82 del 2005 è abrogato.

Scopo del presente documento è quello di definire l'insieme di requisiti tecnici previsti per un servizio elettronico di recapito certificato qualificato in conformità al **Regolamento eIDAS n.910/2014** (come successivamente modificato e integrato dal **Regolamento eIDAS 2.0 (UE) 2024/1183**), che definisce requisiti funzionali, che faranno da base per la definizione delle ***Regole Tecniche***, con il quale i gestori italiani si potranno presentare non solo sul mercato interno, ma anche nell'ambito territoriale di applicazione del **Regolamento eIDAS** beneficiando delle presunzioni legali ivi previste.

Particolare rilevanza, nella stesura dei requisiti tecnici, è stata data al tema dell'***interoperabilità***, fondamento sul quale è stato incentrato l'attuale modello PEC Italiano, che ha consentito il ***libero mercato*** delle soluzioni proposte dai Gestori PEC fino ad oggi.

A tale proposito, si evidenziano il recital (52) e i due nuovi paragrafi inseriti all'articolo 44 del suddetto **Regolamento eIDAS 2.0** - relativo ai servizi

elettronici di recapito certificato qualificato - che rappresentano l'esplicito riferimento al tema dell'***interoperabilità***:

(52) | […] Providers of qualified electronic registered delivery services ***should be encouraged*** *by Member States to make their services* ***interoperable with qualified electronic registered delivery services provided by other qualified trust service providers*** *in order to easily transfer electronic registered data between two or more qualified trust service providers and to promote fair practices in the internal market.*

Article 44

[…]

2a. Providers of qualified electronic registered delivery services may agree on the ***interoperability*** *between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1. The compliance shall be confirmed by a conformity assessment body.';*

(2b) The Commission may, by means of implementing acts, establish a ***list of reference standards*** *and, when necessary, establish* ***specifications and procedures*** *for the interoperability framework referred to in paragraph 2a. The technical specifications and content of standards shall be* ***cost-effective and proportionate****. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).'*

L'attenzione riservata dal GDL in merito all'***interoperabilità*** del sistema da realizzare è coerente con la Relazione della Commissione europea al Parlamento del 3.6.2021 che valutava come necessarie alcune modifiche al **Regolamento eIDAS 1.0**, e cioè cit. "…*in particolare la necessità di ridurre la frammentazione del mercato assicurando l'****interoperabilità transfrontaliera e transettoriale*** *dei* ***servizi fiduciari*** *attraverso l'****adozione di norme comuni****. L'ambito di applicazione attuale del regolamento eIDAS e la sua concentrazione sui regimi di identificazione elettronica notificati dagli Stati membri dell'UE e sull'accesso ai servizi pubblici online sembrano essere troppo limitati.*"

Si è cercato di limitare al solo capitolo 4 e all'ALLEGATO TECNICO la parte strettamente rivolta a chi deve implementare il servizio, dove si presuppone che il lettore abbia una conoscenza tecnica di dettaglio. Le rimanenti parti sono state scritte per una platea più ampia di lettori, interessati a comprendere i concetti base e i razionali delle scelte effettuate.

1.2 Acronimi e definizioni principali

I seguenti termini e definizioni rappresentano una copia di cortesia per il lettore ripresa dai documenti originali e a cui fare riferimento per l'interpretazione autentica.

CSI: Common Service Infrastructure / Common Service Interface

CAdES / CAdES-B-B: CAdES baseline signatures are built on CMS signatures by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases. B-B level provides requirements for the incorporation of signed and some unsigned attributes when the signature is actually generated.

DNS: Domain Name System

DSN: Delivery Status Notification

ERDS: Electronic Registered Delivery Services

ERD user agent/application (ERD-UA): system consisting of software and/or hardware ***components*** by which senders and recipients participate in the exchange of data with electronic registered delivery service providers.

NOTE: As defined in EN 319 401 **[11]**, Clause 3.1, the aforementioned ***information-handling components*** are also often referred to with the term "**information system**".

ENAP: ETSI European Standard (EN) - Approval Procedure (ENAP)

ETSI: European Telecommunications Standards Institute

HSM: Hardware security module

IdP: Identity Provider or **authorization server** (in **OAuth** terminology)

JWT JSON Web Token: as specified in **IETF RFC 7519** **[20]**

M2M: Machine-to-Machine

MTA: Message Transfer Agent

MX record: **M**ail e**X**changer record - resource configured in the **DNS** - responsible for binding the domain part of email address to the address of the competent email server.

non-ERDS/non-REM: Services that are not ERDS, e.g., physical mail, regular email, sector specific delivery system, etc. (*note that, in the present document, **non-ERDS** and **non-REM** are considered as synonyms and refers to the ordinary email or in any case systems external to REM*).

OAuth 2.0 Authorization Framework: As specified in **IETF RFC 6749** **[21]**

NOTE: Many Big Tech/IT providers implemented the so called SALS **XOAUTH2** mechanism that allows to access to their email messaging services (e.g. by means of standard commands like IMAP *AUTHENTICATE* and POP/SMTP *AUTH*) by using the OAuth 2.0 Access Tokens obtained by standards **OAuth** flows (see § 2.4.2.13 of the technical annex) .

Plugtests™: REM Remote Plugtests organized by ETSI Centre for Testing and Interoperability (CTI) - 31 May / 16 July 2021

Qualified Electronic Registered Delivery Service (QERDS): As specified in Regulation (EU) No 910/2014 [].

Qualified Electronic Registered Delivery Service Provider (QERDSP): trust service provider which provides qualified electronic registered delivery services.

Relay interface: Interface that supports ERD message relay between different electronic registered delivery services (*note that, in REM, the ERD message is a REM dispatch and the electronic registered delivery services are* **REMSP**).

REM: Registered Electronic Mail

REM baseline: Minimal set of requirements aiming to ensure maximal interoperability in the cross-REM interoperability domain and, specifically, in cross-border use of REM services. Compliance with REM baseline aims to simplify technical support of REM by

Member States competent authorities supporting qualified registered electronic delivery services.

REMID: REM Interoperability Domain

REMID authority: entity entitled to govern the REMID

NOTE: A REMID authority governs the REMID by the management of the REMID policy and through processes of supervision and monitoring, ensuring the adherence to the REMID policy and the requirements specified in the present document.

REMID policy: set of organizational, security and technical requirements that each adherent **REMSP** is obliged to fulfil to achieve interoperability

REMS: Registered Electronic Mail Service

REMSP: Registered Electronic Mail Service Provider

R-REMS: Recipient's REMS

S-REMS: Sender's REMS

S/MIME: Secure/Multipurpose Internet Mail Extensions (S/MIME). S/MIME provides a consistent way to send and receive secure MIME data by digital signature.

SAN: Subject Alternative Name (or SubjectAltName) X509v3 digital certificate extension.

NOTE: As clarified in EN 319 532-4 **[4]** (Clause D.2.2.1), the SAN extension is used in two different digital certificates inside REM baseline:
(1) the digital certificate used to sign both REM messages and ERDS evidence (see for instance § 2.4.2.11; **Table 4**/row **AP4** § 2.4.1; **Table 2**/row **PP6** § 2.3.1 of the technical annex); and
(2) the digital certificate used for **TLS** transport layer security (see § 2.4.2.15 and 2.4.2.8 and the relevant notes of the technical annex).

TC ESI: (ETSI) Technical Committee - Electronic Signatures and Infrastructures

TL: Trusted List

TLS: Transport Layer Security

time-stamp: Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time - according to the Time-Stamp Protocol defined in IETF RFC 3161 **[22]** and updated in IETF RFC 5816, and

associated to XAdES baseline digital signature according to ETSI EN 319 132-1 V1.2.1 standard.

XAdES / XAdES-B-T: XAdES baseline signatures build on XML digital signatures, by incorporation of signed and unsigned qualifying properties, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases. **B-T** level provides requirements for the generation and inclusion, for an existing signature, of a trusted token proving that the signature itself actually existed at a certain date and time (i.e., by the presence of `SignatureTimeStamp` element containing an electronic **time-stamp**).

Per maggiori dettagli sul significato di questi termini e sulla specifica terminologia utilizzata nel presente documento e nel relativo annesso tecnico si faccia riferimento ai documenti indicati al paragrafo § 4.1 ed in particolare alla Clause 3 dei documenti EN 319 532-1 **[1]**, EN 319 522-1 **[5]** e EN 319 532-4 **[4]**.

È inoltre definito il seguente termine:

REM-Policy-IT: Particular **REMID policy** defined, adopted and operating inside **IT** member state. In other words, the **REMID policy** represents what in Italian is known also with the term "***Regole Tecniche***".

NOTE: The present document provides the **building blocks** to use for the formal definition of the **REM-Policy-IT**.

1.3 Storia del Documento

Versione	Redatto	Revisionato	Note	Approvato	Data
1.0	Alessandra Antolini (AGID) Santino Foti (InfoCert) Marco Mangiulli (Aruba) Carlo Vona (Poste Italiane)	Andrea Caccia (Uninfo) Maria Antonietta Carletti (Sogei)	Prima stesura	GDL	28/05/2021
1.1	"	"	Dopo esecuzione **Plugtests**	GDL	29/07/2021
1.2	Alessandra Antolini (AGID) Santino Foti (InfoCert) Marco Mangiulli (Aruba) Carlo Vona (Poste Italiane) Roberto Reale (AGID)	Andrea Caccia (Uninfo) Maria Antonietta Carletti (Sogei) Roberto De Paolis (Telecom Italia Trust Technologies) Isidoro Orabona (Namirial)	Dopo pubblicazione EN 319 532-4 V1.2.1 **[4]**	GDL	28/07/2022
2.0	Alessandra Antolini (AGID) Santino Foti (InfoCert) Marco Mangiulli (Aruba) Carlo Vona (Poste Italiane) Roberto De Paolis (Telecom Italia Trust Technologies) Isidoro Orabona (Namirial) Elena Grechi (Telecom Italia Trust Technologies) Marina Amato (Telecom Italia Trust Technologies) Serena Giugni (Register) Francesco Barcellini (Intesi Group) Celestino Campopiano (Notartel)	GDL	Dopo pubblicazione EN 319 532-4 V1.3.1 **[4]**	GDL	14/05/2024

2 L'approccio seguito da AGID

Gli articoli 43 e 44 del **Regolamento eIDAS n.910/2014** definiscono gli effetti giuridici di un servizio elettronico di recapito certificato e i requisiti che devono essere soddisfatti per i **servizi elettronici di recapito certificato qualificato**.

L'**ETSI** (*European Telecommunications Standards Institute*) ha attivato nell'ottobre del 2016 all'interno del comitato tecnico *Electronic Signatures and Infrastructures committee* (**TC ESI**) lo sviluppo di una serie di standard con l'obiettivo di supportare la realizzazione di servizi conformi ai requisiti specificati negli articoli 43 e 44 del **Regolamento eIDAS**, in particolare relativi a:

- Electronic Registered Delivery Services (**ERDS**)
- Registered Electronic Mail (**REM**) Services.

AGID, al fine di realizzare un **servizio elettronico di recapito certificato qualificato** a norma del **Regolamento eIDAS n.910/2014**, ha quindi deciso di analizzare i documenti e di costituire un gruppo di lavoro tecnico (abbreviato in **GDL** da qui in poi), analogamente a quanto fatto allora per le vigenti regole tecniche PEC, con l'obiettivo di recepire gli standard ETSI e di trovare le soluzioni per implementare tutti i requisiti obbligatori degli standard (indicati col verbo modale ***shall***) e di decidere se e come implementare i requisiti opzionali (indicati coi verbi modali ***should*** – ***may***), al fine di assicurare l'interoperabilità del sistema. Si rimanda al paragrafo "Modal Verbs Terminology" presente in ogni standard ETSI per la corretta interpretazione di ognuno di questi verbi modali.

Al tavolo sono stati invitati tutti i Gestori di posta elettronica certificata, AssoCertificatori e UNINFO, con comunicazione AGID prot. 2019-12167 del **18 settembre 2019**.

Il GDL è stato coordinato su tutte le attività da Claudio Petrucci fino al 31 marzo 2022, responsabile per AGID del servizio *Gestione servizi Infrastrutturali*. Dal 1° aprile 2022, a seguito del collocamento a riposo, il GDL è stato coordinato, per i lavori finali, da Alessandra Antolini, responsabile per AGID del servizio *Gestione servizi e piattaforme condivise*.

Il GDL ha interagito in maniera costruttiva con **TC ESI** di **ETSI** evidenziando l'esigenza di approfondire alcuni aspetti dello standard relativi all'interoperabilità del sistema.

Le attività congiunte con il **TC ESI** di **ETSI**, realizzate in accordo con un significativo numero di stakeholders, sono arrivate nel maggio del 2022 alla pubblicazione dell'ultima versione degli standard ETSI, che definiscono in modo completo il set minimo di requisiti nel dialogo tra service provider necessari a garantire conformità al **Regolamento eIDAS** (cioè la **REM baseline**).

Di seguito si riportano le organizzazioni che hanno partecipato fattivamente alla realizzazione del presente documento:

Aruba, Actalis, Consiglio Nazionale del Notariato, Notartel, Infocert, Innovapuglia, Irideos, It.net, Namirial, Poste Italiane, Register.it, Sogei, Telecom Italia Trust Technologies, Uninfo, Assocertificatori.

3 Il metodo di analisi seguito dal GDL

3.1 Introduzione

Il GDL ha scelto di implementare il modello REM che si basa su protocolli di posta elettronica essendo la soluzione più prossima alla PEC.

La scelta tiene conto del livello di diffusione che ha raggiunto la PEC in Italia: alla data di stesura della presente versione di documento (Marzo 2024) i Gestori che erogano il servizio sono 16, il numero di caselle di PEC attive supera i 15 milioni, 2,5 miliardi sono i i messaggi PEC scambiati nel 2023 . Molte utenze PEC sono applicative e collegate a sistemi informativi (vedi il protocollo informatico) e l'ampia diffusione dei protocolli e formati standard usati oggi con la PEC (quali ad es. SMTP/IMAP ed **S/MIME**, che sono alla base anche della ETSI REM) ha rappresentato nella PEC una facilitazione e diffusione delle relative integrazioni applicative.

È da evidenziare che una delle chiavi di successo della PEC in Italia, che ha consentito di raggiungere tale diffusione, è stata la scelta da parte del legislatore di implementare un sistema distribuito basato su una pluralità di service provider sottoposti a vigilanza da parte di AGID, che ha garantito livelli di sicurezza e affidabilità, con coefficienti di scalabilità in grado di supportare i suddetti numeri: le architetture implementate dai Gestori, estremamente flessibili, sono in grado di supportare un traffico di messaggi anche più consistente. Il ruolo di AGID, garante della qualificazione, della vigilanza e dalla operatività dei Gestori, ha contribuito a rendere il modello una best practice nel panorama europeo, in grado di assicurare l'interoperabilità tra le varie piattaforme di PEC presenti sul mercato, requisito fondamentale per un servizio di così ampia diffusione.

Il GDL, nella scelta, ha tenuto in ampio conto gli utilizzatori: il minor numero di modifiche al nuovo sistema consentirà agli utenti di gestire il passaggio allo stesso con un minor impatto in termini di "sforzo di

adattamento" e di confidenzialità raggiunta con l'attuale servizio PEC che, come accennato prima, garantisce l'interoperabilità ed usabilità anche attraverso le applicazioni utente; inoltre, l'imponente utilizzo dell'e-mail nel mondo, realizzato grazie all'esistenza e al perfezionamento di prodotti specializzati, dà di per sé una ragguardevole garanzia di resilienza difficilmente realizzabile in tempi brevi con altre tecnologie che non siano naturalmente orientate al messaging: queste richiederebbero il disegno, la re-implementazione e il collaudo, su grandi numeri, di funzionalità quali il formatting/packaging, l'addressing, il routing, lo storing, etc., già ampiamente e nativamente gestiti da prodotti/sistemi specifici per l'e-mail, senza attraversare grandi travagli e forse disservizi nel breve/medio periodo. La scelta degli standard ETSI REM, grazie al grado di interoperabilità con i servizi di tipo ETSI ERDS, consentirà evoluzioni di piattaforme e servizi garantendo la continuità col preesistente.

3.2 Razionale e premessa

I partecipanti al GDL hanno convenuto che l'approccio opportuno (nel seguito **razionale**), nel caso specifico italiano, fosse quello di partire da una "GAP analysis" tra gli standard ETSI relativi alla REM e la PEC, con l'obiettivo di implementare una soluzione che, pur nel rispetto dei requisiti, avesse la distanza minima relativamente a:

- una consolidata "user experience" collegata con l'utilizzo dei protocolli di posta elettronica;
- un allineamento al modello di delivery (accettazione e consegna del messaggio) riconosciuto degli attuali servizi e piattaforme;
- le garanzie di interoperabilità attualmente garantita nel modello italiano;
- una piena conformità rispetto all'attuale quadro normativo vigente.

Altri *protocol/profile/binding* della famiglia ERDS non sono preclusi da evoluzioni future, una volta che gli standard definiranno una baseline con protocolli interoperabili ad ampio spettro (ad. es. anche con contenuti quali quelli prodotti nella REM).

Il risultato della gap analysis è riportato nel documento del 31 dicembre 2019 del GDL, raggiunto solo dopo tre mesi di lavoro del GDL e prodromico a questo documento.

Successivamente alla sopra enunciata analisi, e con l'esperienza acquisita sul tema nel corso del 2020, il GDL ha proseguito l'analisi sui temi Common Service Interface (**CSI**), Trusted List (**TL**) e **time-stamp**, elementi capisaldi per raggiungere l'interoperabilità tra service provider costituenti un sistema REM.

Dall'analisi sono scaturite delle osservazioni di dettaglio, relative all'interpretazione di alcuni punti degli standard, che il GDL ha deciso di proporre al **TC ESI** di **ETSI** per una condivisione.

Da tale collaborazione, che ha dato il via ad una analisi dettagliata del materiale preparato dal GDL, e dopo varie interazioni, il **TC ESI** di **ETSI** ha prodotto e pubblicato il 28 gennaio 2021 il draft V1.1.3 dell'EN 319 532-4 **[4]** (uno dei documenti costituenti il set dello standard della REM) che introduce la **REM baseline** pienamente allineata con i risultati del GDL in ambito Common Service Interface (**CSI**), Trusted List (**TL**) e **time-stamp**. Su tale base, nel corso del 2021 si è svolto un evento di ETSI **Plugtests** seguito dalla pubblicazione del draft V1.1.7, il 31 gennaio 2022, con gli aggiornamenti necessari a risolvere le criticità emerse durante i **Plugtests**, ed in versione finale **V1.3.1 il 9 Maggio 2022**, dopo l'approvazione **ENAP**.

I requisiti generali su come la **REM baseline** si rapporta con l'intero set di standard della REM (e di conseguenza con quelli del set ERDS che sono normativamente legati alla REM) sono dettagliatamente **definiti nella Clause C.1** della nuova versione dell'EN 319 532-4 **[4]**. In tale paragrafo è chiaramente indicato cosa **intende garantire** la **REM baseline**, cosa **è incluso** e

cosa **è escluso** da essa, ed **il principio da rispettare** per introdurre requisiti addizionali al di sopra di essa (ad es. nelle policy locali ad ogni stato membro)[1].

La **REM baseline** è pertanto utilizzata dal presente documento come **principale riferimento**, ed è connessa e rapportata alle varie scelte addizionali consentite dallo standard per un più agevole passaggio del servizio PEC ai **servizi elettronici di recapito certificato qualificato**.

Il presente documento recepisce la **REM baseline** mantenendo integralmente tutti i requisiti obbligatori rappresentati dal verbo modale ***shall*** (obbligo) e definendo la policy italiana (nel seguito indicata come **REM-Policy-IT**) specificando delle scelte nei casi in cui sono presenti margini di libertà - rappresentati dai verbi modali ***should*** (raccomandazione) e ***may*** (opzione) presenti nel set di documenti riportato al § 4.1 e riconducibili alla **REM baseline** - non impattanti sull'interoperabilità del sistema. Tali scelte hanno l'obiettivo di facilitare la transizione al nuovo servizio da parte degli utenti di piattaforme nazionali e servizi attualmente basati sulla PEC.

Alcuni temi presenti negli standard ETSI non sono stati trattati, in quanto **non inclusi** nelle capability della **REM baseline** (si veda quanto indicato sopra) o non contengono prescrizioni: nel seguito tali temi saranno indicati come ***Non applicabile***.

AGID, con la collaborazione degli specialisti di settore ha deciso di predisporre un ALLEGATO TECNICO, parte integrante di questo documento, che ha lo scopo di fornire elementi di chiarezza riguardo:

[1] A titolo esemplificativo ma non esaustivo, la **REM baseline** rappresenta il **mezzo per garantire l'interoperabilità** tra i vari REM service provider che vi aderiscono, come indicato nello standard EN 319 532-4 [4], Clause C.1. A meno che non sia altrimenti specificato nella REM baseline stessa, i requisiti che sono opzionali nell'intero set di standard non si applicano alla REM baseline; i requisiti obbligatori nel set di standard legato alla REM baseline sono obbligatori **anche** nella REM baseline. L'adozione di capabilities che non fanno parte della REM baseline e che sono previste ad es. nella REMID policy **non** devono introdurre comportamenti e funzionalità che vadano ad interrompere o compromettere l'interoperabilità.

- le soluzioni adottate relative ad alcuni argomenti prescrittivi della **REM baseline** che, allo stato della tecnologia corrente, implicano scelte implementative;
- l'implementazione delle scelte discrezionali, previste dalla **REM baseline**, effettuate nell'ambito della **REM-Policy-IT**;

L'ALLEGATO TECNICO, per quanto sopra, si prevede fin da ora che potrà essere aggiornato nel tempo per recepire, quando possibile, la dinamica intrinseca dei servizi digitali coinvolti.

4 Analisi documentazione ETSI

4.1 I documenti di riferimento

Per una maggiore fruibilità, in questo documento si usano i termini "standard" e "standardizzazione" al posto dei termini formalmente corretti di "norma" e "normazione" come da REGOLAMENTO (UE) N. 1025/2012 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 ottobre 2012 sulla normazione europea. ETSI è uno dei tre organismi di standardizzazione europei riconosciuti dal suddetto regolamento. Similarmente CEN e CENELEC, gli altri due organismi di standardizzazione europea, pubblicano EN, TS e TR, ma non sono oggetto del presente documento.

ETSI classifica i documenti prodotti in:

- **European Standard (EN)**: standard europeo redatto da un comitato tecnico e approvato dagli organismi di standardizzazione nazionali europei dell'ETSI e utilizzato quando il documento è destinato a soddisfare esigenze specifiche dell'Europa, in genere su richiesta della Commissione, e richiede la trasposizione in standard nazionali, che sono vincolati a non emettere standard sullo stesso tema (si veda la definizione di "norma europea" nel Regolamento (UE) 1025/2012);
- **Technical Specification (TS)**: contengono requisiti tecnici come gli standard europei e sono utilizzati quando è importante garantire una pubblicazione rapida. Un TS è approvato dalla commissione tecnica che lo ha redatto e non vincola gli enti nazionali (si veda la definizione di "prodotto della normazione europea" nel Regolamento (UE) 1025/2012);
- **Technical Report (TR)**: contengono materiale informativo o ulteriori approfondimenti rispetto a temi trattati in altri standard (anche questo rientra nella definizione di "prodotto della normazione europea" nel Regolamento (UE) 1025/2012).

L'analisi effettuata dal GDL ha considerato i seguenti documenti che definiscono il modello funzionale REM e le parti ad esso collegate (quali ad es. l'ERDS evidence o le capabilities, o ancora aspetti legati all'autenticazione o identificazione dell'utenza):

- **[1]** ETSI EN 319 532-1 V1.1.1 (2018 09) [REM - Part 1 Framework and architecture]
- **[2]** ETSI EN 319 532-2 V1.1.1 (2018 09) [REM - Part 2 Semantic contents]
- **[3]** ETSI EN 319 532-3 V1.3.1 (2024 01) [REM - Part 3 Formats]
- **[4]** ETSI EN 319 532-4 V1.3.1[2] (2024-01) [REM - Part 4 Interoperability profiles (including the new REM baseline)]
- **[4e]** ETSI EN 319 532-4 V1.3.1 (2024-01) [REM - Part 4 Interoperability profiles (ZIP with XSD and INFORMATIVE-WORKING-EXAMPLES)]
- **[5]** ETSI EN 319 522-1 V1.2.1 (2024 01) [ERDS - Part 1 Framework and architecture]
- **[6]** ETSI EN 319 522-2 V1.2.1 (2024 01) [ERDS - Part 2 Semantic contents]
- **[7]** ETSI EN 319 522-3 V1.2.1 (2024 01) [ERDS - Part 3 Formats]
- **[7e]** ETSI EN 319 522-3 V1.2.1 (2024 01) [ERDS - Part 3 Formats (ZIP with XSD)]
- **[8]** ETSI EN 319 521 V1.1.1 (2019 02) [Policy and security requirements for ERDSP]

[2] Alla data di stesura del presente documento lo standard EN 319 532-4 [4] con la definizione della **REM baseline** è stato pubblicato in forma definitiva (versione 1.2.1) e successivamente aggiornato (versione 1.3.1). Sul sito ETSI al seguente indirizzo è riportato l'iter che ha portato alla definizione ed approvazione dello standard V1.2.1 da parte degli stati membri dell'UE e dell'EFTA (procedura **ENAP**):
https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=59579
ed al seguente indirizzo è riportato l'iter che ha portato all'approvazione (procedura **ENAP**) della versione 1.3.1:
https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=66847

- **[9]** ETSI EN 319 531 V1.1.1 (2019 01) [Policy and security requirements for REMSP]
- **[10]** ETSI EN 319 411-1 V1.4.1 (2023 10) [Policy and security requirements for TSP]
- **[11]** ETSI EN 319 401 V3.1.0 (2024-03) [General Policy Requirements for Trust Service Providers]
- **[12]** ETSI EN 319 412-1 V1.5.1 (2023-09) [Certificate Profiles - Part 1 Overview and common data structures]

Come si evince dal prefisso "ETSI EN", questi sono tutti classificati come European Standard[3]. Nella valutazione degli standard della REM è stato necessario integrare l'analisi anche con gli omologhi (quando "normativamente connessi" a quelli REM) che fanno riferimento al modello funzionale ERDS. Quelli relativi alla REM sono riconoscibili perché sono identificati dal prefisso **ETSI EN 319 53****. Mentre quelli della famiglia ERDS sono identificati dal prefisso **ETSI EN 319 52****.

Gran parte delle **abbreviazioni ed acronimi** utilizzati nel presente documento e negli standard stessi sono definiti nella Clause 3 dei documenti EN 319 532-1 **[1]** e EN 319 522-1 **[5]**. Tuttavia, per renderli rapidamente fruibili, tramite cross-reference, quelli più utilizzati sono riportati anche nel § 1.2 del presente documento. Invece la mappa del set completo di standard "normativamente" connesso e costituente i concetti cardine per l'interoperabilità in accordo alla **REM baseline** è riportato in Table B.1 (CSI) e Table B.12 (digital signature & time-stamp) del documento EN 319 532-4 **[4]**.

Oltre ai suddetti EN standard sono referenziati all'interno del presente documento anche i seguenti standard e raccomandazioni internazionali:

[3] Vengono riportate, quando necessario, nei vari paragrafi, le **versioni** puntuali degli standard alle quali si sta facendo riferimento. Notare che eventuali revisioni degli stessi potrebbero rendere inconsistenti i riferimenti a numeri di pagina e di paragrafi, figure, tabelle, note e concetti in genere. Quindi seppur valido il principio generale che "si fa riferimento ad uno standard e alle sue possibili correzioni/evoluzioni", nell'evenienza di ciò, potrebbe essere richiesta almeno una revisione parallela del presente documento come verifica, ed il suo eventuale riallineamento.

- [13] NIST Special Publication 800-81-2 [Secure Domain Name System - (DNS) Deployment Guide]
- [14] FIPS PUB 180-4 [Secure Hash Standard (SHS)]
- [15] RFC 2049 [Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples]
- [16] RFC 5750 [Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling]
- [17] RFC 5322 [Internet Message Format]
- [18] RFC 6931 [Additional XML Security Uniform Resource Identifiers (URIs)]
- [19] RFC 8460 [SMTP TLS Reporting]
- [20] RFC 7519 [JSON Web Token (JWT)]
- [21] RFC 6749 [The OAuth 2.0 Authorization Framework]
- [22] RFC 3161 [Internet X.509 PKI - Time-Stamp Protocol (TSP)]
- [23] RFC 8705 [OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens]
- [24] RFC 9449 [OAuth 2.0 Demonstrating Proof of Possession (DPoP)]
- [25] RFC 7521 [Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants]
- [26] RFC 7523 [JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants]

4.2 Modalità di notazione dell'analisi

L'approccio seguito dal GDL è stato analitico, attraverso l'individuazione e valutazione puntuale dei margini di libertà, associati ai due verbi modali "***may***" e "***should***", presenti nel perimetro dei documenti identificati: in altre parole nel set di standard completo riportato al § 4.1, e quelli "normativamente" legati a questo set ma nel rispetto ed in coerenza con la cosiddetta **REM baseline**. Tali verbi modali sono utilizzati nel presente

documento con lo stesso significato prescrittivo presente nello standard (si rimanda al paragrafo "Modal Verbs Terminology" presente in ogni standard ETSI per la corretta interpretazione di ognuno di questi verbi). Per ogni documento è stata prodotta una scheda con le decisioni prese collegialmente dal GDL, ed i cui contenuti sono nel testo che accompagna la scheda stessa.

Le schede che nel loro complesso definiscono la **REM-Policy-IT** sono disposte in modo tabellare e sintetizzano gli ambiti di discrezionalità presenti negli standard.

CODICE	Ambito	Statement	Riferimento	REM-Policy-IT
A … N	**LISTA PARAGRAFI DEI DOCUMENTI ANALIZZATI**	TESTO COINVOLTO	***NUMERO PAGINA***	NOTE E COMMENTI DEL GRUPPO DI LAVORO (GDL)
		NUOVO TESTO RIFORMULATO PRENDENDO DECISIONI SUI VERBI MODALI may e should		PRESCRIZIONE

La prima colonna contiene una lettera che identifica il rigo della scheda ed è univoca per lo standard di riferimento.

La seconda colonna contiene la lista dei paragrafi significativi dello standard che conducono e guidano fino al testo che si sta esaminando. ATTENZIONE: per comprendere correttamente l'interpretazione data poi nella terza e quinta colonna è fondamentale leggere attentamente l'intero paragrafo (di cui un breve stralcio è mostrato nella terza colonna) direttamente dai documenti di riferimento sorgenti e contestualizzare così il testo coinvolto e le decisioni prese nella **REM-Policy-IT**.

La terza colonna è divisa in due sezioni: la prima, con sfondo grigio, riporta il testo coinvolto, contenente il verbo modale previsto dallo standard; la seconda sezione riporta lo stesso testo con il verbo modale previsto per la **REM-Policy-IT**.

La quarta colonna indica la pagina all'interno del documento di riferimento.

La quinta colonna riporta le note per i casi che prevedono più di una opzione. In alcuni casi è presente infatti una doppia scelta riguardante l'interoperabilità con policy diverse da quella italiana: si vedano i contenuti e le relative note [4] [5] a pag. 22 che spiegano più nel dettaglio questa dualità rappresentata dalla doppia scelta. Per una più agevole lettura è raccomandato avere a disposizione tutti i documenti ETSI precedentemente elencati.

Il caso in cui la seconda riga non sia presente sta ad indicare che la prescrizione prevista per la **REM-Policy-IT** è interamente definita dalla nota in quinta colonna, senza la necessità di riformulazione del testo originale in esame.

I differenti colori utilizzati per i verbi modali, blu e rosso, stanno ad indicare rispettivamente la posizione espressa nello standard e le scelte restrittive previste per la **REM-Policy-IT**, oltre ad eventuali commenti.

In taluni casi, sono formulate soluzioni tecniche per il recepimento degli standard, nonché proposte di soluzioni raccomandate ai service provider. Tali contributi sono descritti nell'ALLEGATO TECNICO.

La **REM-Policy-IT** prevede due distinti livelli di interoperabilità: un **primo livello**[4] specifico per i **servizi elettronici di recapito certificato qualificato** italiani (e cioè all'interno del **REMID policy**=**REM-Policy-IT**), ed un **secondo livello**[5] per l'interazione con **servizi elettronici di recapito certificato**

[4] Questo primo livello è costituito dalla **REM baseline** più un insieme di definizioni e best practice (costituenti l'insieme di requisiti connotati dalla REM Interoperability Domain policy – indicata come REMID policy da qui in avanti; si veda la Clause 3.1 e le Figure B.5 e B.6 dello standard EN 319 532-4 [4] per la definizione completa) specifiche per lo Stato italiano, e identificate come "**REM-Policy-IT**".

[5] All'interno della stessa policy REM-Policy-IT vi è un insieme di regole, sempre ben definito, ma più aperto rispetto alle prime, e rappresenta il secondo livello. Queste sono previste per l'interoperabilità, in una certa misura, con sistemi regolati da policy diverse da quella italiana (es. messaggi provenienti dall'estero). Ciò è evidenziato nelle tabelle con una doppia scelta: es.

qualificato appartenenti ad altre **REMID policy** (anche se comunque aderenti alla **REM baseline**).

Nel seguito saranno analizzati gli item delle schede, relative a ogni documento di standard del set riportato al § 4.1.

*Si noti che, in generale, per facilitarne la consultazione in formato digitale, il presente documento contiene, per quanto possibile, un consistente numero di riferimenti interni applicati a vari elementi quali sigle, acronimi, figure, tabelle, etc. che rimandano, (tramite "**clic**" in avanti e "**Alt ←**" per tornare indietro), direttamente al punto in cui l'elemento stesso è definito o approfondito.*

Ad esempio, laddove le specifiche della **REM baseline** forniscano delle prescrizioni pertinenti al punto trattato nella tabella, queste sono indicate con l'etichetta "**REM baseline**" seguita da un riferimento preciso verso il documento EN 319 532-4 **V1.3.1** [**4**] che consente di individuare il punto dove l'argomento in questione è trattato.

shall=REM-Policy-IT, **should=interoperabilità**. Alcuni temi (indicati come ***Non applicabile***) presenti negli standard ETSI non sono inseriti nel presente documento o perché non presenti nella **REM baseline** o perché non contengono prescrizioni.

4.3 Analisi dei requisiti

4.3.1 ETSI EN 319 532-1 V1.1.1 [REM - Part 1 Framework and architecture]

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
A	**4 REM logical model 4.2 Black-box model 4.2.1 Functional viewpoint**	the REMS ***may*** include the REMS **evidence**[6] **repository** and the REMS **user directory**	***[pag 12]***	
		the REMS may include the REMS evidence repository		**Non si prevede l'implementazione del REMS evidence repository**
		the REMS shall include ... the REMS user directory		**SI - USER DIRECTORY (DISTRIBUITO TRA I SERVICE PROVIDER) SI - IGPEC LIKE (DOMINIO/DNS)**

A. Evidence repository

In merito al punto in questione:

1. le ERDS evidence sono assimilabili alle ricevute della PEC che includono il DATICERT.xml
2. nell'attuale servizio PEC, tutte le evidenze sono in linea (cioè incluse nei messaggi PEC e/o nelle ricevute).

Viste le suddette considerazioni, seguendo il principio della distanza minima dalla PEC (in accordo al **razionale** in premessa e l'adesione alla **REM baseline**), la **REMID policy**=**REM-Policy-IT** non prevede l'implementazione di uno specifico Evidence Repository, in quanto:

- le ERDS evidence sono consultabili come parte dei messaggi e delle ricevute;
- il tracciamento delle operazioni svolte sui messaggi - nei

[6] Nel contesto REMS/ERDS il termine ERDS evidence è spesso utilizzato per indicare sia la "ricevuta" contenente l'xml, sia l'xml stesso. Si tenga pertanto sempre presente il contesto per individuare se ci si sta riferendo all'xml o a tutta la ricevuta (busta S/MIME nel formato prestabilito, nel caso REM).

> punti di accesso, ricezione e consegna - e la relativa conservazione a norma sono implementati con le stesse modalità previste per gli official log della PEC (si veda il § 2.4.2.4 dell'allegato tecnico).

Lo standard prevede il servizio opzionale "user directory" (indicato nello stesso come concetto astratto di alto livello), realizzato all'interno della **REM-Policy-IT** come insieme (non pubblico) dei repository che ogni service provider deve avere, ognuno contenente il dettaglio delle utenze di propria competenza. Si noti che non si tratta di un repository condiviso ma ogni service provider ha il proprio. In altre parole, non esiste una federazione di utenti condivisa tra service provider.

Per consentire la gestione sicura di tutti i domini del circuito (compito svolto, nella PEC, dall'IGPEC), è utilizzato un apposito schema.

Tale modello è definito più nel dettaglio nella **REM baseline** e fa pienamente uso del **DNS** come luogo naturale per la distribuzione ed il mantenimento dei domini (si veda la nota[11] a pag. 37).

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
B	**4 REM logical model 4.2 Black-box model 4.2.2 Sequence viewpoint 4.2.2.1 REM styles of operation**	A REMS ***may*** support S&N style of operation.	***[pag 12]***	***Non applicabile***[7] **REM baseline [4] Clause C.1** ***Vedi spiegazione sottostante e relativa nota***

B. Store and Notify

Lo Store and Notify **non è previsto** nella **REM baseline** come si evince dalla clausola C.1 dello standard EN 319 532-4, e dalla clausola 4.2.2.1 dello standard ETSI EN 319 531-1:

EN 319 532-4 - **REM baseline** cit.

"***C.1 General requirements***

*The present annex defines the so-called **REM baseline**, which **guarantees interoperability** between REMS providers. It also provides the basic features needed for a wide range of business and government use cases for electronic procedures and communications to apply to a wide range of communities when there is a clear **need for interoperability** of registered electronic delivery services. Unless otherwise specified in the present annex:*

[7] Funzionalità la cui efficacia, ad una prima analisi, sembra apprezzabile solo quando lo S&N opera esclusivamente in un ambito di competenza confinata al "singolo" service provider. Infatti, da standard, il colloquio in ambiente distribuito tra i service provider, anche nello schema S&N, deve avvenire sempre attraverso protocollo Store and Forward (**S&F** da qui in avanti). Inoltre, considerando che i service provider devono fornire servizi qualificati, lo S&N pone delle criticità in ambiente distribuito quali ad esempio il requisito dell'autenticazione di utenze che sono di pertinenza di altro service provider. Inoltre, lo S&N è definito in modo compiuto attraverso funzionalità opzionali proprie dei servizi REM ma non di quelle ERDS (infatti la specifica EN 319 522-X non contempla lo S&N se non come cenno: c.f. requisiti Table 1 del EN 319 522-2 **[6]**). Ciò rappresenterebbe un problema volendo aumentare, in futuro, il grado di interoperabilità tra i paradigmi REMS/ERDS. Come ultima osservazione lo S&N, da standard, prevede l'obbligatorietà del "pronunciamento" preventivo dell'utente di accettazione/rifiuto del messaggio prima di potervi accedere: caratteristica non compatibile con il **razionale** in premessa, con l'adesione alla **REM baseline** [4] e con il quadro normativo vigente.

• ***Mandatory requirements*** *in clause 5 (SMTP interoperability profile) of the present document and in the parts ETSI EN 319 532-1 [4], ETSI EN 319 532-2 [5], ETSI EN 319 532-3 [6]* ***shall also be mandatory in REM baseline****; and*

• ***Optional requirements*** *in clause 5 of the present document and in the parts ETSI EN 319 532-1 [4], ETSI EN 319 532-2 [5], ETSI EN 319 532-3 [6]* ***shall not apply on REM baseline*** *either.*

Adoption of capabilities that are not part of REM baseline shall not introduce requirements that break the interoperability*.*".

EN 319 532-1 - cit.

"***4.2.2.1 REM styles of operation***

[…]

A REMS shall support S&F style of operation. A REMS ***may support S&N*** *style of operation.*".

Lo Store and Notify (abbreviato in S&N da qui in poi) è opzionale (***may support S&N***), e quindi, nella parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4] SMTP Interoperability profile** + **REM baseline**) lo S&N **non è previsto**.

Pertanto, in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, il modello S&N **non è previsto** per la **REM-Policy-IT**.

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
C	**4 REM logical model** **4.2 Black-box model** **4.2.2 Sequence viewpoint** **4.2.2.2 REM Store and Forward style of operation**	**4.** The ERDS evidence of submission ***may*** optionally be sent back to the sender.	***[pag 13]***	
		The ERDS evidence of submission shall be sent back to the sender.		**SI - shall** **REM baseline [4]** **Clause C.4.5.1,** **Table C.22** **item g)** **item h) sub-item I**
		10. The REM service tracks the event that the user content has been handed over to the recipient. **In some cases this is done producing one or more attestation** (ERDS evidence of handover).	***[pag 14]***	***Non applicabile*** **REM baseline[4]** **Clause C.1**
		11. The ERDS evidence of handover **can** optionally be sent back to the sender.	***[pag 14]***	***Non applicabile*** **- vedi punto prec. 10.**

C. Evidence of submission (Codice A.1)

L'evidence of submission è assimilabile alla ricevuta di accettazione della PEC, ed è previsto dalla **REM baseline** che venga restituita al mittente. L'evidence di handover è opzionale e non è prevista nella **REM baseline**; e pertanto, coerentemente con il **razionale** in premessa e l'adesione alla **REM baseline** non è prevista per la **REM-Policy-IT**.

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
D	**4 REM logical model** **4.3 4-corner model** **4.3.1 Functional viewpoint**	The routing of REM messages ***may*** be based on the DNS records associated with the domain of the recipient address, just like in regular email messaging.	***[pag 18]***	
		*The routing of REM messages **shall** be based on the DNS records associated with the domain of the recipient address, just like in regular email messaging.*		**SI - shall** **REM baseline [4]** **Clause C.2.3.2** **Table C.1, item a.1)**

D. 4-corner Model – Functional viewpoint

Il modello 4-corner comporta la necessità di effettuare il delivery dei messaggi in uno scenario multi service provider.

Il message routing è indirizzato da una specifica parte della Common Service Interface, ed in particolare, secondo quanto previsto da EN 319 532-4 **[4]** (Clause C.2.3.2), il routing dei messaggi deve essere implementato tramite l'utilizzo del protocollo **DNS**.

Di conseguenza, mentre ogni REMSP mantiene il repository della propria utenza, per poter gestire correttamente il routing verso utenze di altri REMSP è utilizzato il protocollo **DNS**, opportunamente protetto tramite misure atte a mitigare i rischi di attacchi informatici (si veda il § 2.4.2.8 dell'allegato tecnico).

I dettagli del message routing, e più in generale del flusso di comunicazione tra due service provider, sono descritti da EN 319 532-4 **[4]** (Clause C.2.3 - Basic handshake).

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
E	**4 REM logical model** **4.3 4-corner model** **4.3.2 Sequence viewpoint** **4.3.2.1 REM S&F to S&F interaction**	*N1. Sender's REMS (S-REMS) needs to find out how to reach the recipient's REMS (R-REMS). In the general case this happens through a common infrastructure (Shared infrastructure). This is an abstract entity, which **can** correspond to several distinct actors. This step can involve multiple actions:* *- S-REMS needs to determine the recipient's REMS. This **can** be possible using the recipient's mailbox address, as an email address contains the provider domain.* *- S-REMS needs to find a mail route to the R-REMS. This **can** be possible using DNS lookups, as it is done in the case of regular email messages, or using other techniques. In the 4-corner model (clause 4.3) it is assumed that the REM message **can** be forwarded directly to R-REMS. In the extended model (clause 4.4) it is assumed that the REM message is forwarded through a number of intermediate REMSs.* *- S-REMS needs to check the capabilities of the REMSs along the mail route (e.g. supported style of operation, supported policies, etc.) in order to find a suitable route.* *- S-REMS needs to establish a trust relationship with the next-hop REMS along the mail route. This **can** be done, for instance, using Trusted Lists, as defined in ETSI TS 119 612.*	***[pag 19]***	***Non applicabile*** **Questa parte dello standard è ad alto livello, descrittiva ed esemplificativa. Il testo a fianco non contiene prescrizioni. I flussi di dettaglio sono definiti nello standard EN 319 532-4 [4]** **REM baseline [4] Clause C.4.5.1, C.4.5.2, C.4.5.3**
		*N2. The REMS performs a handshake with the next-hop REMS. This **can** include negotiation on different aspects (capabilities, supported style of operation, ERDS evidence, level of authentication of end entities, fees, etc.). Handshake can be omitted in closed systems where this information is defined a priori or available through a centralised infrastructure.*	***[pag 19-20]***	
		N8. The ERDS evidence of handover needs to be relayed back to the previous REMS along the mail route, in case the sender needs this attestation.	***[pag 20]***	

E. REM S&F to S&F interaction

Lo standard prevede lo **S&F** (vedi lettera B). Gli statement del punto E definiscono degli esempi di modalità operative riportate come non prescrittive che sono affrontate in dettaglio nell'ALLEGATO TECNICO, in accordo alla **REM baseline** (si vedano EN 319 532-4 **[4]**, Clause C.2.3, C.2.3.2, C.2.3.3, C.2.3.4, D.4.2, ed anche i § 2.3.2.4, 2.4.2.8, 2.4.2.15 dell'allegato tecnico).

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
F	**4 REM logical model** **4.4 Extended model** **4.4.1 Functional viewpoint**	In the general scenario, the delivery process ***may*** go through several chained REMSs.	***[pag 24]***	***Non applicabile*** **REM baseline [4]** **Clause C.2.3, C.4.5**

F. Extended model – Functional viewpoint

Coerentemente con gli obiettivi del **razionale** in premessa, l'adesione alla **REM baseline** e quanto riportato alla lettera D, la **REMID policy**=**REM-Policy-IT** non prevede il "multihop".

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
G	**6 REM events and evidence** **6.2 Events and evidence** **6.2.3 C. Events related to the acceptance/rejection by the recipient**	**Tutto il paragrafo**	***[pag 33]***	***Non applicabile*** **REM baseline [4]** **Clause C.1** **Si vedano anche le considerazioni del punto B a pag. 26 riguardo la Clause 4.2.2.1 della parte di standard in esame**

G. Events related to the acceptance/rejection by the recipient (S&N model)

Non sono previste per la **REM-Policy-IT** le prescrizioni legate ai suddetti eventi relativi allo S&N, coerentemente con gli obiettivi del **razionale** in premessa e l'adesione alla **REM baseline** (si veda punto **B.** sopra).

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
H	**6 REM events and evidence 6.2 Events and evidence 6.2.4 D. Events related to the consignment**	R-REMS ***may*** optionally notify the recipient about the consigned user content. This ***may*** be done using any channel they agreed upon, it need not use any of the standardised interfaces.	***[pag 33]***	**Prestazioni lasciate alla libera scelta del service provider** ***(notifica debole al destinatario[8] conosciuta anche come <<c'è posta per te>>)***
		R-REMS ***may*** also issue **ERDS evidence** about the successful or unsuccessful **notification** of the recipient about the consigned user content.	***[pag 33]***	***Non applicabile[9]*** **REM baseline [4] Clause C.1 [4], EN 319 531 [9], Clause 4.5 REQ-REMS-4.5-02** **Le ERDS evidence definite dalla REM baseline sono quelle obbligatorie dello standard. Lo S&N è un'opzione. Le ERDS evidence sulle notifiche proprie dello S&N non sono comprese.**

H. Events related to the consigment

Si evidenzia la presenza di una funzione similare, prescritta dai primi due ***may***, già attiva presso alcuni service provider (notifica debole al destinatario). È previsto che per la **REM-Policy-IT** si lasci libera scelta al service provider relativamente ad essa. Il terzo ***may*** permette all'R-REMS di generare ed inviare al mittente una ERDS evidence formale, circa la riuscita o meno dell'invio della suddetta notifica debole al destinatario. Considerata l'assenza di tale evidenza nell'attuale servizio PEC e per coerenza con il **razionale** in

[8] Es. una qualunque tipologia di notifica non tracciata dal sistema REM, come ad esempio SMS, email di posta elettronica ordinaria (detta anche PEO), push in app, o altro.

[9] Questa ERDS evidence **non è prevista** nella **REM baseline** [4]. Infatti essa è definita come D.3 (ConsignmentNotification) e D.4 (ConsignmentNotificationFailure) in Table 6 EN 319 532-1 **[2]**. Questa sarebbe generata dal R-REMS e, come indicato nella Table 1 EN 319 522-1 **[5]**, inviata al "Sender/Utente-Mittente" (o al "previous ERDS" nella catena di delivery rappresentato dal S-REMS) al verificarsi, rispettivamente, degli **eventi** D.3 e D.4 (eventi corrispondenti alle ERDS evidence D.3 e D.4 non previsti nella **REM baseline** [4]).

premessa e l'adesione alla **REM baseline**, questa non è inclusa nella **REMID policy**=**REM-Policy-IT**.

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
I	**6 REM events and evidence** **6.2 Events and evidence** **6.2.5 E. Events related to the handover to the recipient**	The REMS ***may*** issue ERDS evidence about the successful or unsuccessful handover.	***[pag 34]***	***Non applicabile*** **REM baseline[4] Clause C.1** **Le ERDS evidence definite dalla REM baseline sono quelle obbligatorie dello standard.**

I. Event related to the handover of the recipient

La **REMID policy**=**REM-Policy-IT**, in coerenza al **razionale** in premessa e l'adesione alla **REM baseline**, non supporta l'handover. Per cui questa componente non è prevista.

4.3.1	Ambito	Statement	Riferimento	REM-Policy-IT
J	6 REM events and evidence 6.2 Events and evidence 6.2.6 F. Events related to connections with non-ERDS systems	If the REMS supports this feature, it ***should*** issue ERDS evidence corresponding to the events described in this clause.	*[pag 34]*	
		F.1. RelayToNonERDS ***The REMS has successfully relayed the user content to the given non-ERDS system.***		**SI (applicabile nella REM-Policy-IT)** **Si veda il significato preciso dell'evidenza riportato a fianco e la spiegazione sottostante al punto J / F.1.**
		F.2. RelayToNonERDSFailure ***The REMS was unable to relay the user content to the non-ERDS system within a given time period.***		**SI (applicabile nella REM-Policy-IT)** **Si veda il significato preciso dell'evidenza riportato a fianco e la spiegazione sottostante al punto J / F.2**
		F.3. ReceivedFromNonERDS ***The REMS has received the user content from a non-ERDS system, therefore all information related to its sending, like the sender's identifier and the sending time, cannot be trusted per se***		**SI (applicabile nella REM-Policy-IT)** **Si veda il significato preciso dell'evidenza riportato a fianco e la spiegazione sottostante al punto J / F.3**

J. Event related to connections with **non-ERDS** systems

F.1: da REM verso non-REM: quando previsto dall'**S-REMS** provider e richiesto esplicitamente dall'utente che sia presente questa evidenza verso il mittente (opzionale e addizionale rispetto alla **REM baseline**) questa deve essere prodotta come previsto nel § 2.4.2.2 dell'allegato tecnico.

F.2: Come sopra

F.3: Da non-REM a REM – Si tratta del flusso che, attualmente, nella PEC è identificato dalla **busta di anomalia** (e nella REM è implementato attraverso un REM dispatch con allegata l'evidenza "ReceivedFromNonERDS.xml"). Pertanto, per coerenza con gli obiettivi del **razionale** in premessa e l'adesione alla **REM baseline** tale flusso è previsto per la **REM-Policy-IT**. Si vedano i dettagli al § 2.4.2.2 dell'allegato tecnico.

4.3.2 ETSI EN 319 532-2 V1.1.1 [REM - Part 2 Semantic contents]

4.3.2	Ambito	Statement	Riferimento	REM-Policy-IT
A	**4 Overview** **4.2 Typical flows of REM messages** **4.2.2 Use of data structures in Store and Forward style**	In S&F style: - objects relayed between REMSs - through the REM RI: Relay Interface - **shall** always be in the form of REM dispatch, REM payload or REMS receipt; - objects forwarded to the recipient - through the REM MRI: Message Retrieval Interface - ***should*** be in the form of REM dispatch or REM payload; - objects forwarded to the sender or recipient - through the REM ERI: Evidence Retrieval Interface - ***may*** be in the form of REMS receipt.	***[pag 11]***	
		objects forwarded to the recipient - through the REM MRI: Message Retrieval Interface - shall be in the form of REM dispatch.		**SI - shall REM dispatch** **REM payload non applicabile** **REM baseline [4] Clause C.1, C.4.5.1, Table C.22 item a)** **Il REM payload è un'opzione della REM che prevede l'ERDS evidence in forma "detached" rispetto al messaggio. Questa opzione NON è compresa nella REM baseline.**
		objects forwarded to the sender or recipient - through the REM ERI: Evidence Retrieval Interface - shall be in the form of REMS receipt.		**SI - shall** **REM baseline [4] Clause C.4.5.1, Table C.22 item a)**

A. ERDS and REM data structures.

La **REMID policy**=**REM-Policy-IT**, in coerenza al **razionale** in premessa e l'adesione alla **REM baseline**, non supporta il REM payload e richiede che le ERDS evidence siano in linea con le REMS receipt.

Si noti che lo standard REM non prevede una ricevuta di consegna simile a quella della PEC contenente l'*original message* allegato. Per avvicinare

l'usabilità del servizio REM a quello della PEC, e solo per i service provider appartenenti alla **REM-Policy-IT**, sono fornite nell'ALLEGATO TECNICO delle soluzioni risolutive senza impatti verso l'interoperabilità con altre **REMID policy**. Queste, sfruttando alcuni meccanismi previsti dallo standard, consentono di fornire con la REM la ricevuta di consegna con caratteristiche simili a quelle dell'attuale PEC (si veda il § 2.4.2.5 dell'allegato tecnico)[10].

[10] Si noti che la ricevuta di consegna riveste un significato molto importante in quanto chiude il ciclo di comunicazione "assicurata" (cioè "garantita" da punto a punto) da un mittente "registrato" (cioè "sottoscritto") presso un REMSP fino ad un destinatario "registrato" presso un secondo REMSP. Infatti, tale comunicazione si può definire pienamente compiuta (con la certezza di consegna del messaggio nella mailbox del destinatario) solo al completamento della transazione, comprovata con il ricevimento della **ContentConsignment** REMS receipt (si vedano § 2.2, la **Table 1** e la nota[30] a pag. 14 dell'allegato tecnico per ulteriori dettagli).

4.3.2	Ambito	Statement	Riferimento	REM-Policy-IT
B	**9 Common service interface content 9.3 REM trust establishment and governance**	*The requirements and explanations given in clause 9.3 of ETSI EN 319 522-2 **shall** apply to REM, with the following amendments.* *The REMS **should** use Trusted List (TL) to establish trust with other REMSs.* *NOTE: This TL **can** be e.g. the European Trusted List system established pursuant to the Regulation (EU) No 910/2014, or it **can** be a different TL set up specifically for a trust domain of REM services*	***[pag 15]***	
		The REMS shall use Trusted List (TL) to establish trust with other REMSs.		**SI - shall** **REM baseline [4] Clause C.2.3.3.1, Table C.2 item b.2.1.2)** **Nella parte di standard in esame si parla di TRUST e per esso si usa la Trusted List[11]!**
		NOTE: This TL can be e.g. the European Trusted List system established pursuant to the Regulation (EU) No 910/2014, or …		**SI** **REM baseline [4] Clause C.2.3.3.1, Table C.2 item b.2.1.2)** **Poiché il contesto è quello dei servizi QUALIFICATI a norma eIDAS, per tali servizi il TRUST è implementato attraverso l'EU Trusted List System.**

B. REM trust establishment and governance

È adottato un modello che fa riferimento alla EU Trusted List (**TL**) coerentemente con le prescrizioni della **REM baseline**.

[11] Questo punto è racchiuso in quella parte dello standard denominata Common Service Interface (CSI): si vedano le Clause C.2 e B.2 dello standard EN 319 532-4 **[4]**.

4.3.3 ETSI EN 319 522-2 V1.2.1 [ERDS (for REM) - Part 2 Semantic contents]

Nella REM sono richiamati i concetti di "identificazione" e "autenticazione" come indicato negli standard EN 319 521 **[8]**, Clause 4.1.1, 5.2.1, 5.2.2, 5.4.1, 5.4.2 ed EN 319 531 **[9]**, Clause 5.2.1, 5.2.2 e, nell'ALLEGATO TECNICO, rispetto ad alcuni aspetti specifici implementativi (si veda ad es. il § 2.4.2.12 per i concetti generali ed il § 2.4.2.7 in merito all'autenticazione SMTP da client di mercato).

4.3.3	Ambito	Statement	Riferimento	REM-Policy-IT
A1	**5 Identification of actors** **5.4 Identity verification and authentication assurance levels** **information**	This clause defines the information which is necessary to establish the level of assurance for the entities which take part in the electronic delivery process. This information **shall** include: 1) An attribute containing details of the registration and identity proofing and verification assurance level. This attribute: a) **shall** contain one identifier of the assurance level itself. This identifier **shall** have a URI as value; b) ***may*** also contain an identifier of the identification policy. This identifier **shall** have a URI as value; c) ***may*** also contain details on the identification policy; d) ***may*** also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.	***[pag 11]***	
		b) may also contain an identifier of the identification policy. This identifier shall have a URI as value; ***c) may also contain details on the identification policy;*** ***d) may also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.***		**Prestazioni lasciate alla libera scelta del service provider per quanto non altrimenti riportato nella REM baseline [4] Clause C.3.4, Table C.18 ed in particolare gli item g), h), i)**
A2	**5 Identification of actors** **5.4 Identity verification and authentication assurance levels** **information**	2) An attribute containing details of the authentication means and mechanisms assurance level. This attribute: a) **shall** contain one identifier of the assurance level itself. This identifier **shall** have a URI as value; b) ***may*** also contain an identifier of the authentication policy. This identifier **shall** have a URI as value; c) ***may*** also contain details on the authentication policy; d) ***may*** also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.	***[pag 11]***	
		b) may also contain an identifier of the authentication policy. This identifier shall have a URI as value; ***c) may also contain details on the authentication policy;*** ***d) may also contain one or more URIs pointing to resources that contain details of the aforementioned policy provided in different languages.***		**Prestazioni lasciate alla libera scelta del service provider per quanto non altrimenti riportato nella REM baseline [4] Clause C.3.4, Table C.18 ed in particolare gli item g), h), i)**
A3	**5 Identification of actors** **5.4 Identity verification and authentication assurance levels** **information**	Furthermore, the identity assurance information ***may*** include an attribute containing details of the performed authentication, either an assertion generated by an assertion provider or as a sequence of components, consisting of: - the date and time when the authentication process was conducted; - the identification of the authentication method used.	***[pag 11]***	**Prestazioni lasciate alla libera scelta del service provider per quanto non altrimenti riportato nella REM baseline [4] Clause C.3.4, Table C.18 ed in particolare gli item g), h), i)**

A1-A2-A3. Identity verification assurance levels information

Per gli item b) c) d) (***may***), poiché questi ultimi non introducono elementi concreti di garanzia o valore aggiunto, i service provider avranno la facoltà di implementare i ***may*** in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** (nel rispetto delle condizioni riportate nella nota[18] a pag. 55; si veda anche il § 2.9.2 dell'allegato tecnico riguardo gli aspetti relativi alla resilienza).

4.3.3	Ambito	Statement	Riferimento	REM-Policy-IT
B	**7 Digital signatures in ERDS provisioning 7.2 Common requirements for digital signatures**	*For all digital signatures applied by ERDSs to ERD **messages** and ERDS **evidence**:* *1) The digital signature **should** be a CAdES, XAdES or PAdES baseline signature as specified in ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1.* *...* *2) The digital signature **shall** use cryptographic algorithms of sufficient strength, e.g. as recommended by ETSI TS 119 312.* *3) The digital signature **may** include a signed property containing the explicit identifier of the signature policy governing the signing and/or validating processes.* *4) A signature time-stamp **should** be added to the digital signature of evidence; when a CAdES or XAdES signature is used, the B-T signature level **should** be used.*	***[pag 16]***	
		For all digital signatures applied by ERDSs to ERD messages: ***1) The digital signature shall be a CAdES as specified in ETSI EN 319 122-1***		**SI - shall** **REM baseline [4]** **Clause C.4.2 Table C.19 item a)**
		For all digital signatures applied by ERDSs to ERDS evidence: ***1) The digital signature shall be a XAdES as specified in ETSI EN 319 132-1***		**SI - shall** **REM baseline [4]** **Clause C.4.3 Table C.20 item c)**
		3) The digital signature may include a signed property containing the explicit identifier of the signature policy governing the signing and/or validating processes.		**Si conferma il testo originario per quanto non altrimenti riportato nella** **REM baseline [4]** **Clause C.1, Clause C.4.2 Table C.19 item b) per il CAdES** **Clause C.4.3 Table C.20 item d) per lo XAdES**
		4) A signature time-stamp shall be added to the digital signature of evidence; with XAdES signature, the B-T signature level shall be used.		**SI - shall** **REM baseline [4]** **Clause C.4.4 Table C.21 item e) e solo per lo XAdES** **Essendo sufficiente un solo time-stamp per evento, la REM baseline prevede il time-stamp solo nella ERDS evidence (e quindi solo nello XAdES).**

B. Common requirement for digital signatures.

La firma digitale **S/MIME** sull'oggetto costituente il REM message, e sulle ERDS evidence, essendo apposta da un soggetto giuridico è richiesto sia un *sigillo elettronico avanzato* (*advanced electronic seal* come da **Regolamento eIDAS n.910/2014**, Articolo 44 punto 1/(d)). Anche se è necessario che il sigillo sia apposto da un trust service provider qualificato (**Regolamento eIDAS n.910/2014**, Articolo 44 punto 1/(d)) non è strettamente necessario che il

certificato con cui si appongono le firme digitali sia qualificato (**Regolamento eIDAS n.910/2014**, Articolo 3 punto (26)). Inoltre, in accordo a EN 319 521 **[8]**, Clause 7.5 REQ-ERDSP-7.5-03 è necessario che la chiave privata associata al suddetto certificato digitale sia *mantenuta* ed *usata* all'interno di un *secure cryptographic device*. Infine, è necessario che i *secure cryptographic device* (detti anche **HSM**) dispongano di una certificazione common criteria idonea o almeno **FIPS PUB 140-2 level 3** in accordo allo standard ETSI EN 319 411-1 **[10]**, Clause 6.5.2 OVR-6.5.2-01 item b).

I punti cardine nella suddetta tabella indicano dove è applicato il **time-stamp** (e cioè, con lo scopo evidente di favorire l'interoperabilità, direttamente all'XML della ERDS evidence), così come prescritto nella **REM baseline**. Il **time-stamp** - applicato tramite **XAdES-B-T** alle ERDS evidence - è richiesto che sia una *validazione temporale elettronica qualificata* (*qualified electronic time stamp* come da **Regolamento eIDAS n.910/2014**, Articolo 44 punto 1/(f)) e che sia firmato da un *sigillo elettronico avanzato* (*advanced electronic seal* come da **Regolamento eIDAS n.910/2014**, Articolo 42 punto 1/(c)).

In merito al punto 3) nelle scelte ***may*** della suddetta tabella - riguardo la "signature policy" dove è previsto che questo attributo possa essere specificato nella **REMID policy** - si vedano i § 2.3.2.2, 2.3.2.3 e la riga **PP5** della **Table 2** dell'allegato tecnico. Si rimanda, invece, all'apposita Clause C.4 della **REM baseline** contenuta nel documento EN 319 532-4 **V1.3.1** [**4**] che specifica più nel dettaglio le varie scelte relative alle firme digitali (o sigilli) da applicare ai REM message, alle ERDS evidence e al **time-stamp**.

4.3.3	Ambito	Statement	Riferimento	REM-Policy-IT
C	**8.3 Evidence components values 8.3.1 Free text**	*Information in free text **shall** be written in UK English. Text in other languages **may** be added*	***[pag 23]***	
		Information in free text shall be written in UK English. Text in other languages shall/may be added[12]		**shall=REM-Policy-IT** ***may*=interoperabilità**

C. Evidence components values

La presenza del testo in lingua italiana è resa obbligatoria con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT**. Si lascia invece il ***may*** per i messaggi provenienti da altre **REMID policy** per agevolare l'interoperabilità.

[12] Si consideri che ci si sta riferendo ad informazioni che possono essere disposte in ogni "ERDS evidence component" dove risulti permesso l'uso di testo libero. Si vedano gli standard EN 319 522-2 **[6],** Clause 8.3.1 ed EN 319 532-3 **[3]**, Clause 6.2.3.4.

4.3.4 ETSI EN 319 532-3 V1.3.1 [REM - Part 3 Formats]

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
A	**4.2 Internet Message Format in the REM services Tab 1**	This is composed of header + body as defined in IETF RFC 5321 [], clause 2.3.1. It is generated by the sender's ERD user agent or under the sender's technical/legal responsibility (and outside the responsibility of the service), which ***may*** be eventually digitally signed by the sender (note 1). See Figure 1, Figure 4 and also definitions in ETSI EN 319 532-2 [], clause 4.	***[pag 10]***	**Si conferma il testo originario**

A. Internet Message Format in the REM services Tab 1

L'*original message* può opzionalmente essere firmato digitalmente dal mittente. Questa firma è esterna ed ininfluente a livello del servizio REM.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
B	**4.2 Internet Message Format in the REM services Tab 1**	See Figure 3 for the structure of this object and definitions in ETSI EN 319 532-1 [], clause 3.1. The difference from ERDS serviceInfo is that a REMS notification always contains a reference to the user content. Furthermore, it ***may*** optionally carry the relevant evidence.	***[pag 10]***	**Non Applicabile** **REM baseline [4]** **Clause C.1** **La REMID policy=REM-Policy-IT basata sulla REM baseline non supporta lo S&N**

B. Internet Message Format in the REM services Tab 1

Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** la **REMID policy=REM-Policy-IT** non supporta lo S&N.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
C	**4.2 Internet Message Format in the REM services**	As the REM message contents are separated from the transport information/closure information parts in the communication stream, the entire set of REM messages as specified in the present document ***may*** also be properly transported by other underlying transport protocols. NOTE 1: This separation ensures that REM messages are completely unrelated to the underlying protocol stream.	***[pag 11]***	**Non applicabile** **REM baseline [4]** **Clause C.1** **Si veda spiegazione sottostante**

C. Internet Message Format in the REM services

Si noti che la presente scelta, definita come ***may*** nello standard, è rilevante solo se si volessero supportare altri *transport protocols*.

La parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4] SMTP Interoperability profile** & **REM baseline**) è attualmente basata esclusivamente sul protocollo **SMTP**. Infatti, l'adesione alla versione corrente della **REM baseline** non permette di supportare altri protocolli diversi da SMTP.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
D	**4.2 Internet Message Format in the REM services**	The REM Service could add/modify some header fields to the submission metadata during the enveloping process. Anyway, these changes ***should*** be limited to what is proven as essential for the good working of the process and ***should*** be fully defined in the specific REM implementation.	***[pag 11]***	**Si conferma il testo originario** **La REMID policy=REM-Policy-IT basata sulla REM baseline richiede l'impostazione di un Message-ID**

D. Internet Message Format in the REM services

L'uso di ***should*** nello standard, permette di poter effettuare alcune modifiche all'"*original message*"[13] (ad es. la reimpostazione del `Message-ID`, come avviene nella PEC)[14]. Bisogna tuttavia limitare i cambiamenti degli header a quanto effettivamente necessario.

[13] Si vedano la sezione 6.2.4.3, la Fig. 1 e la Fig. A.1 dello standard EN 319 532-3 [3] per individuare la conformazione e la disposizione dell'original message all'interno dell'intera struttura S/MIME. La modifica del Message-ID (per assegnargli un valore secondo il formato specificato e da usare poi come correlatore in tutti i REM message collegati) consiste nella modifica di un header dei "submission metadata".

[14] La modifica del Message-ID è un requisito sistematico e necessario al buon funzionamento "di servizio" REM (come identificativo di correlazione). Per ottemperare a quanto riportato nel regolamento europeo Art. 44 comma e), circa il cambiamento dei dati dell'utente (original message), **tale modifica può essere** <<*chiaramente indicata al mittente e al destinatario dei dati stessi*>> ad esempio **riportandola** nel **manuale operativo** (ad es. come riferimento alla **REM-Policy-IT**) o nel **contratto** ovvero nel **testo della busta** S/MIME del REM dispatch.

Inoltre, la specifica implementazione (cioè il set di requisiti definiti a livello di **REM-Policy-IT**) deve indicare nel dettaglio i cambiamenti che si effettueranno agli header. Si vedano anche tutte le altre parti del presente documento che riportano dei requisiti rispetto al `Message-ID`, i requisiti al § 2.4.2.3 e gli esempi al § 2.7 dell'allegato tecnico per i dettagli realizzativi.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
E	**4.3 REM message - Structure Definition**	A REM message ***may*** flow between different REMSs, and from a REMS to ERD user agents, as defined in ETSI EN 319 532-1 []. It is out of scope of the present document to define how the generic REM message is tailored to the specific mode of operation and interface it flows through.	***[pag 11]***	**Non applicabile** **REM baseline [4] Clause C.1**

E. REM message - Structure Definition

Il suddetto ***may*** (nella prima parte della frase) non può essere applicabile in toto a livello di policy **REMID policy**=**REM-Policy-IT**. Infatti, la parte generale dello standard EN 319 532-1 **[2]** è logicamente aperta rispetto agli style of operations (**S&F** e **S&N**), altri *transport protocols* e/o altre eventuali interfacce di trasferimento. La parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4] SMTP Interoperability profile** & **REM baseline**), come indicato nello scope dello standard stesso, è invece basata esclusivamente sull'**SMTP**. Pertanto, il ***may*** risulta non applicabile coerentemente con il **razionale** in premessa, e in quanto l'adesione alla **REM baseline** e alla **REMID policy**=**REM-Policy-IT** non prevede di supportare altri protocolli diversi da SMTP né altri style of operation diversi da **S&F**. La seconda parte della frase conferma questa scelta indicando proprio che queste caratteristiche sono out of scope nel documento in esame, EN 319 532-3 **[3]**.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
F	**4.3 REM message - Structure Definition**	0..N indicates an optional part that ***may*** occur any number of times;	***[pag 12]***	**Si conferma il testo originario**

F. REM message - Structure Definition

Il suddetto ***may*** è solo una didascalia di spiegazione sulla cardinalità delle varie occorrenze all'interno del template del messaggio.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
G	**4.3 REM message - Structure Definition Fig. 1 - REM dispatch**	A message created by the REMS, to be displayed automatically upon display of the REM message. **Text *may*** contain information for the user (see clause 6.2.3.4)	***[pag 13]***	**shall=REM-Policy-IT *may*=interoperabilità *Nota: esclusivamente con riferimento alle informazioni relative al sender.*** **Inoltre, la REMID policy=REM-Policy-IT richiede l'utilizzo dei testi almeno in lingua italiana ed inglese**
		*A message created by the REMS, to be displayed automatically upon display of the REM message. **Text shall/may** contain information for the user (see clause 6.2.3.4)*		

G. REM message - Structure Definition Fig. 1 - REM dispatch

Indica che il testo di accompagnamento al REM dispatch può contenere del testo TXT libero di spiegazione che, invece, per tutti i messaggi emessi nella **REMID policy=REM-Policy-IT** deve essere presente. Al fine di fornire un collegamento tra il nome della casella mittente (*o sender*) e il soggetto identificato (***titolare*** *o intestatario*) cui appartiene la casella, per tutti i messaggi (*REM dispatch*) emessi nell'ambito della **REM-Policy-IT** si richiede di inserire, nel testo introduttivo del messaggio (*REMS introduction*), gli attributi identificativi del **titolare** *nome*, *cognome* (o *denominazione* azienda/ente in caso di persona giuridica) e *codice fiscale* (questo ultimo raccomandato). Nell'allegato tecnico è fornita una struttura di base da dare a questo testo nell'ambito della **REM-Policy-IT** (si vedano il § 2.4.2.6 e gli esempi al § 2.7). Come descritto negli esempi del § 2.2 dell'allegato tecnico, il suddetto requisito è supportato dalla modalità di identificazione dell'**utenza**, registrata (o sottoscritta) al servizio secondo le norme vigenti, e dall'aderenza allo standard EN 319 521 **[8]**, Clause 5.2.1.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
H	**4.3 REM message - Structure Definition** ***Fig. 1 - REM dispatch***	A message created by the REMS, to be displayed automatically upon display of the REM message. **HTML *may*** contain URIs and other information for the user (see clause 6.2.3.4)	***[pag 13]***	**shall=REM-Policy-IT** ***may*=interoperabilità** ***Nota: esclusivamente con riferimento alle informazioni relative al sender.*** **Inoltre, la REMID policy=REM-Policy-IT richiede l'utilizzo dei testi almeno in lingua italiana ed inglese**
		A message created by the REMS, to be displayed automatically upon display of the REM message. **HTML *shall/may*** contain URIs and other information for the user (see clause 6.2.3.4)		

H. REM message - Structure Definition Fig. 1 - REM dispatch.

Indica che il testo di accompagnamento al REM dispatch può contenere del testo HTML libero di spiegazione. Il presente documento propone un minimo di struttura da dare a questo testo a favore dell'uniformità dei messaggi emessi all'interno della **REM-Policy-IT** (si vedano il § 2.4.2.6 e gli esempi al § 2.7 dell'allegato tecnico). Il contenuto informativo per l'utente di queste due parti *plain text/HTML* deve essere identico. Valgono pertanto tutte le considerazioni fatte al punto **G.** sopra (e con particolare riguardo ai messaggi emessi nella **REMID policy=REM-Policy-IT**, alla presenza degli attributi identificativi del **titolare** e ai dettagli forniti nell'allegato tecnico al § 2.4.2.6). Infatti, questa parte HTML del MIME e la precedente TXT sono due formati dello stesso contenuto (due parti "alternative" del MIME) che un client può usare ed interpretare[15] a seconda di alcune configurazioni e/o preferenze, ma senza alterazioni di contenuto. Eventuali URI contenenti informazioni generiche per l'utente non sono un problema ma devono ovviamente essere allineati su entrambe le parti HTML & TXT. Invece, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, URI relativi a contenuti secondo il modello S&N non sono supportate dalla presente policy **REM-Policy-IT**.

[15] Si veda la Clause 6.2.3.1 del EN 319 532-3 [3] e la relativa NOTA. Si noti che questo requisito di univocità delle due parti alternative plain text & HTML non è complesso da realizzare: sono parti del messaggio emessi dal software REM dei service provider e quindi sotto il loro controllo.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
I	**4.3 REM message - Structure Definition** ***Fig. 2 - REMS receipt***	A message created by the REMS, to be displayed automatically upon display of the REM message. Text ***may*** contain information for the user (see clause 6.2.3.4)	***[pag 13]***	Si conferma il testo originario

I. REM message - Structure Definition Fig. 2 - REMS receipt

Anche il testo di accompagnamento alla **REMS receipt** può contenere del testo TXT libero di spiegazione. Valgono anche per la REMS receipt tutte le considerazioni fatte nei primi due punti precedenti G e H relative al REM dispatch.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
J	**4.3 REM message - Structure Definition** ***Fig. 2 - REMS receipt***	A message created by the REMS, to be displayed automatically upon display of the REM message. HTML ***may*** contain URIs and other information for the user (see clause 6.2.3.4)	***[pag 13]***	Si conferma il testo originario

J. REM message - Structure Definition Fig. 2 - REMS receipt

Anche il testo di accompagnamento alla **REMS receipt** può contenere del testo HTML libero di spiegazione. Valgono anche per la REMS receipt tutte le considerazioni fatte nei primi due punti precedenti G e H relative al REM dispatch. Si rimarca che URI relativi al modello S&N non sono supportate, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
K	**4.3 REM message - Structure Definition** ***Fig. 3 - REM notification***	A message created by the REMS, to be displayed automatically upon display of the REM message. Text ***may*** contain URIs (pointer to a repository from where the original message ***may*** be retrieved) and other information for the user (see clause 6.2.3.4)	***[pag 15]***	Non applicabile REM baseline [4] Clause C.1 La REMID policy=REM-Policy-IT basata sulla REM baseline non supporta lo S&N

K. REM message - Structure Definition Fig. 3 - REM notification

Scelta rilevante solo quando si supporta lo S&N. Per coerenza con il **razionale** in premessa, i suddetti ***may*** risultano non applicabili in quanto l'adesione alla **REM baseline** non prevede di supportare lo S&N.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
L	**4.3 REM message - Structure Definition** ***Fig. 3 - REM notification***	A message created by the REMS, to be displayed automatically upon display of the REM message. HTML ***may*** contain URIs and other information for the user (see clause 6.2.3.4)	***[pag 15]***	**Non applicabile** **REM baseline [4]** **Clause C.1** **La REMID policy=REM-Policy-IT basata sulla REM baseline non supporta lo S&N**

L. REM message - Structure Definition Fig. 3 - REM notification

Per coerenza con il **razionale** in premessa, il ***may*** risulta non applicabile in quanto l'adesione alla **REM baseline** non prevede di supportare lo S&N.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
M	**4.3 REM message - Structure Definition** ***Fig. 4 - REM payload***	A message created by the REMS, to be displayed automatically upon display of the REM message. Text ***may*** contain information for the user (see clause 6.2.3.4)	***[pag 16]***	**Non applicabile** **REM baseline [4]** **Clause C.1** **Il REM payload è un'opzione della REM che prevede l'ERDS evidence in forma "detached" rispetto al messaggio. Questa opzione NON è compresa nella REM baseline.**

M. REM message - Structure Definition Fig. 4 - REM payload

Per coerenza con il **razionale** in premessa, il ***may*** risulta non applicabile in quanto l'adesione alla **REM baseline** non prevede di supportare il REM payload.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
N	**4.3 REM message - Structure Definition** ***Fig. 4 - REM payload***	A message created by the REMS, to be displayed automatically upon display of the REM message. HTML ***may*** contain URIs and other information for the user (see clause 6.2.3.4)	***[pag 16]***	**Non applicabile** **REM baseline [4]** **Clause C.1** **Come il punto precedente.**

N. REM message - Structure Definition Fig. 4 - REM payload

Per coerenza con il **razionale** in premessa, il ***may*** risulta non applicabile in quanto l'adesione alla **REM baseline** non prevede di supportare il REM payload.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
O	**6.1 General requirements**	The presence requirements are defined in Table 5 of ETSI EN 319 522-2 [] and clause 6.2.1 of ETSI EN 319 532-2 []. Header fields not listed in Table 2 ***may*** be absent in REM.	***[pag 17]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

O. General requirements

I requisiti di presenza sono definiti in ERDS in EN 319 522-2 **[6]**, Table 5 e nella **REM baseline** EN 319 532-4 **[4]**, Clause C.4.5.4, Table C.26. Si vedano anche i § 2.3.2.1, **Table 3** e 2.4.2.1, **Table 5** per la relativa trattazione nella **REMID policy**=**REM-Policy-IT**.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
P	**6.1 General requirements Table 2**	**User content** information: **Digest algorithm** REM-DigestAlgorithm: header field. This value shall be as defined in ETSI EN 319 522-2 [], clause 6.2.14 - MD14 and ETSI EN 319 522-3 [], clause 4.3.13. In REM it ***should*** be mapped as a URI compliant with section 4.2 of IETF RFC 6931 [].	***[pag 18]***	
		*- MD14 and ETSI EN 319 522-3 [], clause 4.3.13. In REM it **should** be mapped as a URI compliant with section 4.2 of IETF RFC 6931 [].*		**conditional should** **REM baseline [4] Clause C.4.5.1, C.4.5.2, C.4.5.3 item c) sub-item IV. I suddetti valori si riflettono anche dai contenuti della ERDS evidence. Clause C.3.4 Table C.18 item l).** **I limiti entro i quali definire l'algoritmo scelto tra quelli previsti dallo standard sono riportati nella REM baseline che demanda alla policy nazionale. Si veda la spiegazione sottostante.**

P. General requirements Table 2

Si noti che il *component* in esame è identificato nello standard come **MD14** che, a parte il formato stabilito dalle regole di binding, ha una semantica identica al *component* **M02** (si faccia riferimento agli standard EN 319 522-3 **[7]**, EN 319 532-3 **[3]** e alla **REM baseline** EN 319 532-4 **[4]**, Clause

C.4.5.1, Table C.22 item c) sub-item IV. che spiega come debba essere interpretato, nel contesto e nel binding REM, il *component* in esame).

Come previsto dallo standard e come rimarcato nella suddetta tabella, all'interno della **REMID policy=REM-Policy-IT** è specificato l'algoritmo da usare in emissione (che sarà http://www.w3.org/2001/04/xmldsig-more#sha256) e una lista di algoritmi ammessi e tollerati nella verifica e validazione di *component* emessi da altre entità (ad esempio per comunicazioni provenienti da altre **REMID policy**). Questi algoritmi sono rappresentati sotto forma di URI e ripresi dall'RFC 6931 **[18]**, in accordo allo standard EN 319 532-3 **[3]** e alla seguente disposizione della **REM baseline** EN 319 532-4 **[4]** (c.f. Clause C.4.5.1, Table C.22 item c) sub-item IV.):

"DigestMethod child field of element of UserContentInfo shall be set to an algorithm, amongst those identified in the security policy as per the current best practice, in the form of a URI according to the element REM-DigestAlgorithm defined in ETSI EN 319 532-3 [], Table 2 (see also clause D.1.3)"

(si faccia riferimento alla riga **PP1** della **Table 2** dell'allegato tecnico).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
Q	**6.1 General requirements Table 2**	**User content** information: **Message digest** REM-DigestValue: header field. This value shall be as defined in ETSI EN 319 522-2 [], clause 6.2.14 – MD14 and ETSI EN 319 522-3 [], clause 4.3.13. In REM it ***should*** contain the base64 encoded digest value of original message as computed using the digest algorithm indicated in the aforementioned header field.	***[pag 18]***	**SI – shall** **REM baseline [4]** **Clause C.4.5.1, C.4.5.2, C.4.5.3 item c) sub-item V.**
		In REM it ***shall*** contain the base64 encoded digest value of original message as computed using the digest algorithm indicated in the aforementioned header field.		**I suddetti valori si riflettono anche dai contenuti della ERDS evidence. Clause C.3.4 Table C.18 item l).** **Il *component* in esame, userContentInfo, è rappresentato dai *component code* MD14 e M02. La REM baseline conferma shall.**

Q. General requirements Table 2

Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, all'interno della **REMID policy**=**REM-Policy-IT** la codifica da utilizzare è **base64**. È reso pertanto obbligatorio il suddetto requisito con uno ***shall***.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
R	**6.1 General requirements Table 2**	**User content** information: **Message original identifier** REM-UAMessageIdentifier: header field[16]. This value shall be as defined in ETSI EN 319 522-2 [], clause 6.2.11 – MD11 and ETSI EN 319 522-3 [], clause 4.3.4. In REM it ***should*** contain the Message-ID value of the original message submitted by the ERD-UA.	***[pag 18]***	**shall=REM-Policy-IT** ***should*=interoperabilità**
		In REM it ***shall*** contain the Message-ID value of the original message submitted by the ERD-UA.		**REM baseline [4] Clause C.3.4 Table C.18 item l).** **I suddetti valori si riflettono anche dai contenuti della ERDS evidence (*AppLayerIdentifier*).**

R. General requirements Table 2

L'eventuale `Message-ID` specificato dal client utente nell'*original message* deve essere "salvato" nell'header `REM-UAMessageIdentifier` di ogni REM message. È reso pertanto obbligatorio il suddetto requisito con uno ***shall*** all'interno della **REMID policy**=**REM-Policy-IT**. Si lascia invece lo ***should*** per quanto riguarda i messaggi provenienti da altre **REMID policy**, per agevolare l'interoperabilità. Si vedano anche tutte le altre parti del presente documento che riportano dei requisiti rispetto al `Message-ID` ed i requisiti al § 2.4.2.3 ed esempi al § 2.7 dell'allegato tecnico per i dettagli realizzativi.

[16] Nel caso di header collocati all'esterno della zona firmata e protetta dall'S/MIME, questi danno la possibilità di un accesso immediato ad alcune informazioni senza forzarne il reperimento all'interno dell'ERDS evidence, ma hanno uno scopo puramente di "pre-verifica" o "scrematura" rispetto al contenuto informativo che rappresentano. Il valore di riferimento, quando necessario come elemento certificato, va reperito obbligatoriamente anche all'interno della ERDS evidence (si veda 2.9.2 dell'allegato tecnico).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
S	**6.1 General requirements Table 2**	**User content** information: **AttachmentInformation** This value shall be formatted as defined in ETSI EN 319 522-2 [], clause 6.2.14. In REM it is related to attachment information natively contained in the MIME header fields (see note 1 in Table 1). This ***may*** be further explicitly mapped in REM according to extension mechanisms defined in clause 6.2.1 or clause 6.2.5 for structured information.	***[pag 18]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.** **I suddetti valori si riflettono anche dai contenuti della ERDS evidence. Clause C.3.4 Table C.18 item l).** **L'inserimento di capability che non fanno parte della REM baseline, ma previste ad es. nella REMID policy non devono introdurre comportamenti e funzionalità che vadano ad interrompere o compromettere l'interoperabilità**

S. General requirements Table 2

Questa scelta riguarda informazioni opzionali sugli eventuali allegati (***AttachmentInformation***) dell'*original message*.

Se queste informazioni, per via della loro struttura, non potessero essere inglobate in un header, allora possono essere inserite in un apposito allegato attraverso il meccanismo delle MIME extension (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza e si veda anche il punto successivo che vale in generale e non solo riguardo gli eventuali allegati).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
T	**6.1 General requirements Table 2**	**Extensions** Other metadata ***may*** be specified with the extension mechanism defined in clause 6.2.1 or clause 6.2.5 for structured information. This value shall be formatted as defined in ETSI EN 319 522-2 [], clause 6.2.15 – MD15 and ETSI EN 319 522-3 [], clause 4.3.17.	***[pag 18]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

T. General requirements Table 2 – Extensions

Questo requisito riguarda generici metadati dell'*original message* (non espressamente definiti nella **Table 2**) qualora fosse necessario mapparli nel REM message. In tal caso, le estensioni opzionali in formato ERDS si possono specificare come estensioni in REM secondo i meccanismi indicati (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel

rispetto delle condizioni riportate nella nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
U	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Content-Type**: The value for this header field shall be "multipart/signed". • 'protocol' parameter value shall be "application/pkcs7-signature". • 'micalg' parameter value ***should*** be conformant to ETSI TS 119 312 []. • 'boundary' parameter value ***should*** be conformant to IETF RFC 2046 [], section 5.1.1.	***[pag 19]***	Si conferma il testo originario

U. REMS relay metadata MIME Header Fields Table 3 – Content-Type

La presenza del content-type e dei suoi parametri è già obbligatoria nella tabella 3 del EN 319 532-3 **[3]**. Lo ***should*** si riferisce ai parametri specificati. Come indicato nella suddetta tabella si lasciano inalterati gli obblighi all'interno della **REMID policy**=**REM-Policy-IT** (nel rispetto delle condizioni riportate nelle note[17] [18]). Si rimanda alle apposite prescrizioni al § 2.3.2.2 e la riga **PP6** della **Table 2** dell'allegato tecnico, che specificano più nel dettaglio le varie scelte relative al sigillo da applicare ai REM message. In particolare, il parametro *micalg* può essere ulteriormente selezionato, e appartenere ad un set ristretto di valori previsto nelle best practice di sicurezza correnti.

[17] Il REM message prodotto dai vari service provider deve avere una firma digitale (o **"sigillo") CAdES compliant** in accordo alla **REM baseline**, come prescritto nello standard EN 319 532-4 [4], Clause C.4.2 Table C.19 item a) (si veda anche punto "B. Common requirement for digital signatures." del § 4.3.3, pag. 32 del presente documento).

[18] Il REM message **prodotto** dai vari service provider deve consentire la **corretta interpretazione da parte di ampio set client utenti e/o librerie**, anche attraverso una rimodulazione delle scelte secondo le "best practice" correnti. In taluni casi, per agevolare l'interoperabilità e quando possibile, si può essere più tolleranti, rispetto ai messaggi in **entrata** aderenti ad altre policy e per quanto non altrimenti riportato nella REM baseline, nello standard EN 319 532-4 [4], Clause C.1. Infatti, la presenza di capability che non fanno parte della REM baseline, ma previste ad es. nella REMID policy locale, non deve introdurre comportamenti e funzionalità che vadano ad interrompere o compromettere l'interoperabilità cross-border.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
	6.2.1 REMS relay metadata MIME Header Fields Table 3:	**Message-ID**: The value for this header field ***should*** be an UID as defined in IETF RFC 5322 [].	***[pag 19]***	
V		The value for this header field ***shall*** be an UID…		**shall=REM-Policy-IT** **REM baseline [4] Clause C.3.4 Table C.18 item k).** **I suddetti valori si riflettono anche dai contenuti della ERDS evidence.**

V. REMS relay metadata MIME Header Fields Table 3 – Message-ID

Così come nella PEC, anche nella REM è necessaria una gestione particolare del codice identificativo (`Message-ID`) del messaggio di trasporto e dei messaggi correlati generati (ricevute, errori, ecc.). Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, anche all'interno della **REMID policy**=**REM-Policy-IT** si deve implementare un meccanismo analogo. È reso pertanto obbligatorio il suddetto requisito con uno ***shall***. Si vedano anche tutte le altre parti del presente documento che riportano dei requisiti rispetto al `Message-ID` (nella fattispecie il § 4.3.4 al punto D di pag. 45 e note [13] e [14]) ed i requisiti al § 2.4.2.2 ed esempi al § 2.7 dell'allegato tecnico per i dettagli realizzativi.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
W	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**From**: The value for this header field ***should*** be either a REMSP service address (e.g. "<service_rem_md_x@rem_md_x.com>" or a transformation of the original From field to show the role of the REMSP (e.g. "on behalf of user@rem_md_x.com <service_rem_md_x@rem_md_x.com>").	***[pag 19]***	
		From: The value for this header field ***shall*** be a transformation of the original From field to show the role of the REMSP (i.e. "on behalf of user@rem_md_x.com <sevice_rem_md_x@rem_md_x.com>").		**Shall=REM-Policy-IT** ***should*=interoperabilità**

W. REMS relay metadata MIME Header Fields Table 3 - From

Così come nella PEC, anche nella REM vi è una trasformazione del "`FROM`". Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**,

anche all'interno della **REMID policy**=**REM-Policy-IT** si deve implementare un meccanismo analogo. È reso pertanto obbligatorio il suddetto requisito con uno ***shall***. Si lascia invece lo ***should*** per quanto riguarda i messaggi provenienti da altre **REMID policy**, per agevolare l'interoperabilità (si veda l'identificativo **AP4** della **Table 4** al § 2.4.1 dell'allegato tecnico).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
X	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**To**: In case of a **REM dispatch** or REM payload the value for this header field **shall** match the value of the 'To' header field in the original message. **In case of a REM message carrying evidence for the sender**, the value for this header field ***may*** match the value of the 'From' header field in the original message.	*[pag 19]*	
		… the value for this header field ***shall*** match the value of the 'From' header field in the original message.		**SI – shall** **REM baseline [4]** **Clause C.4.5.1** **Table C.22 item g) & h).** **Clause C.4.5.2** **Table C.24 item g) & h).** **Clause C.4.5.3** **Table C.25 item g) & h).** **Dalle suddette prescrizioni si rileva che solo il REM dispatch è ammesso, e nei casi di SubmissionAcceptance, SubmissionRejection, RelayFailure, ContentConsignment e ContentConsignment failure è implicitamente disposto che la relativa REMS receipt sia inviata indietro al mittente (quindi il *To:* della ricevuta deve essere identico al *From*: dell'*original message***

X. REMS relay metadata MIME Header Fields Table 3: To

Così come nella PEC, anche nella REM ogni ricevuta ha il campo: *To: [mittente originale]*. Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, anche all'interno della **REMID policy**=**REM-Policy-IT** la suddetta scelta (rappresentata dal ***may***) è resa obbligatoria con uno ***shall***, come chiaramente derivabile dai punti della **REM baseline** messi in evidenza nella suddetta tabella.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
Y	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Cc**: REMS ***should*** assign a value to this header field only for REM dispatch. In such case, the value shall match the value of the 'Cc' header field in the original message.	***[pag 19]***	
		Cc: REMS ***shall*** assign a value to this header field only for REM dispatch. In such case, the value shall match the value of the 'Cc' header field in the original message.		**Shall=REM-Policy-IT** ***should*=interoperabilità** **Lo should si riferisce al fatto che il Cc: è previsto solo per il Dispatch e non per le ricevute.**

Y. REMS relay metadata MIME Header Fields Table 3: Cc

Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, all'interno della **REMID policy=REM-Policy-IT** la suddetta scelta è resa obbligatoria con uno ***shall***. Si lascia invece lo ***should*** per quanto riguarda eventuali ricevute provenienti da altre **REMID policy**, che abbiano il `Cc`, per agevolare l'interoperabilità (si veda l'identificativo **AP5** della **Table 4** al § 2.4.1 dell'allegato tecnico).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
Z	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Subject**: The value for this header field ***should*** be transformed as follows starting from the Subject header field contained in the original sender's message, in order to indicate the role that the REM message has within the flow: REM <event identifier>: <original subject> (E.g.: "REM ContentConsignment: subject_of_original_message").	***[pag 19]***	**Non essendo la trasformazione del Subject "normalizzata" nella REM baseline, si propone il consueto schema dove lato REMID policy=REM-Policy-IT ci sono delle scelte da rispettare all'interno della policy. Poiché il Subject: è esterno alla sezione firmata dell'S/MIME è necessario essere resilienti a formati differenti provenienti da altre REMID policy (si veda il § 2.9.2 dell'allegato tecnico).** **I formati previsti per la REM-Policy-IT sono i seguenti:** * REM dispatch relativo ad un messaggio qualificato: **REM Dispatch**: <oggetto originale> * REM dispatch relativo ad un messaggio esterno alla REM baseline: **REM EXTERNAL**: <oggetto originale> * REMS receipt relativa all'accettazione/non-accettazione: **REM SubmissionAcceptance**: <oggetto originale> **REM SubmissionRejection**: <oggetto originale> * REMS receipt relativa alla consegna/non-consegna: **REM ContentConsignment**: <oggetto originale> **REM ContentConsignmentFailure**: <oggetto originale> * REMS receipt relativa alla presa in carico/non-presa-in-carico: **REM RelayAcceptance**: <oggetto originale> **REM RelayRejection**: <oggetto originale> **REM RelayFailure**: <oggetto originale>
		Subject: The value for this header field ***shall*** be transformed as follows starting from the Subject header field contained in the original sender's message, in order …		**shall=REM policy-IT** ***should*=interoperabilità**

Z. REMS relay metadata MIME Header Fields Table 3: Subject

Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, all'interno della **REMID policy=REM-Policy-IT** la suddetta scelta è resa obbligatoria con uno ***shall***. Si lascia invece lo ***should*** per quanto riguarda eventuali ricevute e messaggi provenienti da altre **REMID policy**. Si veda la **Table 14** nel § 2.4.2.10 dell'allegato tecnico. Al fine di facilitare l'interoperabilità si deve essere in grado di ricevere qualsiasi altra forma di subject (si veda l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
AA	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Reply-To**: In the case of a REM dispatch or REM payload the value for this header field **shall** match the value of the 'From' header field in the original message. **In the case of a REM message carrying evidence for the sender**, this header field ***should*** not appear, and if it appears, its value ***should*** be the REM service address.	***[pag 19]***	
		Reply-To: In the case of a REM dispatch or REM payload the value for this header field **shall** match the value of the 'From' header field in the original message**. In the case of a REM message carrying evidence for the sender**, this header field ***should*** not appear, and if it appears, its value ***shall*** be the REM service address.		***Caso REM dispatch*:** **SI – shall** **ReplyTo(dispatch) = From (origMsg)** ***Caso REM payload*:** **non applicabile** ***Caso REM receipt*:** **[not recommended ReplyTo presence]** **Ma se presente:** **ReplyTo=REMS email address** **shall=REM-Policy-IT** ***should*=interoperabilità** **Lo shall per la REM-Policy-IT si riferisce solo alle ricevute (REM messages che trasportano evidenze per il mittente). In tal caso, anche se non raccomandato, se il replyTo viene valorizzato questo deve combaciare con l'email della casella del servizio REMS).**

AA. REMS relay meta-data MIME Header Fields Table 3: Reply-To

All'interno della **REMID policy**=**REM-Policy-IT**, la suddetta scelta è resa obbligatoria con uno ***shall***. Si lascia invece lo ***should*** (cui lo ***shall*** si riferisce, e che vale solo quando l'header è presente) per quanto riguarda le ricevute provenienti da altre **REMID policy**, per agevolare l'interoperabilità. Questo header risulta conditional perché ci sono i vari casi relativi alle tipologie di messaggio, ed è condizionato in base ad essi. Lo ***shall*** si riferisce al solo ultimo ***should***. Si veda la nota all'elemento I-MD09 nelle **Table 3** e **Table 5** dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
BB	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Return-Path**: REMS ***may*** assign a value to this header field only for REM dispatch. In such case, the value ***should*** match the value of the 'Return-Path' header field in the original message.	***[pag 19]***	
		Return-Path: REMS ***may*** assign a value to this header field only for REM dispatch. In such case, the value ***shall*** match the value of the 'Return-Path' header field in the original message.		**shall=REM-Policy-IT** ***should*=interoperabilità** **Il REMS, in riferimento al presente header, quando il client specifica tale valore, nell'ambito della REM-Policy-IT ripropone lo stesso valore anche a livello di busta REM dispatch (questa obbligatorietà è completata al punto seguente)**

BB. REMS relay metadata MIME Header Fields Table 3: Return-Path

Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, all'interno della **REMID policy=REM-Policy-IT** la suddetta scelta (relativa alla corrispondenza rispetto al valore del suddetto header del REM dispatch e dell'*original message*) è resa obbligatoria con uno ***shall***. Si lascia invece lo ***should*** (cui lo shall si riferisce, che vale solo quando l'header è presente nell'*original message*) per quanto riguarda i REM dispatch provenienti da altre **REMID policy**, per agevolare l'interoperabilità. Si veda anche quanto specificato all'identificativo **AP1** della **Table 4** al § 2.4.1 dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
CC	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Return-Path**: REMS ***may*** assign a value to this header field only for REM dispatch. In such case, the value ***should*** match the value of the 'Return-Path' header field in the original message.	***[pag 19]***	
		Return-Path: REMS ***conditionally shall*** assign…		***conditionally shall*=REM-Policy-IT** ***may*=interoperabilità** **Nei REM dispatch emessi nell'ambito della REM-Policy-IT il *Return-Path:* è sempre presente. Quando il client lo specifica nell'*original message* il *Return-Path:* è replicato nel REM dispatch. Quando il client non lo specifica, allora nel REM dispatch verrà inserito un *Return-Path:* con il valore del *From:* dell'*original message*. Questa disposizione completa quella del punto precedente.**

CC. REMS relay metadata MIME Header Fields Table 3: Return-Path

Così come nella PEC il messaggio di trasporto eredita l'header:
`Return-Path:` [come nell'*original message*]

per coerenza con il **razionale** in premessa, anche all'interno della **REMID policy=REM-Policy-IT** si deve implementare un meccanismo analogo. È reso pertanto obbligatorio il suddetto requisito con uno ***shall*** condizionato alla presenza di tale header nell'*original message*. Si lascia invece il ***may*** per quanto riguarda i REM dispatch provenienti da altre **REMID policy**, per agevolare l'interoperabilità. Si veda anche quanto specificato all'identificativo **AP1** della **Table 4** al § 2.4.1 dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
DD	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**Received**: REMS ***may*** assign a value to this header field only for REM dispatch. In such case, the value shall match the value of the 'Received' header field in the original message.	***[pag 19]***	
		Received: REMS ***conditionally shall*** assign…		***conditionally shall*=REM-Policy-IT** ***may*=interoperabilità** **Il REMS, quando (e solo quando) il client specifica tale header, nella REM-Policy-IT ripropone lo stesso header a livello di busta REM dispatch.**

DD. REMS relay metadata MIME Header Fields Table 3: Received

Così come nella PEC il messaggio di trasporto eredita l'header:
`Received:` [come nell'*original message*]

per coerenza con il **razionale** in premessa, anche all'interno della **REMID policy=REM-Policy-IT** si deve implementare un meccanismo analogo. È reso pertanto obbligatorio il suddetto requisito con uno ***shall*** condizionato alla presenza di tale header nell'*original message*. Si lascia invece ***may*** per quanto riguarda i REM dispatch provenienti da altre **REMID policy**, per agevolare l'interoperabilità. Si veda l'identificativo **AP2** della **Table 4** al § 2.4.1 dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
EE	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**In-Reply-To**: REMS ***may*** assign a value to this header field. The value should match the value of the 'In-Reply-To' header field in the original message.	***[pag 19]***	**Si conferma il testo originario**

EE. REMS relay metadata MIME Header Fields Table 3: In-Reply-To

Si lascia alla libertà del service provider la gestione del presente header (ereditando nel REM message il valore dell'*original message*) in modo che, assieme all'header `references`, si possa gestire una vista dei messaggi orientata ai "thread". Si veda la nota implementativa relativa all'elemento I-MD12 nella **Table 3** dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
FF	**6.2.1 REMS relay metadata MIME Header Fields Table 3:**	**In-Reply-To**: REMS ***may*** assign a value to this header field. The value ***should*** match the value of the 'In-Reply-To' header field in the original message.	***[pag 19]***	**Si conferma il testo originario**

FF. REMS relay metadata MIME Header Fields Table 3: In-Reply-To

Al presente punto si applicano le stesse considerazioni e condizioni del precedente (si vedano i commenti al punto EE) Si veda la nota implementativa relativa all'elemento I-MD12 nella **Table 3** dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
GG	**6.2.1 REMS relay metadata MIME Header Fields**	Furthermore, the header section of each REM message ***may*** contain other basic extension header fields. The purpose of these header fields is to give immediate access to important identification information instead of forcing the REMS to process the ERDS evidence.	***[pag 20]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

GG. REMS relay metadata MIME Header Fields

Questa scelta indica che, oltre agli header riportati come obbligatori, altri **header opzionali** possono essere inseriti. Si lascia alla libertà del service provider questa possibilità (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni

riportate nella nota[16] a pag. 53 e nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
HH	**6.2.1 REMS relay metadata MIME Header Fields**	The same naming mechanism ***should*** be used also for other implementation-specific or custom header fields. The following example shows the usage of the aforementioned mechanism to add two header fields: EXAMPLE: • REM-G02: <Evidence version value> • REM-R01: <Evidence issuer policy identifier> In case the character set of the <value> to assign to any aforementioned header fields is not compliant with the supported email standards, a base64 encoding ***should*** be used for a consistent representation in a unique header field body.	*[pag 20]*	**Viene prescritta la codifica base64, ove richiesto, per eventuali header addizionali nei REM messages emessi all'interno della REM-Policy-IT.**
		The same naming mechanism ***should*** be used also for other implementation-specific or custom header fields. The following example shows the usage of the aforementioned mechanism to add two header fields: EXAMPLE: • REM-G02: <Evidence version value> • REM-R01: <Evidence issuer policy identifier> In case the character set of the <value> to assign to any aforementioned header fields is not compliant with the supported email standards, a base64 encoding ***shall*** be used for a consistent representation in a unique header field body.		**Il primo *should* viene lasciato com'è per quanto non altrimenti riportato nella REM baseline [4] Clause C.1** **Il secondo ristretto a shall=REM-Policy-IT *should*=interoperabilità**

HH. REMS relay metadata MIME Header Fields

Il presente requisito descrive il meccanismo che si dovrebbe utilizzare per aggiungere degli header partendo dai TAG semantici definiti nello standard del EN 319 522-2 **[6]**. Lo ***should*** relativo all'uso del base64 come formato per dati non serializzati/serializzabili (si veda anche punto successivo II e nota[19] di pag. 65) è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT**. Si lascia invece lo ***should*** per quanto riguarda i messaggi provenienti da altre **REMID policy**, per agevolare l'interoperabilità (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
II	**6.2.1 REMS relay metadata MIME Header Fields**	In case of structured information, not easily convertible to a simple header body, the REMS structured extension defined in clause 6.2.5 ***may*** be used to host the full structure in a specific file as attachment.	***[pag 21]***	**Si conferma il testo originario[19] per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

II. REMS relay metadata MIME Header Fields

In continuità con il requisito precedente (HH) relativamente ad es. a metadati "custom" o "opzionali", il presente metodo indica come eventualmente ri-mappare dei dati complessi, legati alle semantiche dell'ERDS, come MIME extension, in appositi allegati aggiuntivi del REM message. Come indicato nella suddetta tabella si lasciano inalterati gli obblighi all'interno della **REMID policy=REM-Policy-IT**. Ciò, ovviamente, quando non è possibile usare gli header del requisito precedente HH (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
JJ	**6.2.2 signed data MIME Header Fields Table 4**	Content-Type: The value for this header field shall be: "multipart/mixed" • 'boundary' parameter value ***should*** be conformant to IETF RFC 2046 [], section 5.1.1.	***[pag 21]***	**Si conferma il testo originario**

JJ. signed data MIME Header Fields Table 4: Content-Type

La presenza del content-type e dei suoi parametri è già obbligatoria nella tabella 4 del EN 319 532-3 **[3]**. Lo ***should*** si riferisce al parametro specificato,

[19] Infatti, gli header MIME sono del tipo "Chiave: valore" in un'unica riga. Questa sintassi non è agevole per ospitare dati con una struttura complessa (ad es. disposta su più righe, come può essere un XML). Sono previsti quindi questi due metodi utili nelle definizioni di **interoperability profile**: (**HH**) "encoding/embedding" in un'unica riga con codifica base64 (possibile quando la struttura del dato codificato è nota/definita a priori) o (**II**) "new attachment" che in modo flessibile permette di inglobare nel REM message direttamente il contenuto come "allegato addizionale" (che incorpora in modo auto-consistente la struttura desiderata, per via ad es. del MIME-TYPE o dell'estensione del file). Questi ultimi vengono visti come "estensioni MIME" rispetto allo schema proposto.

che si lascia così come previsto dallo standard (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
KK	**6.2.3 REMS introduction MIME Header Fields-Body 6.2.3.1 General requirements Table 5**	REM-Section-Type: The value of this field ***should*** be: "rem_message/introduction".	***[pag 21]***	
		REM-Section-Type: The value of this field ***shall*** be: "rem_message/introduction".		**shall**[20]

KK. REM-Section-Type

Il valore del presente header è reso obbligatorio con uno ***shall*** all'interno della **REMID policy**=**REM-Policy-IT**, in coerenza con lo standard EN 319 532-4 **[4]**, Clause 5.4.3.1 Table 8 item a), relativo al profilo di interoperabilità adottato, dove questo header è prescritto come obbligatorio. Si veda la nota implementativa relativa all'elemento I-HFC-ST nelle **Table 3** e **Table 5**, nel § 2.4.2.5 e nella **Figure 19** dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
LL	**6.2.3 REMS introduction MIME Header Fields-Body 6.2.3.1 General requirements Table 5**	Content-Type: The value for this field shall be: "multipart/alternative" • 'boundary' parameter value ***should*** be conformant to IETF RFC 2046 [], section 5.1.1.	***[pag 21]***	**Si conferma il testo originario**

LL. Content-Type

La presenza del content-type e dei suoi parametri è già obbligatoria nella tabella 5 del EN 319 532-3 **[3]**. Lo ***should*** si riferisce al parametro specificato,

[20] Generalmente si usa il razionale di far prevalere le scelte più stringenti presenti nei requisiti di interoperabilità definiti nel documento EN 319 532-4 [4], rispetto ad aperture presenti nei vari altri documenti dello standard. La **REM-Policy-IT** – costituita principalmente dall'allegato tecnico - e rappresentata solo in parte dalle scelte definite nel presente documento, potrà ulteriormente restringere e rimodulare in modo opportuno queste scelte; ciò in armonia con le norme italiane, con le sensibilità del GDL e come indicato nel **razionale** in premessa, e secondo le prerogative delle autorità competenti.

che si lascia così come previsto dallo standard (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
MM	**6.2.3 REMS introduction MIME Header Fields-Body 6.2.3.2 multipart/alternative: free text subsection Header Fields Table 6**	Content-Type: The value for this field shall be: "text/plain" • 'charset' parameter value ***should*** be "UTF-8".	***[pag 22]***	
		• 'charset' parameter value ***shall*** be "UTF-8".		**shall=REM-Policy-IT** ***should*=interoperabilità**

MM. Content-Type

La presenza del content-type e dei suoi parametri è già obbligatoria nella tabella 6 del EN 319 532-3 **[3]**. Lo ***should*** si riferisce al parametro specificato che è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT** (nel rispetto delle condizioni riportate nella nota[18] a pag. 55 e a quanto deciso, sempre per questo parametro, nei requisiti presenti nel EN 319 532-4 **[4]**, Clause 5.4.3.2, Table 9 all'item a)).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
NN	**6.2.3 REMS introduction MIME Header Fields-Body 6.2.3.2 multipart/alternative: free text subsection Header Fields Table 6**	Content-Disposition: The value of this header field shall be "inline" in order to display the present body part automatically, upon display of the message in mail client. **Optional**	***[pag 22]***	
		Content-Disposition: The value of this header field shall be "inline" in order to display the present body part automatically, upon display of the message in mail client. **Mandatory**	**mandatory/ optional**	**Mandatory=REM-Policy-IT** ***Optional*=interoperabilità**

NN. Content-Disposition

Questo header permette la visualizzazione, come di consueto, del messaggio utente imbustato nel REM dispatch (l'analogo della busta di trasporto della PEC) che è reso obbligatorio (indicandolo come *mandatory* nella suddetta tabella) all'interno della **REMID policy=REM-Policy-IT**, e *optional* per agevolare l'interoperabilità per messaggi provenienti da altre **REMID policy** (nel rispetto delle condizioni riportate nella nota[18] a pag. 55 affinché l'usabilità che ne derivi sia analoga a quella dell'attuale PEC).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
OO	**6.2.3 REMS introduction MIME Header Fields-Body 6.2.3.2 multipart/alternative: free text subsection Header Fields Table 6**	Content-Transfer-Encoding: The value for this field ***should*** be: 7bit, 8bit or quoted-printable.	***[pag 22]***	**Si conferma il testo originario**

OO. Content-Transfer-Encoding

È previsto che per la **REM-Policy-IT** si lasci libera la scelta al service provider relativamente all'header riportato in tabella (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
PP	**6.2.3.3 multipart/alternative: HTML subsection Header Fields Tab 7**	Content-Type: The value for this field **shall** be: "text/html" • 'charset' parameter value ***should*** be "UTF-8".	***[pag 22]***	
		• 'charset' parameter value ***shall*** be "UTF-8".		**shall=REM-Policy-IT** ***should*=interoperabilità**

PP. Content-Type

La presenza del content-type e dei suoi parametri è già obbligatoria nella tabella 7 del EN 319 532-3 **[3]**. Lo ***should*** si riferisce al parametro specificato che è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT** (nel rispetto delle condizioni riportate nella nota[18] a pag. 55 e quanto deciso, sempre per questo parametro, nei requisiti presenti nel EN 319 532-4 **[4]**, Clause 5.4.3.3, Table 10 all'item a)).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
QQ	**6.2.3.3 multipart/alternative: HTML subsection Header Fields Tab 7**	Content-Transfer-Encoding: The value for this field ***should*** be: 7bit, 8bit or quoted-printable.	***[pag 22]***	**Si conferma il testo originario**

QQ. Content-Transfer-Encoding

È previsto che per la **REM-Policy-IT** si lasci libera la scelta al service provider relativamente all'header riportato in tabella (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
RR	**6.2.4.2 original message – MIME section Header Fields Tab 8**	Content-Description: The value for this header field ***may*** be a brief text describing the type of extension.	***[pag 23]***	**Si conferma il testo originario**

RR. Content-Description

È previsto che per la **REM-Policy-IT** si lasci libera la scelta al service provider relativamente all'header riportato in tabella (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
SS	**6.2.4.2 original message – MIME section Header Fields Tab 8**	REM-Section-Type: The value of this field ***should*** be "rem_message/original".	***[pag 23]***	
		REM-Section-Type: The value of this field ***shall*** be "rem_message/original".		**shall**

SS. REM-Section-Type

Il valore del presente header è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT**, in coerenza con lo standard EN 319 532-4 **[4]**, Clause 5.4.4 Table 11 item a), relativo al profilo di interoperabilità adottato, dove questo header è prescritto come obbligatorio. Si veda la nota implementativa relativa all'elemento I-HFC-ST nelle **Table 3** e **Table 5**, nel § 2.4.2.5 e nella **Figure 19** dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
TT	**6.2.4.3 original message – MIME section Body formats**	The REMS ***may*** modify some header fields of the original message, only if the change is limited to what is strictly necessary for the good working of the REM exchange of information. EXAMPLE: The MessageID can be changed, see notes 2 and 3 in clause 4.2.	***[pag 23]***	
		The REMS ***shall*** modify some header fields of the original message, only if the change is limited to what is strictly necessary for the good working of the REM exchange of information. EXAMPLE: The MessageID can be changed, see notes 2 and 3 in clause 4.2…		**shall=REM-Policy-IT** ***may*=interoperabilità** ***I REMS appartenenti alla REM-Policy-IT, implementano il comportamento indicato al § 2.4.2.3 dell'allegato tecnico.***

TT. *original message* – MIME section Body formats

Così come nella PEC, anche nella REM è necessaria una gestione particolare del codice identificativo (`Message-ID`) del messaggio di trasporto e dei messaggi correlati generati (ricevute, errori, ecc.). Per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, anche all'interno della **REMID policy**=**REM-Policy-IT** si deve implementare un meccanismo analogo. È reso pertanto obbligatorio il suddetto requisito con uno ***shall***. Si vedano anche tutte le altre parti del presente documento che riportano dei requisiti rispetto al `Message-ID` ed i requisiti al § 2.4.2.2 ed esempi al § 2.7 dell'allegato tecnico per i dettagli realizzativi.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
UU	**6.2.5 REMS extensions MIME Header Fields Table 9**	Content-Type: The value for this header field ***should*** be either "application/xml" or application/octet-stream. • 'name' parameter value ***should*** be "<REM_EXTENSION_NAME>". • 'charset' parameter value ***should*** be "UTF-8" in case of xml attachments.	***[pag 24]***	**L'intera sezione è opzionale.** **Si conferma il testo originario[21].**
		• 'charset' parameter value ***shall*** be "UTF-8" in case of xml attachments.		**shall=REM-Policy-IT** ***should*=interoperabilità**

UU. Content-Type

La presenza del content-type e dei suoi parametri è già obbligatoria nella tabella 9 del EN 319 532-3 **[3]**, qualora l'intera sezione "REM extensions", opzionale del MIME, fosse presente. Lo ***should*** si riferisce ai vari parametri specificati. Come indicato nella suddetta tabella si lasciano inalterati gli obblighi riguardo i primi due parametri, mentre l'ultimo parametro ***should*** è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT** (nel rispetto delle condizioni riportate nella nota[18] a pag. 55) nel caso di estensione in formato xml.

Si noti che questa specifica opzione delle estensioni MIME è quella che permette di usufruire dell'*original message* all'interno della ricevuta di consegna (ContentConsignment receipt) come indicato al § 2.4.2.5 dell'allegato tecnico.

[21] Si veda a modello esemplificativo dell'uso di questa sezione quanto riportato nella figura A.4 del EN 319 532-3 [3]:

```
Content-Type: application/octet-stream; name="extension.dat"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: attachment; filename="extension.dat"
REM-Section-Type: rem_message/extension
…
```

il quale va adattato opportunamente nei vari parametri come ad es. indicato nel seguito, avendo cura di aggiungere obbligatoriamente il parametro charset al Content-Type, nel caso in cui l'allegato della MIME extension fosse in formato xml, e l'header REM-Extension-Code avendo cura di adottare metodiche opportune per evitare sovrapposizioni (es. assegnare codice a livello **REM-Policy-IT**):

```
Content-Type: application/xml; charset=UTF-8; name="extension-1.xml"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: attachment; filename="extension-1.xml"
REM-Section-Type: rem_message/extension
REM-Extension-Code: it-extension-1
…
```

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
VV	**6.2.5 REMS extensions MIME Header Fields Table 9**	Content-Description: The value for this header field ***should*** be a brief text describing the type of extension. ***Optional***	***[pag 24]***	Si conferma il testo originario

VV. Content-Description

L'intera sezione è opzionale. Come indicato nella suddetta tabella si lasciano inalterati gli obblighi, se/quando si rendesse necessario utilizzarla, riguardo l'header in questione (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
WW	**6.2.5 REMS extensions MIME Header Fields Table 9**	REM-Section-Type: The value of this field ***should*** be "rem_message/extension".	***[pag 24]***	
		REM-Section-Type: The value of this field ***shall*** be "rem_message/extension".		shall

WW. REM-Section-Type

L'intera sezione è opzionale. Se/quando si rendesse necessario utilizzarla, lo ***should*** è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT**, in merito all'header in questione, in coerenza con lo standard EN 319 532-4 **[4]**, Clause 5.4.5 Table 12 item a), relativo al profilo di interoperabilità adottato, dove questo header è prescritto come obbligatorio (si veda esempio di nota [21] a pag. 71).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
XX	**6.2.5 REMS extensions MIME Header Fields Table 9**	REM-Extension-Code: The value of this field ***should*** be, in accordance with the type of the attachment, a unique code identifying the type of extension in order to allow automatic processing.	***[pag 24]***	
		REM-Extension-Code: The value of this field ***shall*** be, in accordance with the type of the attachment, a unique code identifying the type of extension in order to allow automatic processing.		shall=REM-Policy-IT *should*=interoperabilità

XX. REM-Extension-Code

L'intera sezione è opzionale. Se/quando si rendesse necessario utilizzarla, lo ***should*** è reso obbligatorio con uno ***shall*** all'interno della **REMID policy=REM-Policy-IT**, in merito all'header in questione, nel rispetto delle condizioni riportate nella nota[18] a pag. 55 (si veda anche esempio di nota [21] a pag. 71 riguardo il requisito di univocità del codice).

Si noti che questa specifica opzione torna utile per la corretta implementazione della funzionalità che permette di usufruire dell'*original message* all'interno della ricevuta di consegna (ContentConsignment receipt) come indicato al § 2.4.2.5 dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
YY	**6.2.5 REMS extensions MIME Header Fields Table 9**	REM-Extension-Namespace-URI: The value of this field ***should*** contain the namespace URI relevant to the extension.	***[pag 24]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

YY. REM-Extension-Namespace-URI

L'intera sezione è opzionale. Se/quando si rendesse necessario utilizzarla, è previsto che per la **REM-Policy-IT** si lasci libera scelta al service provider relativamente all'header riportato in tabella (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55 e della semantica dell'header).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
ZZ	**6.2.5 REMS extensions MIME Header Fields**	In some particular case, one of these extensions ***may*** be used to associate an electronic time-stamp to the REM message certifying the date and time of some specific event.	***[pag 24]***	***Non applicabile*** **REM baseline [4] Clause C.4.2, C.4.4** ***Il time-stamp è applicato esclusivamente alla ERDS evidence. Si veda in particolare la Nota della Clause C.4.2 del EN 319 532-4 [4]***

ZZ. REMS extensions MIME Header Fields

La soluzione prescritta nella REM baseline non comporta l'associazione del **time-stamp** attraverso l'inserimento di un nuovo allegato XML (come estensione della busta **S/MIME**) ma l'inclusione del **time-stamp** nella firma della ERDS evidence elevandola al livello XAdES-B-T. Pertanto, il ***may*** risulta non applicabile coerentemente con il **razionale** in premessa, e in quanto l'adesione alla **REM baseline** e alla **REMID policy**=**REM-Policy-IT** non prevede l'uso dell'estensione in questione. Si rimanda alle apposite sezioni dello standard EN 319 532-4 **[4]**, Clause C.4.2 e C.4.4 per il dettaglio delle varie prescrizioni relative al **time-stamp** della ERDS evidence. Si vedano anche i seguenti punti collegati:

- il § 2.3.2.2 e 2.3.2.3 dell'allegato tecnico
- il punto UUU al § 4.3.4, pag. 84

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
AAA	**6.2.5 REMS extensions MIME Header Fields**	Other extensions with other purposes ***may*** be contemporarily present. As defined in Table 2 and clause 6.2.1, extensions ***may*** also contain structured metadata or evidence components	***[pag 24]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

AAA. Other extensions

Eventuali altri allegati opzionali (estensioni della busta **S/MIME**) sono possibili in REMS (esattamente così come può avvenire nella PEC).

È previsto che per la **REM-Policy-IT** si lasci libera scelta al service provider ed, in caso se ne preveda l'utilizzo, i dati siano strutturati come indicato (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55 ed in accordo con le altre scelte relative alla Clause "6.2.5 REMS extensions" definite nei vari punti del presente documento; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
BBB	**6.2.5 REMS extensions MIME Header Fields**	Other extensions with other purposes **may** be contemporarily present. As defined in Table 2 and clause 6.2.1, extensions **may** also contain structured metadata or evidence components. In these cases: - REM-Extension-Code: value **shall** contain the component code identifying the related metadata or evidence component in Table 5 or Table 6 of ETSI EN 319 522-2 [] (e.g. I06...). - The "name" component of the Content-Type: header field: <REM_EXTENSION_NAME> **shall** be based on the component name identifying the related metadata or evidence component in Table 5 or Table 6 of ETSI EN 319 522-2 [] (e.g. name="Recipient's delegate identifier.xml"). - REM-Extension-Namespace-URI: ***should*** contain the target name space URI for the structured component.	***[pag 24]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

BBB. Other extensions

Questa scelta si riferisce all'header opzionale prescritto con uno ***should***.

Al presente punto si applicano le stesse considerazioni e condizioni del punto precedente (si vedano i commenti al punto AAA).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
CCC	**6.2.6 ERDS evidence MIME Header Fields 6.2.6.1 General requirements**	The ERDS evidence ***should*** be in XML format.	***[pag 25]***	
		The ERDS evidence ***shall*** be in XML format.		**shall**

CCC. ERDS evidence

Poiché devono essere sempre presenti delle ERDS evidence almeno nel formato XML, lo ***should*** presente nello standard EN 319 532-3 **[3]** è reso obbligatorio con uno ***shall***, in coerenza con lo standard EN 319 532-4 **[4]**, Clause 5.4.6 Table 14 item a), relativo al profilo di interoperabilità adottato, dove il formato XML per l'ERDS evidence è prescritto come obbligatorio.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
DDD	**6.2.6 ERDS evidence MIME Header Fields 6.2.6.1 General requirements**	The ERDS evidence should be in XML format. It ***may*** be in PDF format.	***[pag 25]***	**Si conferma il testo originario[22] per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

DDD. ERDS evidence

È previsto che per la **REM-Policy-IT** che le evidenze possano essere opzionalmente anche in formato PDF (come ulteriore allegato rispetto a quanto stabilito al punto CCC) oltre che in XML (obbligatorio), e si lasci libera scelta al service provider (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55 ed in coerenza con le altre scelte relative alla Clause "6.2.6 ERDS evidence MIME Header Fields" definite nei vari punti del presente documento; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
EEE	**6.2.6 ERDS evidence MIME Header Fields 6.2.6.1 General requirements**	The tag <REM_EVIDENCE_NAME> present in Table 10 and Table 11 ***should*** be replaced with the event identifier G03 to which it relates plus the ".xml" extension (e.g. SubmissionAcceptance.xml, SubmissionRejection.xml, etc.).	***[pag 25]***	
		The tag <REM_EVIDENCE_NAME> present in Table 10 and Table 11 ***shall*** be replaced with the event identifier G03 to which it relates plus the ".xml" extension (e.g. SubmissionAcceptance.xml, SubmissionRejection.xml, etc.).		**shall=REM-Policy-IT *should*=interoperabilità**

EEE. REM EVIDENCE NAME

L'uso dei seguenti filename, per le ERDS evidence, è resa obbligatoria con uno ***shall*** nel caso di **emissione** REM message all'**interno** della **REMID policy=REM-Policy-IT** (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella

[22] Si potrebbe usare il formato PDF per facilitare la lettura dell'evidenza ad un utente umano, ove se ne ravvisasse l'utilità. Infatti, l'evidenza in formato XML si presta molto di più, per sua natura, al processing applicativo.

nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza). I seguenti casi distinguono i vari tipi di messaggio e per ciascuno le possibili ERDS evidence allegate:

- **REM dispatch**: SubmissionAcceptance.xml
  [caso messaggi inviati sia all'interno che all'esterno del circuito della REM baseline: si veda SEF3 in **Table 14** dell'allegato tecnico]
- **REMS receipt**: SubmissionAcceptance.xml o SubmissionRejection.xml
  [caso equivalente alla ricevuta di accettazione in ambito PEC: si veda SEF1 & SEF2 in **Table 14** dell'allegato tecnico]
- **REMS receipt**: ContentConsignment.xml o ContentConsignmentFailure.xml
  [caso equivalente alla ricevuta di consegna in ambito PEC: si veda SEF4 & SEF5 in **Table 14** dell'allegato tecnico]
- **REMS receipt**: RelayAcceptance.xml o RelayRejection.xml
  [caso equivalente alla ricevuta di presa in carico in ambito PEC: si veda SEF6 & SEF7 in **Table 14** dell'allegato tecnico]
- **REMS receipt**: RelayFailure.xml
  [caso ricevuta di fallimento inoltro REM dispatch al service provider destinatario: si veda SEF8 in **Table 14** dell'allegato tecnico]
- **REM dispatch**: ReceivedFromNonERDS.xml
  [caso messaggi provenienti dall'esterno del circuito della REM baseline: si veda SEF9 in **Table 14** dell'allegato tecnico]

Si lascia invece lo ***should*** per agevolare l'interoperabilità, non rifiutando – quando possibile – REM message provenienti da altre **REMID policy** che non rispettino le suddette convenzioni.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
FFF	**6.2.6 ERDS evidence MIME Header Fields 6.2.6.1 General requirements**	According to the structures and the presence requirements defined in Figure 1, Figure 2 and Figure 3 it is allowed to attach more than one ERDS evidence to each REM message, if its type allows to attach ERDS evidence. These additional evidence attachments (eventually different – in terms of semantic/content/name – from all the ERDS evidence set provided with the present document) obey to peer-to-peer and/or interoperability agreements and/or specific profiles. In any case, these additional evidence attachments **should** be specified, in the MIME header fields structure, according with their type, in a similar way of that defined in clauses 6.2.6.2 (for XML), 6.2.6.3 (for PDF) and 6.2.5 (for other types of attachments).	***[pag 25]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

FFF. ERDS evidence MIME Header Fields – General requirements

Nel caso ci siano evidenze addizionali basate su particolari profili e/o accordi peer-to-peer, è ammissibile che queste vengano allegate, in base al proprio tipo seguendo le regole stabilite in 6.2.6.2, 6.2.6.3 o 6.2.5 – in caso di tipi di file diversi da XML e PDF. Come indicato nella suddetta tabella si lasciano inalterati gli obblighi all'interno della **REMID policy=REM-Policy-IT**. Si vedano sopra punti AAA, BBB, CCC e DDD (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[18] a pag. 55; si veda anche l'allegato tecnico al § 2.9.2 riguardo gli aspetti relativi alla resilienza).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
GGG	**6.2.6.2 Header Fields for XML ERDS evidence usage Table 10**	Content-Description: The value for this header field **may** be a brief text describing the type of ERDS evidence.	***[pag 25]***	**Si conferma il testo originario**

GGG.Content-Description

È previsto che per la **REM-Policy-IT** si lasci libera la scelta al service provider relativamente all'header riportato in tabella (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
HHH	6.2.6.2 Header Fields for XML ERDS evidence usage Table 10	REM-Section-Type: The value of this field should be "rem_message/xml_evidence".	*[pag 25]*	
		REM-Section-Type: The value of this field shall be "rem_message/xml_evidence".		shall

HHH. REM-Section-Type

Il valore del presente header è reso obbligatorio con uno ***shall***, in coerenza con lo standard EN 319 532-4 **[4]**, Clause 5.4.6 Table 13 item a), relativo al profilo di interoperabilità adottato, dove questo header è prescritto come obbligatorio.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
III	6.2.6.3 Header Fields for PDF ERDS evidence usage Table 11	Content-Description: The value for this header field may be a brief text describing the type of ERDS evidence.	*[pag 26]*	Si conferma il testo originario

III. Content-Description

È previsto che per la **REM-Policy-IT** si lasci libera la scelta al service provider relativamente all'header riportato in tabella, che è usato opzionalmente nel caso di presenza evidenze (come allegato addizionale) in PDF oltre che in XML (nel rispetto delle condizioni riportate nella nota[18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
JJJ	6.2.6.3 Header Fields for PDF ERDS evidence usage Table 11	REM-Section-Type: The value of this field should be "rem_message/pdf_evidence".	*[pag 26]*	
		REM-Section-Type: The value of this field shall be "rem_message/pdf_evidence".		shall=REM-Policy-IT *should*=interoperabilità

JJJ. REM-Section-Type

Usato opzionalmente nel caso di presenza evidenze (come allegato addizionale) in formato PDF oltre che in XML. Questa opzione non è nella **REM**

baseline pertanto il suo uso deve essere previsto nella **REMID policy**=**REM-Policy-IT** e vale sono all'interno della stessa. Se/quando si rendesse necessario prevederne l'uso, lo ***should*** è reso obbligatorio con uno ***shall*** all'interno della **REMID policy**=**REM-Policy-IT** (nel rispetto delle condizioni riportate nella nota[18] a pag. 55, convenzionalmente sempre presenti) per facilitare l'interoperabilità con messaggi provenienti dall'estero.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
KKK	**6.2.7 REMS signature MIME Header Fields-Body Table 12**	Content-Type: The value for this header field shall be: "application/pkcs7-signature; name=smime.p7s". • The parameter 'name' **should** be present, indicating "SignedData", as defined above.	***[pag 26]***	
		The parameter 'name' **shall** be present, indicating "SignedData", as defined above.		**Shall**

KKK. Content-Type

La presenza del `Content-Type` e dei suoi parametri è già obbligatoria nella tabella 12 del EN 319 532-3 **[3]**. Per chiarezza lo ***should*** è reso obbligatorio con uno ***shall*** relativamente al parametro "`name`" (indicato come opzionale con ***should*** nella suddetta tabella), in coerenza al constraint di interoperabilità in EN 319 532-4 **[4]**, Clause 5.4.7 Table 15 item a) il parametro "`name`" è fissato a "`smime.p7s`".

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
LLL	**6.2.7 REMS signature MIME Header Fields-Body Table 12**	Content-Disposition: The value for this header field shall be: "attachment" • 'filename' parameter value **should** be "smime.p7s".	***[pag 26]***	
		Content-Disposition: The value for this header field shall be: "attachment" • 'filename' parameter value **shall** be "smime.p7s".		**shall**

LLL. Content-Disposition

In merito alla scelta della suddetta tabella lo ***should*** è reso obbligatorio con uno ***shall***, in coerenza con lo standard EN 319 532-4 **[4]**, Clause 5.4.7

Table 15 item b), relativo al profilo di interoperabilità adottato, dove il parametro "`filename`" è obbligatoriamente fissato a "`smime.p7s`".

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
MMM	**6.2.7 REMS signature MIME Header Fields-Body Table 12**	Content-Description: The value for this header field **may** be: "S/MIME Cryptographic Signature".	***[pag 26]***	**Si conferma il testo originario**

MMM. Content-Description

Il ***may*** si riferisce al parametro specificato. È previsto che per la **REM-Policy-IT** si lasci libera la scelta al service provider relativamente a tale parametro (nel rispetto delle condizioni riportate nelle note[17] [18] a pag. 55).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
NNN	**7 REMS – evidence set formats**	Requirements for XML ERDS evidence defined in ETSI EN 319 522-3 [], clause 5 shall apply…. Furthermore, other mappings **may** be supported as agreements among interested parties.	***[pag 27]***	**Si conferma il testo originario**

NNN. REMS – evidence set formats

Indica che, oltre alle evidenze obbligatorie in formato XML, altre evidenze in altri formati concordati tra le parti possono essere presenti. Al presente punto si applicano la premessa e le condizioni del punto FFF al § 4.3.4, pag. 78 che sono da considerare prescrittive anche per il presente caso.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
OOO	**8 REMS – signatures formats 8.1 General**	The present clause specifies the format of the signatures involved in REM messages. For this purpose ETSI EN 319 522-2 [], clause 7 shall apply. The algorithms and key lengths used to generate digital signatures **should** be as specified in ETSI TS 119 312 [].	***[pag 27]***	**Si conferma il testo originario**

OOO. REMS – signatures formats

Si lascia libertà di implementazione al service provider (nel rispetto delle condizioni riportate nelle note[17] [18] a pag. 55 ed in coerenza con tutti i punti

che nel presente documento definiscono delle scelte in tema di firme digitali e/o sigilli). Si rimanda alle apposite prescrizioni al § 2.3.2.2 dell'allegato tecnico che specificano, più nel dettaglio, le varie scelte relative al sigillo da applicare ai REM message.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
PPP	**8 REMS – signatures formats** **8.1 General**	Within a REM message the following digital signatures shall apply: • **Signatures generated by a REMS** or by the delegated entity on **each ERDS evidence individually**. • **S/MIME signature** protecting all the MIME parts that constitute a REM message. This **signature is generated by a REMS**. NOTE: Senders can additionally sign the original message submitted to the recipient, supporting the signature with their own certificates. All the above signatures **may** coexist, each securing one part of the REM message.	***[pag 27]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline e nella REM-Policy-IT**

PPP. REMS – signatures formats

Il ***may*** indica la possibilità di coesistenza di più firme. Le prime due, richieste nel servizio REM, l'ultima (applicata dal sender allo user content) è opzionale ed ininfluente dal punto di vista del servizio. Si lascia pertanto alla libera scelta di implementazione del service provider.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
QQQ	**8.2 Signatures individually signing ERDS Evidence**	Signatures individually signing ERDS evidence shall comply with ETSI EN 319 522-2 [], clause 7.2 and ETSI EN 319 522-3 [], clause 5.2.2.28. In addition, in case PDF evidence format is used, the evidence **should** be protected by PadES digital signatures as defined in ETSI EN 319 142-1 [].	***[pag 27]***	
		Signatures individually signing ERDS evidence shall comply with ETSI EN 319 522-2 [], clause 7.2 and ETSI EN 319 522-3 [], clause 5.2.2.28. In addition, in case PDF evidence format is used, the evidence **shall** be protected by PadES digital signatures as defined in ETSI EN 319 142-1 [].		**shall=REM-Policy-IT** ***should*=interoperabilità**

QQQ. Signatures individually signing ERDS evidence

La protezione, tramite firma digitale, di eventuali evidenze addizionali in formato PDF nei REM message è resa obbligatoria con uno ***shall*** per tutti i

messaggi emessi all'interno della **REMID policy**=**REM-Policy-IT**. Silascia invece lo ***should*** per i messaggi provenienti da altre **REMID policy**, per agevolare l'interoperabilità (si veda il § 2.9.3 dell'allegato tecnico).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
RRR	**8.3 Signatures on REM messages**	2) The digital signature **should** be a CAdES signature according to the semantics specified in ETSI EN 319 522-2 [], clause 8.2.9.	***[pag 27]***	
		2) The digital signature **shall** be a CAdES signature according to the semantics specified in ETSI EN 319 522-2 [], clause 8.2.9.		**SI – shall** **REM baseline [4] Clause C.4.2, Table C.19 item a)**

RRR. Signatures on REM messages

In merito alla scelta della suddetta tabella lo ***should*** è reso obbligatorio con uno ***shall*** come definito, al punto suindicato, nella **REM baseline** (nel rispetto delle condizioni riportate nelle note[17] [18] a pag. 55 ed in coerenza con tutti i punti che nel presente documento definiscono delle scelte in tema di firme digitali e/o sigilli). Si rimanda alle apposite prescrizioni al § 2.3.2.2 dell'allegato tecnico che specificano, più nel dettaglio, le varie scelte relative al sigillo da applicare ai REM message.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
SSS	**8.3 Signatures on REM messages**	3) This digital signature **should** be a CAdES baseline signature as specified in ETSI EN 319 122-1 [].	***[pag 28]***	
		3) This digital signature **shall** be a CAdES baseline signature as specified in ETSI EN 319 122-1 [].		**SI – shall** **REM baseline [4] Clause C.4.2, Table C.19 item a)**

SSS. Signatures on REM messages

Al presente punto si applicano le stesse considerazioni e condizioni del punto precedente (si vedano i commenti al punto RRR).

L'oggetto in formato **S/MIME** costituente il REM message deve essere sigillato in formato CAdES (nel rispetto delle condizioni riportate nelle note[17] [18] a pag. 55 ed in coerenza con tutti i punti che nel presente documento

definiscono delle scelte in tema di firme digitali e/o sigilli). Si rimanda alle apposite prescrizioni al § 2.3.2.2 dell'allegato tecnico che specificano, più nel dettaglio, le varie scelte relative al sigillo da applicare ai REM message.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
TTT	**8.3 Signatures on REM messages**	3) This digital signature should be a CAdES baseline signature as specified in ETSI EN 319 122-1 []. This digital signature **may** include the signed attribute signature-policy-identifier, containing the explicit identifier of the signature policy governing the signing and validating processes.	***[pag 28]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

TTT. Signatures on REM messages

In merito al parametro **signature-policy-identifier** ospitato nel certificato di firma su vedano i § 2.3.2.2, 2.3.2.3 e la riga PP5 della **Table 2** dell'allegato tecnico.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
UUU	**8.3 Signatures on REM messages**	Once the CAdES-B-B baseline signature has been generated, it **should** be augmented to a CAdES-B-T baseline signature by incorporation into the digital signature of the unsigned attribute signature-timestamp, containing a time-stamp token computed as specified in ETSI EN 319 122-1 [].	***[pag 28]***	***Non applicabile*** **REM baseline [4] Clause C.4.2, C.4.4** ***Il time-stamp è applicato esclusivamente alla ERDS evidence. Si veda in particolare la Nota della Clause C.4.2 del EN 319 532-4 [4]***

UUU. Signatures on REM messages

La soluzione prescritta nella **REM baseline** non comporta l'associazione del **time-stamp** al CAdES (relativo alla firma **S/MIME** del REM message) ma l'inclusione del **time-stamp** nella firma della ERDS evidence elevandola al livello XAdES-B-T. Pertanto, lo ***should*** risulta non applicabile coerentemente con il **razionale** in premessa, e in quanto l'adesione alla **REM baseline** e alla **REMID policy**=**REM-Policy-IT** non prevede l'uso della firma digitale aumentata in questione sul CAdES. Si rimanda alle apposite sezioni dello standard EN 319

532-4 **[4]**, Clause C.4.2 e C.4.4 per il dettaglio delle varie prescrizioni relative al time-stamp della ERDS evidence. Si vedano anche i seguenti punti collegati:

- il § 2.3.2.2 e 2.3.2.3 dell'allegato tecnico
- il punto ZZ al § 4.3.4, pag. 73

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
VVV	**9.2 Routing information**	The REM RI (Relay Interface) **should** be identified by a **transport protocol**, a **hostname** and a **port** number.	***[pag 28]***	
		The REM RI (Relay Interface) **shall** be identified by a transport protocol, a hostname and a port number.		**SI – shall**[23] **REM baseline [4] Clause C.2.3.3.2, Table C.5 item b.2.4.2)**

VVV. Routing information

La parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4]** **SMTP Interoperability profile** & **REM baseline**), come indicato nello scope dello standard stesso, è basata esclusivamente sull'**SMTP**; e pertanto, coerentemente con il **razionale** in premessa lo ***should*** è reso obbligatorio con uno ***shall*** così come riportato nella suddetta tabella e quanto previsto per la Common Service Interface in accordo alle prescrizioni della **REM baseline** (si veda anche la nota[11] a pag. 37).

[23] Lo standard EN 319 532-4 [4] (SMTP Interoperability Profile) rende obbligatori almeno il DNS e l'SMTP/TLS sulla Relay Interface. L'SMTP è anche un requisito fondante di tale standard: << *…[omissis]… the present document specifies a profile …[omissis]… that use the same formats (**S/MIME based**) and the same transport protocols (**SMTP**)… [omissis]… although many aspects …[omissis]… are valid and reusable in other contexts, format and protocols … [omissis]…, all the sentences **mainly refer to SMTP** and its related updates, extensions and improvements …[omissis]…* **>>.**

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
WWW	9.2 Routing information	*The REM RI (Relay Interface) should be identified by a transport protocol, a hostname and a port number.* EXAMPLE: When the REMS uses SMTP for relay and uses DNS for routing, then for the target REM RI the protocol is implicitly SMTP, the port is implicitly 25, and the hostname is the one found in the MX record of the DNS when queried for the domain part of the recipient's identifier (which has the format of an email address, see clause 5). The target REMS can provide multiple REM RIs, and so the DNS MX records **can contain multiple** hostnames. **Other techniques may be used** either according to clause 6.1 of ETSI EN 319 522-3 [], peer-to-peer agreements between REMSPs or based on the best practices recommended in Annex A of ETSI EN 319 532-4 [].	***[pag 28]***	
				Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.2, Table C.5 item b.2.4.2); Clause C.2.3.4.2, Table C.8 item c.3.3.1); e cioè che nella REM baseline è previsto un solo MX record.

WWW. Routing information

Al presente punto si applicano le stesse considerazioni e condizioni del punto precedente (si vedano i commenti al punto VVV). Si noti che la **REM baseline**, al punto indicato nella suddetta tabella, prevede un unico hostname valorizzato nel ServiceSupplyPoint della **TL** in accordo alla semantica di tale *element*. Pertanto, attraverso il ***may*** (si veda il contesto completo in grassetto che fa riferimento a "*Other techniques*") è possibile ricondurre ad un unico valore la cardinalità degli **MX record**, così come prescritto nella REM baseline (si noti anche, a conferma di ciò, la singolarità rispetto al numero di **MX record** in ogni menzione presente nella REM baseline nei punti indicati nella suddetta tabella).

Altri protocolli possono teoricamente essere utilizzati in generale, come indicato, su base "peer-to-peer agreements" o best practices. Ma è necessario che ne sia previsto l'uso. Si rimanda quindi questa prospettiva ad ulteriori

studi e approfondimenti futuri, che potrebbero coinvolgere anche altre policy ed eventualmente altre profilature.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
XXX	**9.3 Trust information**	The requirements and explanations given in clauses 7.2 and 7.3 of ETSI EN 319 522-4-3 [] should apply to REM, with the following amendments. If Trusted List (TL) is used to publish trust information about a REMS, then the section describing a REM service shall be populated in conformance to ETSI TS 119 612 [], with the restrictions defined in Table 13.	***[pag 28]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.**

XXX. Trust information

La **REMID policy**=**REM-Policy-IT**, in coerenza al **razionale** in premessa e l'adesione alla **REM baseline**, conferma l'adozione di un modello che si appoggia all'EU Trusted List (**TL**) System nel rispetto delle condizioni ed in accordo con tutti i punti che nel presente documento definiscono delle scelte in tema di Trusted List (si veda la nota[11] a pag. 37). Si noti che la **REM baseline**, al punto indicato nella suddetta tabella, mantiene l'opzionalità dell'*element* in esame, in accordo alla semantica dello stesso. Tutte le ulteriori scelte che seguono sono conseguenza, ognuna con le proprie peculiarità, rispetto a questa.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
YYY	**9.3 Trust information**	If Trusted List is used to establish trust with another REMS, then the information in the TL should be interpreted as defined in Table 13.	***[pag 28]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.**

YYY. Trust information

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
ZZZ	**9.3 Trust information Table 13**	Service digital identity (as per clause 5.5.3 of ETSI TS 119 612 []). This element shall contain an X.509 certificate,… This element **may** contain optionally the corresponding X509SKI element.	***[pag 29]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.2 Table C.4.**

ZZZ. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
AAAA	**9.3 Trust information Table 13**	Service supply point (as per clause 5.5.7 of ETSI TS 119 612 []). This element **should** provide one or more URIs to access the REM RI (Relay Interface) defined in clause 5 of ETSI EN 319 532-1 [].	***[pag 29]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] C.2.3.3.2, Table C.5 item b.2.4.1).**

AAAA. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
BBBB	**9.3 Trust information Table 13**	Service supply point (as per clause 5.5.7 of ETSI TS 119 612 []). This element should provide one or more URIs to access the REM RI (Relay Interface) defined in clause 5 of ETSI EN 319 532-1 []. Depending on the implemented transport protocol, this element **may** provide a pointer e.g. to an SMTP server, to a web service, etc. If the Relay Interface is provided using SMTP then this URI should be an smtp: URI.	***[pag 29]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.2, Table C.5 item b.2.4.2).**

BBBB. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX. Inoltre, la parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4] SMTP Interoperability profile** & **REM baseline**), come indicato nello scope dello standard stesso, è basata esclusivamente sull'**SMTP**. (si veda il punto C al § 4.3.4, pag. 44).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
CCCC	**9.3 Trust information Table 13**	Service supply point (as per clause 5.5.7 of ETSI TS 119 612 []). This element should provide one or more URIs to access the REM RI (Relay Interface) defined in clause 5 of ETSI EN 319 532-1 []. Depending on the implemented transport protocol, this element may provide a pointer e.g. to an SMTP server, to a web service, etc. If the Relay Interface is provided using SMTP then this URI **should** be an smtp: URI.	***[pag 29]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.2, Table C.5 item b.2.4.2).**

CCCC. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
DDDD	**9.3 Trust information Table 13**	TSP service definition URI (as per clause 5.5.8 of ETSI TS 119 612 []). If present, this URI **may** point to published general information relevant to the users like public certificates, addresses, etc.	***[pag 29]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] (Figure C.1).**

DDDD. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
EEEE	**9.4 Capability management**	The REMS capability metadata **should** be in the format specified in clause 6.3.2 of ETSI EN 319 522-3 [].	***[pag 29]***	
		The REMS capability metadata ***shall*** be in the format specified in clause 6.3.2 of ETSI EN 319 522-3 [].		**SI – shall** **REM baseline [4]** **Clause C.2.3.4.1, Table C.6 item c.3.1.9) sub-item i.** **La Clause A.1 del EN 319 522-3 [7] raccoglie le varie definizioni XML incluse quelle della Clause 6.3.2 in questione**

EEEE. Capability management

La **REMID policy**=**REM-Policy-IT**, in coerenza al **razionale** in premessa e l'adesione alla **REM baseline**, conferma l'adozione di un modello che si

appoggia alle **Capability and Security Information** nel rispetto delle condizioni ed in accordo con tutti i punti che nel presente documento definiscono delle scelte in tema di capability (si veda anche la nota[11] a pag. 37). Tutte le ulteriori scelte che seguono sono conseguenza, ognuna con le proprie peculiarità, rispetto a questa.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
FFFF	**9.4 Capability management**	If the REMS uses TL to publish trust information about itself, the **REMS capability metadata may also be published using the TL**, as indicated for ERDS capability metadata in clause 7.2 of ETSI EN 319 522-4-3 []. In this case the options given in Table 14 may be used.	***[pag 29]***	***Non applicabile*** **REM baseline [4] Clauses C.1, C.2.3.4.1, Table C.6 item c.3.1.8) sub-item viii.**

FFFF. Capability management Table 14

Al presente punto si applicano le stesse considerazioni e condizioni del punto EEEE. In accordo alle prescrizioni della **REM baseline** (circa l'implementazione dei requisiti obbligatori ed opzionali dell'intero set di standard coinvolto – si veda Clause C.1 EN 319 532-4 **[4]**) ed al **razionale** in premessa, le informazioni relative alle REMS capability metadata sono pubblicate indirettamente nella **TL** attraverso la struttura XML di supporto denominata "CapabilityAndSecurityInformation". Attraverso l'opzione rappresentata dal ***may*** (si veda il contesto completo in grassetto che fa riferimento a "***may also*** *be published using the TL*") è possibile realizzare la pubblicazione dei REMS capability metadata come indicato nella Clause C.2.3.4.1, Table C.6, (dove in particolare l'item c.3.1.6) riporta la struttura XML della CapabilityAndSecurityInformation e l'item c.3.1.8) sub-item viii. il CSIDistributionPoints dove la struttura in questione è pubblicata) dello standard EN 319 532-4 **[4]**.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
GGGG	**9.4 Capability management**	If the REMS uses TL to publish trust information about itself, the REMS capability metadata may also be published using the TL, as indicated for ERDS capability metadata in clause 7.2 of ETSI EN 319 522-4-3 []. In this case the options given in Table 14 may be used.	*[pag 29]*	***Non applicabile*** **REM baseline [4] Clauses C.1, C.2.3.4.1, Table C.6 item c.3.1.8) sub-item viii.**
		Furthermore, other protocols or adaptations of the aforementioned processes may be supported, according to other documents like agreements among interested parties.		***Non applicabile*** **REM baseline [4] Clauses C.1, C.2.3.4.1, Table C.6 item c.3.1.8) sub-item viii.**

GGGG. Capability management

Al presente punto si applicano le stesse considerazioni e condizioni del punto FFFF.

4.3.5 ETSI EN 319 532-4 V1.3.1 [4] [REM – Part 4 Interoperability profiles]

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
A	**5.3.2 REM MSI: Message Submission Interface**	Implementation guidance: a) The Message Submission Interface shall be implemented with a protocol that shall secure the communication from the originating mail User Agent to the SMTP server. More specifically this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the submitted data. For example, SMTP on TLS according to IETF RFC 7817 [] or SSL plus a check of credential over SMTP-AUTH ***may*** be used.	***[pag 13]***	
		Implementation guidance: a) .... For example, SMTP on TLS according to IETF RFC 7817 [] or SSL plus a check of credential over SMTP-AUTH **shall** be used.		**Shall/at least=REM-Policy-IT**

A. REM MSI: Message Submission Interface

Questo tipo di interfaccia non risulta rilevante ai fini dell'interoperabilità in quanto condiziona unicamente il colloquio utente-mittente / **S-REMS**.

All'interno della **REMID policy=REM-Policy-IT** (in accordo alle prescrizioni della **REM baseline** riguardo i requisiti obbligatori ed opzionali – Clause C.1 EN 319 532-4 **[4]** - oltre ai requisiti riportati nella *implementation guidance* nella terza colonna della suddetta tabella, ed al **razionale** in premessa) questo requisito è reso obbligatorio con uno ***shall*** arricchito da un ***at least*** in modo da poter coprire eventuali requisiti aggiuntivi, nel caso in cui la best practice lo richiedesse (si veda il § 2.6.1 dell'allegato tecnico), attraverso un aggiornamento della policy (ad esempio evoluzioni di protocolli deprecati).

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
B	**5.3.3 REM MRI-ERI: Message and Evidence Retrieval Interface**	Implementation guidance: a) The Message and Evidence Retrieval Interface shall be implemented with a protocol that shall secure the communication from the sender/recipient mail User Agent to the REMSP server. More specifically this protocol shall ensure proper identification and authentication of the user, confidentiality of the communication, authenticity and integrity of the retrieved data. For example, IMAP or POP or HTTP on TLS according to IETF RFC 7817 [] or SSL ***may*** be used.	***[pag 13]***	
		Implementation guidance: *a) .... For example, IMAP or POP or HTTP on TLS according to IETF RFC 7817 [] or SSL **shall** be used.*		**Shall/at least=REM-Policy-IT**

B. REM MRI-ERI: Message and Evidence Retrieval Interface

Questo tipo di interfaccia non risulta rilevante ai fini dell'interoperabilità tra REMSP in quanto condiziona unicamente il colloquio utente-ricevente / R-REMS.

Al presente punto si applicano le stesse considerazioni e condizioni del punto "A REM MSI: Message Submission Interface" in quanto, anche per la 5.3.3 REM MRI-ERI, valgono le stesse considerazioni fatte per la 5.3.2 REM MSI riguardo la **REMID policy=REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
C	**5.3.5 CSI: Common Service Interface Table 6**	TL [R] TL/SMP [O] Implementation guidance: … b) The Trusting Interface, part of CSI, ***should*** be implemented using TL protocol. [R] c) The Discovery/management Interface, part of CSI, ***may*** be implemented using both or either TL or SMP protocols. [O]	***[pag 14]***	***Non applicabile*** **REM baseline [4] Clause C.1, C.2**

C. CSI: Common Service Interface - Table 6

La Common Service Interface è interamente e dettagliatamente definita all'interno della Clause C.2 dello standard EN 319 532-4 **[4]**. Pertanto, i suddetti ***may*** e ***should*** risultano non applicabili in accordo alle prescrizioni della **REM baseline** (circa l'implementazione dei requisiti obbligatori ed

opzionali dell'intero set di standard coinvolto si veda Clause C.1 EN 319 532-4 **[4]**) ed al **razionale** in premessa.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
D	**5.4.1 REMS relay metadata MIME Header Fields constraints Table 7**	REM-ReasonIdentifier [R] Implementation guidance: … d) Its value shall be the G04 component corresponding to a URI defined in table 3 of ETSI EN 319 522-3 [], clause 5.2.2.7. EventReasons is a multivalue element. This property reflects a list of REM-ReasonIdentifier header fields in REM message, each with the corresponding URI value.	***[pag 14]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline**

D. REMS relay metadata MIME Header Fields constraints Table 7

Si lascia a [R] (Raccomandato) il suddetto header, all'interno della **REMID policy=REM-Policy-IT** (secondo le cardinalità stabilite per l'elemento **REM-ReasonIdentifier** in § 2.3.2.1, **Table 3** e § 2.4.2.1, **Table 5**), per permetterne la valorizzazione durante la costruzione del REM message, quando se ne vedesse la necessità. Si veda il § 2.3.1 dell'allegato tecnico in fondo alla riga **PP24** della **Table 2** per i dettagli su come valorizzarlo, quando inserito.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
E	**5.4.3.2 multipart/alternative: free text subsection Header Fields constraints Table 9**	Content-Type [R] Implementation guidance: a) The header field constraints in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.2 shall apply. An encoding according to charset="UTF-8" parameter ***should*** be used.	***[pag 15]***	
		… a) The header field constraints in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.2 shall apply. An encoding according to charset="UTF-8" parameter **shall** be used.		**shall=REM-Policy-IT** ***should*=interoperabilità**

E. multi-part/alternative: free text subsection Header Fields constraints Table 9

Al presente punto si applicano le stesse considerazioni e condizioni del punto "MM Content-Type" al § 4.3.4, pag. 67.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
F	**5.4.3.3 multipart/alternative: HTML subsection Header Fields constraints Table 10**	Content-Type **[R]** Implementation guidance: a) The header field constraints in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.3 shall apply. An encoding according to charset="UTF-8" parameter ***should*** be used.	***[pag 15]***	
		… a) The header field constraints in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.3 shall apply. An encoding according to charset="UTF-8" parameter **shall** be used.		**shall=REM-Policy-IT** ***should*=interoperabilità**

F. multi-part/alternative: HTML subsection Header Fields constraints Table 10

Al presente punto si applicano le stesse considerazioni e condizioni del punto "PP Content-Type" al § 4.3.4, pag. 68.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
G	**5.4.6 ERDS evidence MIME Header Fields constraints Table 14**	For the ERDS evidence attachment, the present profile requires XML format (defined in clause 7.4 of ETSI EN 319 532-3[]). Optionally, the PDF format ***may*** be additionally present as defined in clause 6.2.6.3 of ETSI EN 319 532-3 [].	***[pag 16]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

G. ERDS evidence MIME Header Fields constraints

Al presente punto si applicano le stesse considerazioni e condizioni del punto "FFF ERDS evidence MIME Header Fields – General requirements" al § 4.3.4, pag. 78.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
H	**5.5.1 ERDS evidence types constraints 5.5.1.1 Mandatory evidence – all styles of operation Table 16**	Table 16: Mandatory ERDS evidence set N. 5 e 6 NotificationForAcceptance NotificationForAcceptanceFailure NOTE 3: Rationale: The sender is made aware of whether the recipient was/was not made available (within the boundaries of the recipient's REMS) of the notification the sender's REMS generated with the original message (where the sender's REMS style of operation is "S&N")	***[pag 17]***	***Non applicabile*** **REM baseline [4] Clause C.1**

H. ERDS evidence types constraints / Mandatory evidence – all styles of operation

Non viene considerato, in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, perché si riferisce allo stile S&N.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
I	**5.5.1.2 Mandatory evidence – S&N style of operation Table 17**	Table 17: Mandatory ERDS evidence set for store-and-notify	***[pag 17]***	***Non applicabile*** **REM baseline [4] Clause C.1**

I. Mandatory evidence – S&N style of operation

Non viene considerato, in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, perché si riferisce allo stile S&N.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
J	**5.5.1.3 Conditional evidence – all styles of operation Table 18** (RelayAcceptance, RelayRejection, agreement or interoperability provision)	a) RelayAcceptance [C] and RelayRejection [C] shall be generated if: - no opposite provision is explicitly specified in the applicable REMID rules; - no previous opposite agreement exists between the involved REMSPs. Such agreement or interoperability provision ***should*** specify one of the following defaults, in case of timeout: I) The sender's REMS will assume that the recipient's REMS has rejected a REM dispatch or payload if any other contrary indication (e.g. REMS receipt and or SMTP DSN) is received within a predefined time period. II) The sender's REMS will assume that the recipient's REMS has accepted a REM dispatch or payload if any other contrary indication (e.g. REMS receipt and or SMTP DSN) is received within a predefined time period. *Alternative conditions to I) and II) may be specified in the aforementioned agreement provided that these conditions deal with the relay transaction closure with an exhaustive method.* *b) If the evidence type is considered mandatory, the recipient's REMS shall send back to the sender's REMS a REMS receipt, including the RelayAcceptance or the RelayRejection evidence.* *c) Void.*	***[pag 18]***	**a)** **[C] RelayAcceptance - Sì Shall be generated (eccetto il caso R-REMS=S-REMS)** **[C] RelayRejection - Sì Shall be generated (eccetto il caso R-R-REMS=S-REMS)** **REM baseline [4]** **Table C.23, Clause C.4.5.2** **"agreement" - non applicabile** **"interoperability provision *should* specify one of I) and II)" – la REM baseline risulta prevalente per quanto non riguardi prescrizioni obbligatorie o legate a funzionalità specifiche del protocollo.** **REM baseline [4], Clause C.1** **Facendo inoltre riferimento alla REM baseline [4], Clause C.4.5.2, Table C.23** **NOTE 2 (*ERDS/REMS standard does not prescribe the intra-provider relay operation in the case when R-REMS is the same of S-REMS...*)** **si evince che la suddetta prescrizione sulla generazione delle RelayAcceptance / RelayRejection è da intendere solo nel dialogo tra REMSP differenti (cioè non nel caso in cui R-REMS=S-REMS).**

J. Conditional evidence – all styles of operation

Le varie scelte presenti nella suddetta tabella, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, seguono le prescrizioni della colonna **REM-Policy-IT**. Si veda anche quanto specificato a pag. 34 del § 2.3.2.1 dell'allegato tecnico dove è dettagliata la semplificazione del caso intra-provider dove **R-REMS=S-REMS**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
K	**5.5.1.3 Conditional evidence – all styles of operation Table 18** (Alternative conditions, b) and c))	*a) RelayAcceptance [C] and RelayRejection [C] shall be generated if:* *- no opposite provision is explicitly specified in the applicable REMID rules;* *- no previous opposite agreement exists between the involved REMSPs.* *Such agreement or interoperability provision **should** specify one of the following defaults, in case of timeout:* *I) The sender's REMS will assume that the recipient's REMS has rejected a REM dispatch or payload if any other contrary indication (e.g. REMS receipt and or SMTP DSN) is received within a predefined time period.* *II) The sender's REMS will assume that the recipient's REMS has accepted a REM dispatch or payload if any other contrary indication (e.g. REMS receipt and or SMTP DSN) is received within a predefined time period.* Alternative conditions to I) and II) may be specified in the aforementioned agreement provided that these conditions deal with the relay transaction closure with an exhaustive method. b) If the evidence type is considered mandatory, the recipient's REMS shall send back to the sender's REMS a REMS receipt, including the RelayAcceptance or the RelayRejection evidence. c) Void.	***[pag 18]***	**L'opzione "Alternative conditions" - non applicabile** **REM baseline [4], Clause C.1** **b) If the evidence… "send back" - Sì Shall REM baseline [4] Clause C.4.5.2, Table C.23 item g), h)**

K. Conditional evidence – all styles of operation

Le varie scelte presenti nella suddetta tabella, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, seguono le prescrizioni della colonna **REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
L	**5.5.1.3 Conditional evidence – all styles of operation Table 18** (RelayFailure)	d) RelayFailure [C] shall be generated if there is no explicit requirement against its generation within REMID. Such interoperability requirement ***should*** specify: III) The sender's REMS will assume that is impossible to relay a REM dispatch or payload to the recipient's REMS, if any contrary indication (e.g. REMS receipt and or SMTP DSN) is received within a predefined time period. *Alternative conditions to III) may be specified in the requirement above provided that these conditions deal with the relay transaction closure with an exhaustive method.* e) The sender's REMS shall build a REMS receipt, including the pertinent components of RelayFailure evidence (and any other contrary indication to the relay, like SMTP DSN) and shall send it back to the sender.	***[pag 18]***	**d)** **[C] RelayFailure - Sì Shall be generated** **REM baseline [4]** **Table C.24, Clause C.4.5.2** **la REM baseline risulta prevalente per quanto non riguardi prescrizioni obbligatorie o legate a funzionalità specifiche del protocollo.**

L. Conditional evidence – all styles of operation

Le varie scelte presenti nella suddetta tabella, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, seguono le prescrizioni della colonna **REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
M	**5.5.1.3 Conditional evidence – all styles of operation Table 18** **(**Alternative conditions**)**	*d) RelayFailure **[C]** shall be generated if there is no explicit requirement against its generation within REMID. Such interoperability requirement should specify:* *III) The sender's REMS will assume that is impossible to relay a REM dispatch or payload to the recipient's REMS, if any contrary indication (e.g. REMS receipt and or SMTP DSN) is received within a predefined time period.* Alternative conditions to III) ***may*** be specified in the requirement above provided that these conditions deal with the relay transaction closure with an exhaustive method. *e) The sender's REMS shall build a REMS receipt, including the pertinent components of RelayFailure evidence (and any other contrary indication to the relay, like SMTP DSN) and shall send it back to the sender.*	***[pag 18]***	**L'opzione "Alternative conditions" - non applicabile** **REM baseline [4], Clause C.1** **e) the sender's REMS … - Sì Shall** **REM baseline [4], Clause C.4.5.2** **Table C.24 item g)** **La REM baseline risulta prevalente per quanto non riguardi prescrizioni obbligatorie o legate a funzionalità specifiche del protocollo.** **REM baseline [4], Clause C.1, Clause C.4.5.2**

M. Conditional evidence – all styles of operation

Le varie scelte presenti nella suddetta tabella, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, seguono le prescrizioni della colonna **REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
N	**5.5.2 ERDS evidence components constraints 5.5.2.1 General requirements**	Evidence components not listed in table 19, table 20, table 21, table 22 and table 23 from clause 5.5.2.2 to clause 5.5.2.6 ***may*** be absent within REMS based on the present interoperability profile.	***[pag 19]***	**Questa parte dello standard è ad alto livello. La REM baseline specifica nel dettaglio quali sono i *component* da prevedere nella ERDS evidence REM baseline [4] Clause C.3.4**

N. ERDS evidence components constraints – General requirements

La scelta presente nella suddetta tabella, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, seguono le prescrizioni della colonna **REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
O	**5.5.2.2 SubmissionAcceptance – SubmissionRejection Table 19**	**Reason code [M]** a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when submission is regularly accepted. Multiple Reason codes ***may*** be present depending on the reasons that caused the evidence's triggering event.	***[pag 19]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

O. SubmissionAcceptance - SubmissionRejection - Reason code [M]

Nella **REMID policy**=**REM-Policy-IT** un solo "reason code" deve essere presente a meno che non venga previsto il contrario nelle best and security practice. Si veda il § 2.3.1 dell'allegato tecnico alla riga **PP24** della **Table 2** e le relative note per i dettagli riguardo le cardinalità dell'elemento più esterno ("container", oggetto della presente prescrizione) e quella dei sotto-elementi ("inner" Code/Details), e quanto riportato nei vari punti dell'allegato tecnico

riguardo la componente **G04** in particolare in § 2.3.2.1, **Table 3** e § 2.4.2.1, **Table 5**. Si lascia invece il ***may*** per i messaggi provenienti da altre **REMID policy** per agevolare l'interoperabilità, in accordo alle prescrizioni della **REM baseline** (circa l'implementazione dei requisiti obbligatori ed opzionali dell'intero set di standard coinvolto si veda Clause C.1 EN 319 532-4 **[4]**) ed al **razionale** in premessa.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
P	**5.5.2.2 SubmissionAcceptance – SubmissionRejection Table 19**	**Sender 's identity assurance details [O]** b) **If this field is not present**, the class of authentication is Basic. In the other cases, it specifies the class of Authentication according to the semantic of ETSI EN 319 522-2 [], clause 5.4. **Table 13 EN 319 522-2: Requirements on presence and cardinality of components in different evidence** NOTE: *(a) If more Policies are to be complied with, each requiring a specific log content and format, multiple instances of component G06 Transaction log information are possible.* (b) either "I10 Sender's identity assurance level detail" component or I11 "Sender's delegate identity assurance level detail" component **shall** be present in these evidences. I either "I12 Recipient's identity assurance level detail" component or I13 "Recipient's delegate identity assurance level detail" component shall be present in these evidences.	***[pag 19]***	**Relativamente a questo requisito prevale la prescrizione restrittiva dello standard EN 319 522-2 [6] sul *component* I10.** **Pertanto, questo livello deve essere inserito.** **Shall**

P. Sender 's identity assurance details [O]

La **REMID policy**=**REM-Policy-IT** intende implementare un servizio qualificato dove non è sufficiente una "**basic**" authentication. Pertanto, questo *component* della ERDS evidence DEVE essere presente, secondo i requisiti della Table 13 EN 319 522-2 **[6]** in cui sono specificate tutte le cardinalità per ogni tipo di ERDS evidence relativa a **servizi elettronici di recapito certificato qualificato**. Infatti, come riportato nella nota b) della suddetta tabella, la "identity assurance level" (I10) o la "delegate assurance level" (I11) ***shall*** be present. Prevedendo la REM baseline solo la prima delle due, la scelta diventa

obbligata. In ambito **REM-Policy-IT** questa proprietà è applicata ad ogni evidenza secondo le cardinalità stabilite per l'elemento **I10** in § 2.3.2.1, **Table 3**. Come descritto negli esempi del § 2.2 dell'allegato tecnico, il requisito in esame è supportato dalla modalità di identificazione dell'**utenza**, registrata (o sottoscritta) al servizio secondo le norme vigenti, e dall'aderenza allo standard EN 319 521 **[8]**, Clause 5.2.1.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
Q	**5.5.2.3 ContentConsignment – ContentConsignmentFailure Table 20**	**Reason code** [M] a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when consignment regularly occurred. Multiple Reason codes ***may*** be present depending on the reasons that caused the evidence's triggering event.	***[pag 20]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

Q. ContentConsignment - ContentConsignmentFailure - Reason code [M]

Al presente punto si applicano le stesse considerazioni e condizioni del punto O. (SubmissionAcceptance - SubmissionRejection - Reason code [M]) sopra.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
R	**5.5.2.4 ContentHandover – ContentHandoverFailure Table 21**	**Reason code** [M] a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when download regularly occurred. Multiple Reason codes ***may*** be present depending on the reasons that caused the evidence's triggering event.	***[pag 20]***	***Non applicabile*** **REM baseline [4] Clause C.1**

R. ContentHandover – ContentHandoverFailure - Reason code [M]

L'evidence di handover è opzionale e non è prevista nella **REM baseline**; e pertanto, coerentemente con il **razionale** in premessa e l'adesione alla **REM baseline** non è prevista per la **REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
S	**5.5.2.4 ContentHandover – ContentHandoverFailure Table 21**	**Recipient Authentication details [O]** b) **If this field is not present**, the class of authentication is Basic. In the other cases, it specifies the class of Authentication.	***[pag 20]***	***Non applicabile*** **REM baseline [4]** **Clause C.1**

S. ContentHandover – ContentHandoverFailure - Recipient Authentication details [O]

L'evidence di handover è opzionale e non è prevista nella **REM baseline**; e pertanto, coerentemente con il **razionale** in premessa e l'adesione alla **REM baseline** non è prevista per la **REM-Policy-IT**.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
T	**5.5.2.5 RelayAcceptan–e – RelayRejection Table 22**	**Reason code [M]** a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when the relay to the recipient's REMS regularly occurred. Multiple Reason codes ***may*** be present depending on the reasons that caused the evidence's triggering event.	***[pag 21]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

T. RelayAcceptance – RelayRejection - Reason code [M]

Al presente punto si applicano le stesse considerazioni e condizioni del punto O. (SubmissionAcceptance - SubmissionRejection - Reason code [M]).

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
U	**5.5.2.6 RelayFailure Table 23**	**Reason code [M]** a) At least one Reason code shall be present, unless the applicable REMIDs explicitly require that no Reason code is necessary when relay to the recipient's REMS failed. Multiple Reason codes ***may*** be present depending on the reasons that caused the evidence's triggering event.	***[pag 21]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

U. RelayFailure - Reason Code [M]

Al presente punto si applicano le stesse considerazioni e condizioni del punto O. (SubmissionAcceptance - SubmissionRejection - Reason code [M]).

5 Considerazioni finali

5.1 Contributi del GDL in ambito europeo

Con il presente documento il percorso avviato dal GDL AGID nel mese di ottobre 2019 ha raggiunto l'obiettivo di dare a tutti i gestori PEC italiani interessati gli elementi per sviluppare le loro piattaforme REM e realizzare i propri **servizi elettronici di recapito certificato da qualificare** in conformità ai requisiti del **Regolamento eIDAS** per il quale, così come evidenziato nei § **2** e **3.1**, si è deciso di adottare gli standard **ETSI REM** (che attraverso la **REM baseline** definiscono il set minimo di requisiti nel dialogo tra trust service provider necessari a garantire conformità al **Regolamento eIDAS**).

I suddetti standard hanno rappresentato per il GDL AGID il modello da seguire, e a minima distanza dalla realtà esistente e già consolidata in Italia, per realizzare "**by design**" e nella modalità più completa possibile i requisiti e pilastri fondanti di **eIDAS** (la cui portata è stata ulteriormente confermata e rafforzata nella cosiddetta **eIDAS 2.0** come ricordato nel § **1.1**) in termini di "**security**", "**privacy**" e "**harmonization**" (i.e. "**interoperability**") con il più ampio e auspicabile ecosistema rappresentato dal panorama europeo.

L'interazione costruttiva tra il GDL AGID e il **TC ESI** di **ETSI** è stata di impulso per la sperimentazione del modello individuato dal GDL. Le soluzioni tecniche proposte e da validare riguardavano i seguenti argomenti, legati a dettagli implementativi e all'interoperabilità del sistema, ad integrazione di quanto già presente negli standard:

- **CSI**,
- Trusted List (**TL**),
- Time stamping.

Sei Gestori **PEC** (Aruba, Poste Italiane, Telecom Italia Trust Technologies, Namirial, InnovaPuglia, InfoCert), che siedono al tavolo del GDL, hanno scelto

di cogliere l'opportunità di effettuare una PoC; sono stati predisposti gli use case e realizzata una suite di test, conclusasi a gennaio 2021 con la conferma del il corretto funzionamento del modello proposto.

Dopo aver definito la **REM baseline**, ETSI ha stabilito di condurre una fase di test (nell'ambito degli ETSI **Plugtests**™ events) al fine di verificarne le funzionalità previste, a partecipazione libera e gratuita. A seguito dell'esito dei Plugtests è stato pubblicato un draft della **REM baseline** che è stato sottoposto ad inchiesta pubblica (**ENAP** Public Enquiry / E.U. + EFTA countries) nel mese di gennaio 2022. L'inchiesta si è conclusa positivamente il 2 maggio 2022 senza voti negativi o commenti tecnici, e con una partecipazione che ha superato il 98% dei paesi aventi diritto. A seguito dei risultati, il 9 maggio è stato pubblicato lo standard ETSI EN 319 532-4 **V1.3.1** [**4**] con la **REM baseline**.

5.2 Contributi del GDL per la transizione ai servizi elettronici di recapito certificato qualificato

I gestori **PEC** che hanno partecipato al GDL hanno manifestato l'esigenza di disporre di una piattaforma campione con la quale verificare la conformità dei servizi implementati in accordo alla **REM baseline**. A tale scopo, come fu fatto per la **PEC**, AGID ha deciso di farsi carico della realizzazione di tale piattaforma da rendere disponibile sia durante il periodo transitorio (ante migrazione) che a regime, quando i servizi saranno qualificati **eIDAS** da AGID, per verificarne il mantenimento della conformità nel tempo.

Il GDL ha manifestato inoltre la necessità di definire un modello di migrazione dalla **PEC** alla REM coerente con il quadro normativo italiano esistente: tale quadro prevede che sia un DPCM a stabilire la data di migrazione.

È stata definita una soluzione in grado di condurre tutti i Gestori **PEC** in esercizio, interessati alla migrazione verso la **REM baseline** (ed ognuno con le proprie scelte tecnologiche, organizzative e strategiche) al successo della

transizione da un sistema all'altro, limitando il più possibile eventuali impatti sulla stabilità del sistema e l'interoperabilità tra Gestori.

Tale ipotesi salvaguarda inoltre anche i Gestori **PEC** non interessati alla migrazione, che potranno proseguire con l'esercizio del servizio **PEC** attualmente erogato, senza ulteriori impatti o investimenti, fino al momento dello switch-off che sarà previsto dal DPCM.

La soluzione è da intendersi quindi come la proposta che sarà portata da AGID al tavolo regolatorio del Ministero per l'innovazione e le tecnologie per l'emanazione del DPCM.

AGID
Agenzia per l'Italia Digitale

Agency for Digital Italy – Infrastructure service management

REM SERVICES

– Criteri di adozione standard ETSI: REM-Policy-IT

– Adoption criteria of ETSI standards: REM-Policy-IT

ALLEGATO TECNICO | TECHNICAL ANNEX

Version 2.0

I seguenti contributi sono stati redatti a cura di:

Edited by:

Santino Foti (InfoCert)

Marco Mangiulli (Aruba)

Carlo Vona (Poste Italiane)

Indici | Table of contents

Indice principale | Main index

Indice delle tabelle | Index of tables

Indice delle figure | Index of figures

*Nota: per facilitarne la consultazione in formato digitale, il presente documento contiene, per quanto possibile, un consistente numero di riferimenti interni applicati a vari elementi quali sigle, acronimi, figure, tabelle, etc. che rimandano, (tramite "**clic**" in avanti e "**Alt ←**" per tornare indietro), direttamente al punto in cui l'elemento stesso è definito o approfondito.*

Inoltre, per facilitare l'individuazione dei "valori" all'interno di strutture quali XML o similari è utilizzata la convenzione di metterli in evidenza tramite i colori verde ed azzurro (per le singolarità o i commenti).

*Note: to facilitate the digital consultation, the present document is provided, as far as possible, with a large number of internal cross-references applied to elements like abbreviations, acronyms, figures, tables, etc. jumping (by "**click**" to go forward, and "**Alt ←**" to turn back) directly where the element is defined or treated.*

Furthermore, to facilitate the individuation of the "values" inside XML and similar structures, the convention to outline them through green and azure (for the comments or particular points) is used.

1 Introduzione | Introduction

Il presente allegato tecnico contiene un insieme di requisiti addizionali che definiscono la cosiddetta **REMID policy** che, nel caso italiano, è identificata come "**REM-Policy-IT**" ed in piena conformità con la cosiddetta **REM baseline**. I requisiti generali della **REM baseline** e come essa si rapporta con l'intero set di standard della REM (e di conseguenza con quelli del set ERDS che sono normativamente legati alla REM) sono dettagliatamente **definiti nella Clause C.1** dell'EN 319 532-4 **[4]**. In tale paragrafo è chiaramente indicato cosa **intende garantire** la **REM baseline**, cosa **è incluso** e cosa **è escluso** da essa, ed **il principio da rispettare** per introdurre requisiti addizionali al di sopra di essa (ad es. nelle policy locali ad ogni stato membro)[24].

The present technical annex contains a set of additional requirements defining the so called **REMID policy** that, for the Italian Member State, is identified as "**REM-Policy-IT**" and it is fully compliant with the so called **REM baseline**. The general requirements of the **REM baseline** and how it relates to the full set of REM standard (and consequently with those of the ERDS set, that are normatively bound to the REM) are clearly **defined in the Clause C.1** of EN 319 532-4 **[4]**. In such clause is clearly stated what **REM baseline aims to ensure**, what **is included** and **excluded** from it, and **the principle to respect** in the introduction of additional requirements on top of it (e.g. in any member state local policies)[24].

[24] A titolo esemplificativo ma non esaustivo, la **REM baseline** [4] rappresenta il **mezzo per garantire l'interoperabilità** tra i vari REM service provider che vi aderiscono. A meno che non sia altrimenti specificato nella **REM baseline** stessa, i requisiti che sono opzionali nell'intero set di standard non si applicano tout court alla **REM baseline**; i requisiti obbligatori nel set di standard legato alla **REM baseline** sono obbligatori **anche** nella **REM baseline**. L'adozione di capabilities che non fanno parte della **REM baseline** e che sono previste ad es. nella REMID policy non devono introdurre comportamenti e funzionalità che vadano ad interrompere o compromettere l'interoperabilità.

[24] **REM baseline** [4] represents, as an example but not limited to, a **means to ensure the interoperability** among various REMSP who adhere to it. Unless it is otherwise specified in the **REM baseline** itself, the optional requirements of the full set of standards not apply, tout court, to the **REM baseline**; the mandatory requirements in set of standards bounds to the **REM baseline** are mandatory also in the **REM baseline**. The adoption of capabilities that are not part of **REM baseline** and that they are foreseen, for example, in the **REMID policy** do not introduce behaviours and features that break or compromise interoperability.

Come indicato nella Clause 3.1 del documento EN 319 532-4 **[4]** valgono i seguenti principi:

La **REMID policy** specifica i requisiti che ogni REM service provider (**REMSP** da qui in avanti) è "obbligato" a rispettare per il raggiungimento dell'interoperabilità.

La **REMID authority** è l'entità titolata a governare, stato membro per stato membro, la **REMID policy**. Nel caso italiano tale autorità è espletata da **AGID**, che ha il ruolo di gestire la **REM-Policy-IT** attraverso un processo di "supervisione" e "monitoring" dei servizi ivi attestati, ne assicuri l'aderenza ai requisiti minimi della **REM baseline** e della policy stessa, al fine di garantirne l'interoperabilità.

The following principles are valid according to the Clause 3.1 of the document EN 319 532-4 **[4]**:

The **REMID policy** specifies the requirements that every REM service provider (**REMSP** hereinafter) is "obliged" to fulfil to achieve interoperability.

The **REMID authority** is the entity entitled to govern, state member by state member, the **REMID policy**. For the Italian case this authority is carried out by **AGID**, that has the role to manage **REM-Policy-IT** through a "supervision" and monitoring process of the services therein registered, ensuring the compliance to the minimal requirements of the **REM baseline** and the policy itself, in order to guarantee interoperability.

2 Dettagli tecnici | Technical details

2.1 Requisiti generali | General requirements

La presente sezione contiene i dettagli tecnici della **REM-Policy-IT** ed è composta da una prima sezione (§ 2.2) con la connotazione tecnica di base dettata dall'intero set di standard e dalla presente policy, da una seconda sezione (§ 2.3) con la specifica di dettaglio dei parametri e comportamenti "previsti" nella **REM baseline**, da un'altra sezione (§ 2.4) con la specifica di dettaglio dei parametri e comportamenti "addizionali" alla **REM baseline** e locali alla **REM-Policy-IT**. Le sezioni che seguono (§ 2.6, 2.7 e 2.7.10.1) sono di carattere più informativo ed utili ad un più rapido raggiungimento di un'interpretazione condivisa ed uniforme sia dello standard che della **REM-Policy-IT** stessa.

The present section contains technical **REM-Policy-IT** details and it consists of: a first section (§ 2.2) containing the basic technical connotation derived from the entire standard set and from the present policy; a second section (§ 2.3) with the detailed specification of the parameters and of the "expected" behaviours in the REM baseline; another section (§ 2.4) that specifies the parameters details and behaviours "additional" to the REM baseline, and defined in **REM-Policy-IT**. The other sections (§ 2.6, 2.7 e 2.7.10.1) have an informative purpose and are useful for a quick achievement of a shared and uniform interpretation of both standard set and **REM-Policy-IT**.

2.2 Interpretazione tecnica dei principi del regolamento eIDAS | Technical interpretation of eIDAS regulation principles

La presente policy connessa al set completo di standard normativamente legato ad essa rappresenta, nel suo complesso, una concretizzazione dei principi e dei capisaldi enunciati nel **Regolamento eIDAS**.

In sintesi, la policy e gli standard forniscono uno strumento per l'implementazione di quelli che nel **Regolamento eIDAS** sono indicati come *qualified trust services*[25]. Ciò detto, è necessario sottolineare che connotare un trust service come "***qualified*** *trust service*" non è un compito esclusivamente tecnico, ma rappresenta una valutazione che invece "fa uso" degli strumenti tecnici in grado di assicurare tale proprietà (costituiti, nel nostro caso, dal set di standard utilizzati e dal presente documento). Di conseguenza il presente dispositivo tecnico, che delinea la cosiddetta **REM-Policy-IT**, colleziona e raccorda tutti i concetti utili allo scopo assumendo una fisionomia tale che, anche

The present policy is connected to the whole set of standards normatively bound to it and represents, overall, a concretization of principles and strongholds enunciated in **eIDAS Regulation**.

In synthesis, the policy and the standards give an instrument for the implementation of those that in the **eIDAS Regulation** are indicated as *qualified trust services*[25]. Having said that, it is necessary to outline that to connote a trust service as "***qualified*** *trust service*" it is not only a technical task, but it represents a decision that instead "uses" the technical instruments able to ensure such property (constituted, in our case, by the standard set and the policy represented in the present document). It follows that the present technical document, outlining the so called **REM-Policy-IT**, collects and links all the concepts useful for the scope assuming a

[25] Vedi regolamento eIDAS (EU) No 910-2014 <<*(28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of* ***qualified trust services*** *and qualified trust service provider should be introduced with a view to indicating* ***requirements*** *and* ***obligations*** *that ensure* ***high-level security*** *of whatever qualified trust services and products are used or provided.*>>

[25] See eIDAS regulation (EU) No 910-2014 <<*(28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of* ***qualified trust services*** *and qualified trust service provider should be introduced with a view to indicating* ***requirements*** *and* ***obligations*** *that ensure* ***high-level security*** *of whatever qualified trust services and products are used or provided.*>>

nella terminologia stessa, rappresenti un supporto al suddetto compito.

La presenza quindi di termini/ruoli/funzionalità, quali quelli seguenti, non deve essere interpretata come uno sconfinamento di ambito ma piuttosto come la predisposizione di concetti funzionali (spesso attraverso sinonimi e sillogismi) da vedere come ausilio all'utilizzo dello strumento tecnico stesso, al fine di concretizzare i principi espressi nei regolamenti.

A titolo di chiarezza, si fornisce il seguente schema interpretativo semplificato.

Il primo atto è quello di fornire una panoramica del servizio fortemente orientata al *punto di vista dell'utente*.

La REM è per definizione una "**registered**" e-mail; e per semplicità, nel presente documento, il termine “registered” è utilizzato per indicare l’utente che si “sottoscrive” (cioè si registra) al servizio; oltre che ovviamente, sulla base del contesto, indica che si tratta di messagistica “tracciata” in qualche misura su dei registri (cioè registrata). Si vuole rimarcare bene questo concetto attraverso la seguente

physiognomy such that, even in its own terminology, represents a support to the aforementioned task.

Therefore, the presence of terms/roles/functionalities, like the following, must not be interpreted as trespassing of boundaries. Rather they are a predisposition of technical concepts (often throughout synonyms and syllogisms) as aids to the use of the technical instrument itself, and in order to implement the principles expressed in the regulations.

For a clarity, is provided the following simplified schema.

The first act is to provide a service overview strongly oriented to the *user's viewpoint*.

The REM is by definition a "**registered**" e-mail; and for the sake of simplicity, in the present document, the term “registered” is used to denote the users that are “subscribed” (i.e., registered) to the service; and of course, depending on the context, it means that we are dealing with messages tracked in some extent to some registry (i.e., registered). The following **Figure 1** (and from

Figure 1 (e dalla **Figure 2** alla **Figure 5** per le condizioni di errore) che serve a contraddistinguere, ad alto livello, l'uso *interno* al servizio (cioè interscambi tra **utenze** in qualche modo "**registrate**" al servizio REM visto come un'unica entità di REMS in qualche modo federati, trusted e tra loro interoperabili[26]) dall'uso da/per l'*esterno* del suddetto servizio (cioè interscambi con sistemi diversi quali ad esempio la posta elettronica ordinaria).

Di seguito si riportano alcune definizioni di principio su cui è basato il modello rappresentato con la **REM-Policy-IT**. I termini *utente* e ***utenza*** sono assimilati alla stessa entità, quando non diversamente specificato, in accordo alla loro accezione più generale ed

Figure 2 to **Figure 5** for the error conditions) emphasize from an high level view perspective, the *internal* use of the service from the *from/to-external* one. Where, the *internal* use is for interchanges between users "registered" to the REM service (seen as a unique entity of somehow mutually federated/trusted and interoperable REMSs[26]). Whereas the external use is for interchanges with different systems (e.g., like ordinary e-mail).

Follows some definitions of the principles at the basis of the model represented by the **REM-Policy-IT**. The terms *user* and ***account*** are assimilated to the same entity, unless otherwise specified, according to their most general and abstract

[26] Le proprietà che regolano la federazione, il trust e l'interoperabilità (e quindi cosa è considerato interno o esterno al sistema) sono costituite proprio dal set di standard ETSI utilizzato e dall'aderenza alla **REM baseline**, come indicato nello standard EN 319 532-4 [4], Clause C.1. La presenza delle policy (nel nostro caso della **REM-Policy-IT**) fornisce ulteriori dettagli utilizzabili dalle norme e dai regolamenti locali per effettuare il **collegamento** del servizio alla specifica realtà nazionale, ma sempre con l'attenzione che eventuali funzionalità, scelte o aggiunte siano realizzate attraverso modalità che preservino l'interoperabilità cross-border con altre realtà aderenti alla **REM baseline** [4]. Pertanto, nel contesto ricoperto dalla **REM baseline**, il livello di interoperabilità di interesse è esclusivamente quello tra REMSP che gestiscono utenza registrata in accordo allo standard e ai regolamenti vigenti.

[26] The properties regulating the federation, the trust and the interoperability (and so what is considered internal or external to the system) are constituted just by the ETSI set of standards and by the adherence to the **REM baseline**, as per the standard EN 319 532-4 [4], Clause C.1.

The presence of the policies (in our case of the **REM-Policy-IT**) provides further details usable by rules and local regulations as a **connection** of the service to specific national reality, but always with the attention to preserve cross-border interoperability with other realities that adhere to the **REM baseline** [4]. So, in the context covered by the **REM baseline**, the interesting interoperability level is exclusively that among REMSPs handling registered users according to the standard and to the current regulation in force.

astratta (si veda invece la **Table 16** al § 2.8.1 per ulteriori dettagli).

Utenza registrata (registered): **utenza** che è necessario sia registrata presso un REMSP perché possa usufruire del servizio REM, nel pieno delle sue potenzialità. In altre parole, il servizio è inteso nel pieno delle potenzialità quando la trasmissione avviene tra utenze sottoscritte al servizio stesso, come spiegato in dettaglio nel seguito (si veda **Table 1** ed in particolare la prima riga **TUC1** che illustra tale tipo di trasmissione).

Utenza identificata (identified): il processo di registrazione prevede che il **titolare** dell'**utenza** ("**titolare registrato**") venga "identificato" secondo le norme vigenti prima di utilizzare il servizio. Tipicamente l'identificazione avviene solo una volta, inizialmente, come indicato nello standard EN 319 521 **[8]**, Clause 5.2.1 "initial identity verification" ed in accordo all'interpretazione e gli adattamenti alle realtà locali, che sono stabiliti all'interno dei regolamenti nazionali vigenti.

Utenza autenticata (authenticated): il processo di registrazione al servizio REM, una volta identificato il **titolare**, prevede che vengano rilasciate delle **credenziali** sicure, una per ognuno degli utenti fisici (persone o

meaning (see instead **Table 16** and § 2.8.1 for further details).

Registered users: users **account** needed to be registered to a REMSP so that they can take benefit, on its full potential, of the REM service. In other words, the service is intended on its full potential when the transmission takes place between users subscribed to the service itself, as detailed below (see **Table 1** and in particular the first row **TUC1** that illustrates such type of transmission).

Identified users: the registration process foresees that the **owner** of the user(s) **account** ("**registered holder**") is "identified" according to the regulations in force before the use of the service. Typically, this procedure occurs only once, initially, as outlined in the standard EN 319 521 **[8]**, Clause 5.2.1 "initial identity verification" and according to the interpretation and arrangement to the local realties, that are defined inside national regulations in force.

Authenticated users: the registration process to the REM service, once identified the **owner**, foresees that a set of secure **credentials** will be released: one for each physical user (individual and/or application one) will really access to the "**registered email**" (or **REM mailbox(es)**) subscribed by

applicativi) che accederanno alle "**registered email**" (o **casella/e REM**) sottoscritte dal **titolare**. In altre parole, il **titolare** è il soggetto fisico o giuridico che "sottoscrive" il servizio presso un REMSP (diventando un **titolare registrato**); il REMSP crea la relativa **utenza** che lo abilita all'accesso del servizio. A tale **utenza** sono associate una o più "**registered email**" o caselle (indicate sopra come "utenti fisici" del servizio utilizzabili da utenti umani o applicativi) cui sono associate delle **credenziali** sicure e distinte, una o più per ognuna di esse.

Il processo di accesso al servizio mediante "autenticazione forte"[27], come indicato nello standard EN 319 521 **[8]**, Clause 5.2.2 ed in accordo all'interpretazione e gli adattamenti che sono stabiliti all'interno dei regolamenti nazionali, fornisce tutte le garanzie richieste rispetto all'uso pieno e corretto del servizio[28].

the **owner**. In other words, **owner** means the person (natural or legal person) requesting to a REMSP the subscription to the service (becoming a **registered holder**); the REMSP creates the relevant **account** enabling to the access of the service. One or more of these "**registered emails**" or mailboxes (mentioned above as "physical users" of the service usable by individual users or applications) are associated to such **account**, and have distinct and secure **credentials**, one or more for each of them.

The access process to the REMS by a "strong authentication"[27], as prescribed in standard EN 319 521 **[8]**, Clause 5.2.2 and according to the interpretation and arrangement to the local realties, that are defined inside national regulations in force, provides all the necessary guarantees regarding the full and correct use of the service[28].

[27] In altre parole, la procedura di "autenticazione", attraverso i propri meccanismi di sicurezza, permette di perpetuare nel tempo, e ad ogni uso, il processo di identificazione iniziale. Dal punto di vista del servizio, ogni REMSP, ad ogni autenticazione, ha tutte le garanzie che l'utilizzo del servizio da parte delle utenze sottoscritte (individualmente e opportunamente tracciate) sia indissolubilmente legato all'identificazione del titolare attraverso i dati da lui forniti, riguardo gli utilizzatori, durante la registrazione iniziale. È questa la ragione per cui non è necessario identificare, ogni volta, chi usa il servizio ma è sufficiente che sia autenticato, individualmente, in modo forte, durante ogni accesso.

[28] Si veda anche ad es. il § 2.4.2.7 relativo agli accessi da client utente con protocolli standard.

[27] In other words, the "authentication" procedure, through itself security mechanisms, allows to perpetuate over time, at any use, the initial identification process. From the service point of view, every REMSP, at each authentication, is fully guaranteed that the service utilization, by the subscribed users account, is indissolubly bound (and tracked) to the identification data given by the owner, regarding any user, during the initial registration. This is the reason why it is not necessary to identify, every time, who uses the service. While it is enough that the user is authenticated, individually, in strong manner, during any access.

[28] See for ex. § 2.4.2.7 relative to the login from the client user with standard protocols.

Il secondo passo è quello di connettere *il punto di vista dell'utente* con *le modalità di trasmissione*.

La seguente **Table 1** riassume, dal punto di vista tecnico[29], le caratteristiche relative ai tipi di trasmissione possibili, all'interno e da/per l'esterno del circuito **REM baseline**, in relazione ai ruoli delineati sopra.

In particolare:

1. Trasmissione assicurata tra **utenze** registrate[30].
2. Livello di assicurazione nella trasmissione tra **utenza** registrata e **utenza** non registrata.
3. Livello di assicurazione nella trasmissione proveniente da **utenza** non registrata verso **utenza** registrata.

Thereby, a further step is to correlate *the user viewpoint* with the *modes of transmission*.

The following **Table 1** sums up, from a technical viewpoint[29], the characteristics relevant to the possible types of transmission, *inside* and from/to *outside* the **REM baseline** circuit, considering the aforementioned roles.

In particular:

1. Ensured transmission between registered users **account**[30].
2. Level of assurance of transmission between registered and not registered users **account**.
3. Level of assurance in the transmission coming from not registered towards registered users **account**.

[29] In coerenza con l'ambito e lo scopo della presente documentazione, i flussi qui messi in evidenza sono sempre da mettere in relazione, e quindi considerare regolamentati, dalle norme nazionali correntemente vigenti.

[30] L'intenzione, qui, è di mettere in evidenza l'utenza che fa parte "a pieno titolo" del servizio, e distinguerla da quella che non ne fa parte, o ne fa parte solo in modo parziale. Il processo di "registrazione" scandisce proprio questa differenza. Rimane ovvio che nel caso in esame relativo al punto 1., oltre alla registrazione, per poter accedere ai contenuti trasmessi è indispensabile anche l'autenticazione, da considerare quindi implicitamente sottintesa per entrambi gli attori Sender/Recipient (si veda caso **TUC1** del suddetto schema di **Table 1**: massima garanzia punto-punto tra utenze "registrate"). Pertanto, la locuzione *trasmissione assicurata* è da intendere nel presente documento come trasmissione "**garantita**" da punto a punto.

[29] In coherence with the scope of this documents, the flows outlined here are always to put in relation, and therefore considered regulated, from national regulations currently in force.

[30] The scope, here, is to make evident the users that are part "with full right" of the service, and distinguish them from those that are not part, or that are a partially part. The "registration" process marks just this difference. It remains obvious that in the case under consideration relevant to point 1., beside registration, to access to the transmitted content it is needful also the authentication, to consider implicitly implied for both Sender/Recipient (see case **TUC1** of **Table 1**: maximum guarantee point-to-point between "registered" users). Therefore, the expression *ensured transmission* is to be understood in the present document as point-to-point "**granted**" transmission.

Table 1 – REMS Intra/inter transmission of "user content" between users

Id	Sender	Recipient	Transmission type
TUC1	**registered**	**registered**	Intra-REM Transmission "**ensured**" from the sender up to the recipient of the REM service (e.g., provided by a set of interoperable REMSPs applying the REM baseline). See **Figure 1**.
TUC2	**registered**	**unregistered**	Outflow Transmission "**ensured**" from the sender up to the S-REMS. The "**last stretch**" from S-REMS, through R-REMS, to the recipient (that could be also registered to another type of service) is "**not ensured**", in the sense of the REM standards, by a end-to-end evidence. See **Figure 6.**
TUC3	**unregistered**	**registered**	Inflow Transmission "**ensured**" from the R-REMS up to the recipient. The "**first stretch**" from the sender (that could be also registered to another type of service), through its provider, to the R-REMS is "**not ensured**" in the sense of the REM standards, by a end-to-end evidence. See **Figure 8.**

Come conseguenza alle suddette considerazioni, già l'evidenza di presa in carico dell'**R-REMS** (REM **RelayAcceptance** receipt), possibile solo nelle trasmissioni tra REMSP, potrebbe rilevare che il destinatario sia non "pertinente" (e cioè non "registrato") presso l'R-REMS che la emette. Pertanto, tale ricevuta (ad es. una cumulativa per ogni R-REMS, o comunque un insieme esaustivo di ricevute rispetto alla totalità degli utenti destinatari, indipendentemente dal fatto che la REM **RelayAcceptance** provenga da uno o più R-REMS) può già fornire garanzia che la trasmissione stia avvenendo tra **utenze** in quel momento registrate (cioè come indicato nella tipologia **TUC1** in **Table 1**). Mentre la ricevuta di avvenuta consegna (REM **ContentConsignment** receipt), rappresenta poi l'elemento che chiude definitivamente il

As consequence of the aforementioned considerations, already the evidence of occurred relay by **R-REMS** (REM **RelayAcceptance** receipt), possible only in transmissions between REMSPs, could detect that the intended recipient is not "pertinent" (and so not "registered") at the R-REMS issuing it. Therefore, such receipt (e.g., one cumulative for each R-REMS, or anyway an exhaustive set of receipt in respect to the entirety of recipients, independently if these come from one or more R-REMSs) can already provide assurance that the transmission is occurring between users at that time registered (i.e., as per the type **TUC1** in **Table 1**). While the evidence of occurred delivery (REM **ContentConsignment** receipt), represents the element closing the entire cycle

ciclo (a copertura dei casi volutamente non gestiti nella **RelayAcceptance** o cambiamenti di stato dell'**utenza** sopraggiunti dopo tale evento) e fornisce tutte le garanzie (o assicurazioni per usare lo stesso termine specificato all'inizio) riguardo la avvenuta trasmissione dello *user content* dal mittente fino alla mailbox del destinatario[31].

Si noti infine che i meccanismi di identificazione dell'**utenza** sono regolati da opportuni *assurance level* descritti più nel dettaglio nel § 2.4.2.14.

Si faccia riferimento al § 2.3.2.1 riguardo i macro tipi trasmissioni previsti (rappresentati in **Table 1**) in correlazione alla granularità più marcata dei flussi e degli eventi definiti nella **Figure 1** e dalla **Figure 2** alla **Figure 5** per le condizioni di errore.

(covering cases intentionally not managed during the **RelayAcceptance** or status change of the recipients occurring after such event) and it provides the overall assurances regarding the occurred transmission of the *user content* from the sender to the recipient mailbox[31].

Finally, note that the user's identification mechanisms are regulated by appropriate *assurance levels* described in detail in § 2.4.2.14. See the reference § 2.3.2.1 regarding the intended macro-types of transmissions (represented in **Table 1**) in correlation to the more marked granularity of the flows and events defined in **Figure 1**, and from **Figure 2** to **Figure 5** for the error conditions.

[31] Infatti, in un sistema distribuito, non è ritenuta un'informazione accurata quella di fornire assicurazione al mittente che un destinatario sia effettivamente "**registrato**" all'R-REMS (e cioè che abbia superato le fasi di identificazione iniziale, e che quindi sarà obbligato ad autenticarsi per poter prelevare il contenuto inviatogli) durante l'invio del messaggio. Ecco perché questa assicurazione non può essere data con la SubmissionAcceptance REMS receipt. Ma invece è necessario che, prima della "delivery" del contenuto: (1) l'R-REMS si assicuri che il ricevente sia "**registrato**", e (2) produca tale assicurazione al mittente con l'invio della ContentConsignment REMS receipt al mittente (si noti che la RelayAcceptance non è sufficiente perché alcuni servizi potrebbero decidere di effettuare il controllo solo prima della delivery).

[31] In fact, in a distributed system, it is not considered an accurate information to provide insurance to the sender that a recipient is effectively "**registered**" to the R-REMS (and therefore, that the recipient has passed the initial identification phase, and she/he will be obliged to the authentication to withdraw the content sent to her/him) during the message sending phase. That's why this assurance cannot be supplied in the SubmissionAcceptance REMS receipt. Whereas is certainly accurate that, before the "delivery" of the content: (1) R-REMS make sure that the receiving is "**registered**", and (2) R-REMS produces such insurance with sending the ContentConsignment REMS receipt to the sender (note that the RelayAcceptance is not sufficient because some service could decide to implement the existence check only before the delivery.

2.3 Scelte parametri e funzioni della REM-Policy-IT previste dalla REM baseline | REM-Policy-IT parameters and functions envisaged in REM baseline

2.3.1 Parametri | Parameters

Nella seguente **Table 2** è riportata la specifica, all'interno della **REM-Policy-IT**, di parametri previsti all'interno della REM baseline.

In the following **Table 2** is given the specification, inside the **REM-Policy-IT**, of parameters that are envisaged inside the REM baseline.

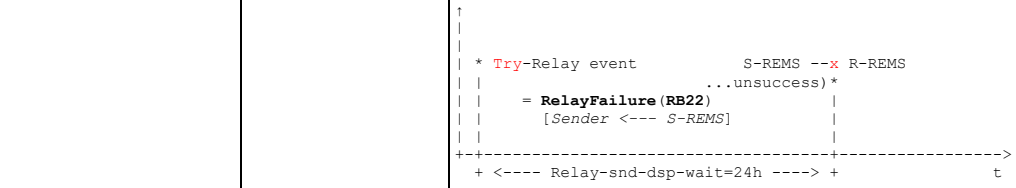
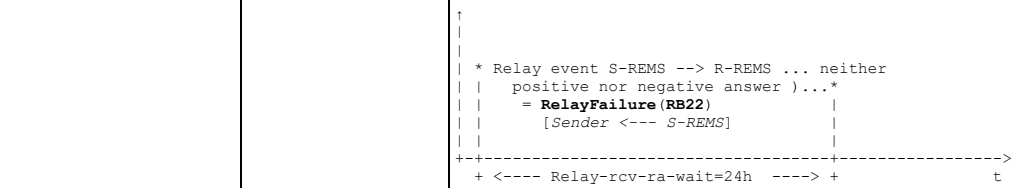
Table 2 – Parameters and main properties of the REM baseline

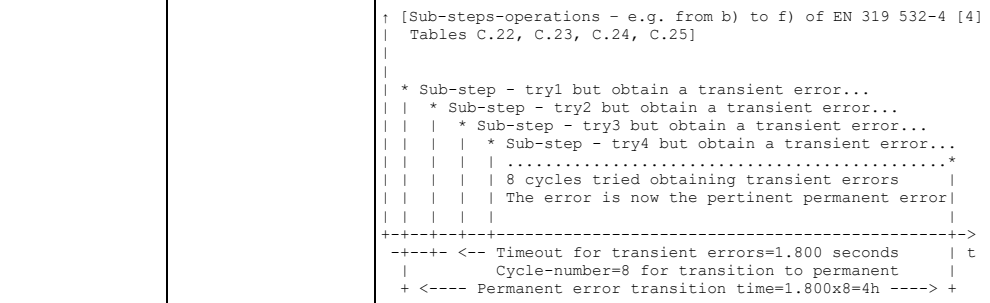
ID	Element / Parameter	Reference	Prescription
PP1	Any ERDS evidence UserContentInfo PartInfo **DigestMethod** algorithm Any REM dispatch Any REMS receipt **REM-DigestAlgorithm**	EN 319 532-4 **[4]**, Clause C.3.4 Table C.18, l), EN 319 522-2 **[6]**, **M02** EN 319 522-2 **[6]**, **MD14** NIST.FIPS.180-4 **[14]** https://www.w3.org/TR/xmldsig-core2/ 3.1.1, 10.1	Algorithm used for the digest of entire "*original message*" during emission (i.e., for any ERDS evidence and REM message issued inside REM-Policy-IT): http://www.w3.org/2001/04/xmlenc#sha256 Algorithms, from RFC 6931 [18], accepted from other policies during verification phases: http://www.w3.org/2001/04/xmlenc#sha256 http://www.w3.org/2001/04/xmldsig-more#sha224 http://www.w3.org/2001/04/xmldsig-more#sha384 http://www.w3.org/2001/04/xmlenc#sha512 The present digest algorithm is set in: **PartInfo/DigestMethod** ERDS evidence element and in the following REM dispatch / REMS receipts header: **REM-DigestAlgorithm** *Note that this algorithm is subject to the current security practices (see § 2.6.1).*
PP2	Any ERDS evidence UserContentInfo PartInfo **DigestValue** Any REM dispatch Any REMS receipt **REM-DigestValue**	EN 319 532-4 **[4]**, Clause C.3.4 Table C.18, l), EN 319 522-2 **[6]**, **M02** EN 319 522-2 **[6]**, **MD14** NIST.FIPS.180-4 **[14]** https://www.w3.org/TR/xmldsig-core2/ 3.1.1, 10.1	Value of the digest of entire "*original message*" during emission computed according to algorithm specified above in PP1. The digest value, obtained with such algorithm is set in: **PartInfo/DigestValue** ERDS evidence element and in the following REM dispatch / REMS receipts header: **REM-DigestValue** The digest-value is computed as the **SHA256** digest of "*original message* MIME part" (in base64 format). Note that, as defined in EN 319 532-4 **[4]**, Clause C.4.5.1 Table C.22, item c) sub-item V. point i. and NOTE 1, the "*original message*", upon which to calculate the digest value, is conventionally converted in the Canonical Encoding Model, and so terminated by «0d0a» pair of bytes (CRLF windows end-of-line marker; see Section 4(2) of RFC 2049 [15]).

PP3m	**MessageIdentifier / Message-ID**	EN 319 522-2 **[6]**, **M01 /** EN 319 532-3 **[3]**, **MD11** Table 2, Table 3	**MessageIdentifier** element is a unique identifier as defined for the **M01/MD11** components in EN 319 522-2 [6], Clause 6.2.1 and, as mentioned in NOTE 2 of EN 319 532-3 [3], Clause 4.2, it is mapped to the **Message-ID** of the REM dispatch. In particular, for any ERDS evidence and REM dispatch issued inside REM-Policy-IT, the same identifier is represented by a UID generated according to RFC 5322 [17], section 3.6.4. It is recommended to use the angle bracket characters '<' '>' for the **Message-ID** header but not for **MessageIdentifier** ERDS evidence element. EXAMPLE - *REM dispatch*: Message-ID: <2669.rem-service@s-rems-only-for-test.it> - Any *ERDS evidence* related to such REM dispatch: <tns:MessageIdentifier>2669.rem-service@s-rems-only-for-test.it</tns:MessageIdentifier> Using the same syntax rules above, all the REMS receipts have a per-receipt specific **Message-ID** header, and the same **MessageIdentifier** ERDS element contained in the SubmisisonAcceptance/REM dispatch. EXAMPLE - *REM RelayAcceptance receipt*: Message-ID: <6670.rem-service@r-rems-only-for-test.it> - RelayAcceptance *ERDS evidence* (related to the REM dispatch above): <tns:MessageIdentifier>2669.rem-service@s-rems-only-for-test.it</tns:MessageIdentifier> See arrows Nr. 2, 4, 6 and 8 on the left of the examples from Figure 15 up to Figure 18 for a full illustration of these settings, and § 2.4.2.3 for more details. *Note that* **Message-ID** *value inside the ERDS evidence can optionally appear either with* '<' and '>' sequences in place of the angle bracket characters '<' '>' respectively or without them (e.g., as per arrow Nr. 2 on the left of the example of Figure 15).
PP3e	**EvidenceIdentifier [,ID] / REM-Evidence-ID**	EN 319 522-2 **[6]**, **G01** EN 319 522-3 **[7]**, Clause 5.2.2.3 **/** EN 319 532-4 **[4]**, Clause 5.4.1 Table 7, c)	**EvidenceIdentifier** element is a unique identifier as defined for the **G01** component in EN 319 522-2 [6], Clause 8.2.1 and, as mentioned in EN 319 532-4 **[4]**, Clause 5.4.1 Table 7, item c) (row N° 3), it is mapped to the **REM-Evidence-ID** of any REM message. In particular, for any ERDS evidence and REM message issued inside REM-Policy-IT, the same identifier is represented by a UID generated according to RFC 5322 [17], section 3.6.4. It is recommended to use the angle bracket characters '<' '>' for the **REM-Evidence-ID** header but not for **EvidenceIdentifier** ERDS evidence element. EXAMPLE - *REM dispatch*: REM-Evidence-ID: <16C1.rem-service@s-rems-only-for-test.it> - SubmissionAcceptance *ERDS evidence* related to such REM dispatch: <tns:EvidenceIdentifier>16C1.rem-service@s-rems-only-for-test.it</tns:EvidenceIdentifier> Using the same syntax rules above, all the REMS receipts have a per-receipt specific **REM-Evidence-ID** header aligned with the **EvidenceIdentifier** ERDS element contained in the REM message. EXAMPLE - *REM RelayAcceptance receipt*: REM-Evidence-ID: <56C2.rem-service@r-rems-only-for-test.it> - RelayAcceptance *ERDS evidence* (attached to such REMS receipt): <tns: EvidenceIdentifier >56C2.rem-service@r-rems-only-for-test.it</tns:EvidenceIdentifier> See arrows Nr. 1, 5, and 7 on the left of the examples from Figure 15 up to Figure 18 for a full illustration of these settings, and § 2.4.2.3 for more details. *Note that* **REM-Evidence-ID** *value inside the ERDS evidence can optionally appear either with* '<' and '>' sequences in place of the angle bracket characters '<' '>' respectively or without them (e.g., as per arrow Nr. 1 on the left of the example of Figure 15).

PP3o	**AppLayerIdentifier / REM-UAMessageIdentifier**	EN 319 522-2 **[6]**, **M02 /** EN 319 532-3 **[3]**, **MD11-MD14** Clause 6.1 Table 2, Clause 6.2.1	When the sender's user agent specifies the Message-ID in the *original message*, its value is set in the **AppLayerIdentifier** element, according to the component **M02 / MD14** EN 319 522-2 [6], Clause 6.2.14 (given that the **Message-ID** header of both *original message* and REM dispatch is [re-]set to the same new UID specified in **PP3m**). In particular, for any ERDS evidence and REM message issued inside REM-Policy-IT, the same *original message* Message-ID identifier is mapped, as it is, also to the **REM-UAMessageIdentifier** header of any REM message (and of the *original message*). It is recommended to use, only for the **AppLayerIdentifier** ERDS element, '<' and '>' sequences in place of the angle bracket characters '<' '>' respectively (given that the angle brackets are XML delimiters). EXAMPLE - *REM dispatch*: REM-UAMessageIdentifier: <30f0$@de> - *original message*: REM-UAMessageIdentifier: <30f0$@de> - SubmissionAcceptance *ERDS evidence* related to such REM dispatch: <AppLayerIdentifier><30f0$@de></AppLayerIdentifier> Using the same syntax rules above, all the REMS receipts have the same **REM-UAMessageIdentifier** header aligned with the **AppLayerIdentifier** ERDS element contained in the REM message and in the REM dispatch. EXAMPLE - *REM RelayAcceptance receipt*: REM-UAMessageIdentifier: <30f0$@de> - RelayAcceptance *ERDS evidence* (attached to such REMS receipt): <AppLayerIdentifier><30f0$@de></AppLayerIdentifier> See all the arrows Nr. 3 on the left of the examples from Figure 15 up to Figure 18 for a full illustration of these settings, and § 2.4.2.3 for more details.
PP4	**Subject**	EN 319 532-3 **[3]**, Table 2, Table 3	The subject of the *original message* is replicated to the subject of any REM message related to it, according to a set of mapping rules. See Table 14 § 2.4.2.10 for more details.
PP5	signature-policy-identifier	EN 319 532-3 **[3]**, Clause 8.3 EN 319 532-4 **[4]**, Clause C.4.2, Table C.19, b) Table C.20, d) Clause D.2.2.3	This element is left optional. Inside **REM-Policy-IT** its presence and / or possible values can be ignored.

PP6	*SignatureMethod* of REM message EMLs digital signatures *micalg* and S/MIME type of REM message digital signatures	EN 319 532-4 **[4]**, Clause C.4.2 Table C.19, a), Table C.19, b)	Algorithm and type of S/MIME signature of any REM message. At S/MIME level the key points are: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha-256; For **REM-Policy-IT** the following additional properties shall apply: The S/MIME digital signature is also a **CAdES** baseline digital signature. The **SHA256** Digest Algorithm is used for the CAdES S/MIME digital signature. In order that the S/MIME signature is automatically validated by any email client it is necessary that the digital certificate contains the extension: **X509v3 Subject Alternative Name (SAN) set to the email address of the *From* header. It represents the signer and it is set (by using the rfc822Name CHOICE of the GeneralName type of the present X09v3 extension according to IETF RFC 5750** [16]**, section 4.4.3**. In case of REM dispatch, the From: header containing the signer email address is compliant with the form defined at the point **AP4** of **Table 4**. *Note that this parameter is subject to the current security practices (see § 2.6.1).*
PP7	*SignatureMethod* and *SignatureTimeStamp* of ERDS evidence XMLs digital **Signature**	EN 319 532-4 **[4]**, Clause C.4.3 Table C.20, c) Table C.20, d) EN 319 532-4 **[4]**, Clause C.4.4 Table C.21, e)	Algorithm and methods XML signature of any ERDS evidence. At XML level the key points are: <ds:Signature Id="xx"><ds:SignedInfo>… <ds:SignatureMethod Algorithm="http://www.w3.org/..."/> … It is a **XAdES-B-B** baseline digital signature. For **REM-Policy-IT** the Algorithm to use is: SignatureMethod Algorithm=**http://www.w3.org/2001/04/xmldsig-more#rsa-sha256.** Furthermore, the XAdES-B-B has to be augmented by the **time-stamp** in order to achieve the **XAdES-B-T** level. At XML level the key points are: <xades:SignatureTimeStamp Id="xx"> Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/> Where xml-exc-c14n represents, in this example, the canonicalization method. *Note that anyone of the aforementioned values is subject to the current security practices, and so it may change during the time (see § 2.6.1).*
PP8	Certificate properties	EN 319 532-4 **[4]**, Clause D.2.2	See § 2.4.2.11

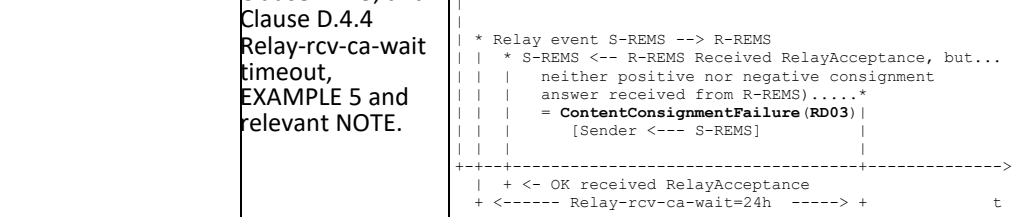
PP9	**SenderDetails/Identity** **RecipientDetails/Identity** PersonIdentifierType "**CC**"/"**CC**"/"**userid**"	EN 319 522-2 **[6]**, **I01** **I05** EN 319 532-4 **[4]**, Clause C.3.4, Table C.18, h) and i), eIDAS TS SAML Attribute Profile	For any ERDS evidence issued under **REM-Policy-IT**, when applicable: First **CC**=the Country Code of the user Second **CC**= the Country Code of the pertinent service provider EU Member State **userid**: recommended to use the sha256 of user@domain (in hex uppercase format). Example: `ES/IT/B792...3DD66DA` `ES` for a Spanish user `IT` for an Italian REMSP `B792...3DD66DA` is the sha256 in uppercase of the user's email. This element is provided by the pertinent service: S-REMS for the sender and R-REMS for the recipient respectively, according to the semantic of the ERDS evidence components **I01** and **I05**.
PP10	CSIIssueDateTime	EN 319 532-4 **[4]**, Clause C.2.3.4.1, Table C.6, item c.3.1.8 sub-item vi.	*Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*
PP11	CSINextUpdate	EN 319 532-4 **[4]**, Clause C.2.3.4.1, Table C.6, item c.3.1.8 sub-item vii.	*Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*
PP12	Timeout for transient errors	EN 319 532-4 **[4]**, Clause D.4.4	*0,5h/1 800 seconds* *The recovery of the transient error is tried each 30 min for 8 times (see PP15 below) before to consider of the transient error as a "permanent error" (that is after 4h).* *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*
PP13	Relay-snd-dsp-wait timeout	EN 319 532-4 **[4]**, Clause D.4.4	24h/86 400 seconds - [Relaying and **s**ending **disp**atch wait time]  *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*
PP14	Relay-rcv-ra-wait timeout	EN 319 532-4 **[4]**, Clause D.4.4	24h/86 400 seconds - [Relay and receiving **r**elay **a**nswer (accept/reject) receipt wait time (*after SMTP Relay operation succesfully completed*)]  *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*

PP15	Cycle-number so that persistent errors or temporary conditions causing abandon or delay in sending messages attempts lead to a final behaviour	EN 319 532-4 **[4]**, Clause D.4.4	*8 cycles* *The recovery of the transient error is tried each 30 min for 8 times (see PP12 above) before to consider the transient error as a "permanent error" (that is after 4h).*  *Note that, inside the **REM-Policy-IT**, this mechanism can be used to manage the temporary SMTP errors (e.g., 4.y.z).* *Note also that this parameter is subject to the current Authority and security practices (see § 2.6.1)*
PP16	Number of historical elements for SIPointersToOtherMetadata	EN 319 532-4 **[4]**, Clause D.3	*Note that this parameter is subject to the current Authority and security practices (see § 2.6.1)*
PP17	<tns:CSISchemeInformationURI> <tl:URI xml:lang="en">… </tl:URI> <tl:URI xml:lang="it">… </tl:URI> </tns:CSISchemeInformationURI>	EN 319 532-4 **[4]**, Clause C.2.3.4.1, Table C.6, item c.3.1.8 sub-item iv.	The following URIs reference the same informational content, even if it may be in different language: _https://www.agid.gov.it/REM/en/platforms/qualified-electronic-registered-delivery-services https://www.agid.gov.it/REM/it/piattaforme/servizi-elettronici-di-recapito-certificato-qualificato *Note that these parameters are subject to the current Authority and security practices (see § 2.6.1)*
PP18	CSISchemePolicyCommunityRules	EN 319 532-4 **[4]**, Clause C.2.3.5, Table C.14 b), Clause C.3.4, Table C.18 f), Clause C.2.3.4.1, Table C.6, item c.3.1.8 sub-item iv.	URIs where is published the REMID policy: <tl:URI xml:lang="en">http://uri.etsi.org/19532/v1#/REMbaseline</tl:URI> <tl:URI xml:lang="en">https://eidas.agid.gov.it/REM/rem-policy-it</tl:URI> *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1). These URIs, representing the "master copy" of the policy, have the same values of **REM-ApplicablePolicy** (see next item PP19)*
PP19	**REM-ApplicablePolicy**	EN 319 522-2 **[6]**, **MD05** EN 319 532-3 **[3]**, Table 2	This parameter used inside the **REM-Policy-IT** is composed by the following two values: **REM-ApplicablePolicy**: http://uri.etsi.org/19532/v1#/REMbaseline **REM-ApplicablePolicy**: https://eidas.agid.gov.it/REM/rem-policy-it The two aforementioned URIs have to be specified in REM messages even for interactions from/to **non-ERDS** systems (**TUC2** e **TUC3** cases in **Table 1**). The **REM baseline** leaves open this possibility (first URI) and the **REM-Policy-IT** (second URI) specify the implementation details about it. *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1). Here, these URIs have the same values of **CSISchemePolicyCommunityRules** (see previous item PP18)*

PP20	**EvidenceIssuerPolicyID**	EN 319 522-2 **[6]**, **R01** EN 319 532-4 **[4]**, Clause C.3.4 Table C.18, f), Clause C.4.5.x, Table C.22 d), Table C.23 d), Table C.24 d), Table C.25 d)	URIs where is published the REMID policy Composed of two values: <tns:EvidenceIssuerPolicyID> <PolicyID>http://uri.etsi.org/19532/v1#/REMbaseline</PolicyID> <PolicyID>https://eidas.agid.gov.it/REM/rem-policy-it#evidence-issuer-policy</PolicyID> </tns:EvidenceIssuerPolicyID> The two aforementioned URIs have to be specified issuing ERDS evidence even for interactions from/to **non-ERDS** systems (**TUC2** e **TUC3** cases in **Table 1**). The **REM baseline** leaves open this possibility (first URI) and the **REM-Policy-IT** (second URI) specify the implementation details about it. *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1)*
PP21	**TL**: DistributionPoints CSI: CSIPointerToTL	ETSI TS 119 612 Clause 5.3.16 EN 319 532-4 **[4]**, Clause C.2.3.4.1, Table C.6, item c.3.1.8 sub-item v.	The same URI for the following two pointers (one of TL and one of CSI): **TL**: <DistributionPoints> <URI>https://eidas.agid.gov.it/TL/TSL-IT.xml</URI> </DistributionPoints> **CSI**: <tns:CSIPointerToTL>https://eidas.agid.gov.it/TL/TSL-IT.xml</tns:CSIPointerToTL> *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1)*
PP22	*SignatureMethod* and *SignatureTimeStamp* of CapabilityAndSecurityInformation XMLs digital signatures	EN 319 532-4 **[4]**, Clause C.2.3.4.1, Table C.6, c.3.1.11 Clause D.2.2	The same digital signature and time-stamp requirements defined for ERDS evidence at row **PP7** used also for the signature of CapabilityAndSecurityInformation XML (except for the issuer if the digital certificate that in this case is different, in fact it represents the REMID authority and this reflects, as an example on the subject of the digital certificate, amongst others). *See § 2.3.2.4 for more details.* *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1)*

PP23	**SenderDetails/AssuranceLevelsDetails** (LoA hereinafter) element of ERDS evidence.	EN 319 522-2 **[6]**, **I10** Table 13, NOTE (b)	The ***sender's*** *identity assurance level detail* **I10** ERDS evidence component is mandatory present for the whole ERDS evidence set of the **REM baseline** except for the **ReceivedFromNonERDS** evidence where it shall be absent. The recipient's LoA shall be always absent. See **Figure 37** for a full example. When present its parameters are: <AssuranceLevelsDetails> … <AssuranceLevel>http://eidas.europa.eu/LoA/substantial</AssuranceLevel> <PolicyID>https://eidas.agid.gov.it/REM/rem-policy-it#assurance-level-policy</PolicyID> … <AuthenticationMethod>https://eidas.agid.gov.it/REM/rem-policy-it#authentication-method</AuthenticationMethod>… … </AssuranceLevelsDetails>
	REM-RecipientAssuranceLevel header of REM message	EN 319 522-2 **[6]**, **MD04** Table 5	The **REM-RecipientAssuranceLevel** header is not in **REM baseline;** it is even more not used in the **REM-Policy-IT** or in delivery from/to **non-ERDS** systems events. Anyway, in case of its presence, values different from the following URI can be ignored: http://eidas.europa.eu/LoA/substantial *See § 2.4.2.14 for more details on LoA and on the rationales defining the level to "substantial".*

PP24	**EventReasons /** **REM-ReasonIdentifier**	EN 319 522-2 **[6]**, **G04** EN 319 532-4 **[4]**, Clause C.3.4 Table C.18, d) Clause C.4.5.x, Table C.22 a), h) Table C.23 a), h) Table C.24 a), h) Table C.25 a), h) Table C.27/G04 EN 319 532-4 **[4]**, Clause 5.4.1 Table 7 item b)	URI and details composing the event reason during the ERDS evidence issuing: First sub-element: <Code> with a uri from the 3rd column of **Table 15** Second sub-element: <Details> with the code from the 2nd column of **Table 15** Third sub-element: <Details> with reason message taken from the 2nd columns from Table 7 to Table 12 of EN 319 522-2 **[6]**, Clause 8.3.3, in correspondence with the second elements (RA01, RA02, ... etc, set as primary <Details> element). See also the descriptions after **Table 15** for <Details> reason messages of new code *RF51* defined inside the **REM-Policy-IT**. Other <Details> components could be added, where necessary, after the two prescribed elements according to EN 319 532-4 **[4]**, Clause C.3.4 Table C.18 item d) sub-item III (see below in red). Example: <tns:EventReasons> <tns:EventReason> <Code>http://uri.etsi.org/19522/EventReason/**MessageAccepted**</Code> <Details>**RA01**</Details> <Details>Message accepted</Details> <Details>[...] optional rows with text, if any, with further details [...]</Details> <Details>[...] ... [...]</Details> </tns:EventReason> </tns:EventReasons> Note: The cardinality of "EventReasons" element in EN 319 532-4 [4], Table C.27/G04, and EN 319 522-2 [6], Table 13/G04 refers to the ERDS evidence external "container" element. Whereas, the cardinality of G04 component in Table 3 and Table 5 of the present document refers to the inner ".../EventReason/Code" ".../EventReason/Details" sub-elements. In any case, **for any ERDS evidence issued inside REM-Policy-IT**, the cardinality of each sub-element is that in Table 3 and Table 5 after the '|' separator. *Note that every one of the optional additional free texts - that could be used after the two canonical "<Details>" components and their cardinality - are subject to the current best and security practices. Therefore, they could be, to some extent, delimited and/or further updated during the time (see § 2.6.1).* Different values (and cardinalities different from that above) for <Details> optional elements are accepted during validation/verification of ERDS evidence issued under other policies. For any REM message issued under the REM-Policy-IT, the **REM-ReasonIdentifier** header is set according to EN 319 532-4 [4], Clause 5.4.1 Table 7 item d) (row N° 4), by replicating the same URI of the ".../EventReason/Code" ERDS evidence element seen above.

PP25	**EvidenceIssuerDetails** **ExternalERDSDetails**	EN 319 522-2 **[6]**, **R02** **M05** EN 319 532-4 **[4]**, Clause C.3.4 Table C.18, g), q)	Legal name of the **issuer** (for **EvidenceIssuerDetails**) or **counterpart** (for **ExternalERDSDetails**) **service provider** used during emission: the same name which is used in formal legal registrations declared by the REMSP in the TSPName (English "en" distinguished part) of the Trusted List. **TL fragment example**: <TSPName> <Name xml:lang="en">S-REMS *provider*</Name> </TSPName> **ERDS evidence fragment example**: <tns:EvidenceIssuerDetails> <tns:Identity> <saml:Attribute FriendlyName="LegalName" Name="http://eidas.europa.eu/attributes/legalperson/LegalName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"> <saml:AttributeValue type="eidas:LegalNameType">S-REMS *provider*</saml:AttributeValue> </saml:Attribute> </tns:Identity> </tns:EvidenceIssuerDetails> It is recommended to use the same name also in the CN of the Subject of the digital certificate signing REM messages and ERDS evidence XMLs, to facilitate additional automatic matching checks.
PP26	Relay-rcv-ca-wait	EN 319 532-4 **[4]**, Clause C.4.5.3 Table C.25 item a) sub-item l; and Clause D.1.3; and Clause D.4.4 Relay-rcv-ca-wait timeout, EXAMPLE 5 and relevant NOTE.	24h/86 400 seconds - [Relay and receiving **c**onsignment **a**nswer (success/failure) receipt wait time (*after RelayAcceptance operation succesfully received*)]  S-REMS was unable to receive a ContentConsignment or ContentConsignmentFailure REMS receipt response from R-REMS within a given time period). Once such timeout is achieved, S-REMS has to close the transaction towards the sender (so it is inside the **REM-Policy-IT**) with a specific REMS receipt: a REM **ContentConsignmentFailure** with code ***RD03 - S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP*** *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*

2.3.2 Funzionalità comportamenti e formati | Functionalities behaviours and formats

2.3.2.1 Adozione 4-corner model base | Basic 4-corner model adoption

Il modello operativo adottato nella **REM-Policy-IT** è in primo luogo quello canonico della **REM baseline** rappresentato dal 4-corner model semplice **senza** opzioni quali multihop, re-imbustamenti del REM dispatch etc. (si vedano i punti D di pag. 28 e F di pag. 31 del § 4.3.1 del documento base). I flussi ed eventi previsti sono pertanto quelli illustrati nei seguenti scenari e schematizzati in **Table 1**. Di fatto, la trasmissione canonica tra utenze registrate (rappresentata come "ensured"), ed indicata come **TUC1** in **Table 1**, è quella riportata nella seguente **Figure 1** (e dalla **Figure 2** alla **Figure 5** per le condizioni di errore, rappresentate come "failing").

In aggiunta al suddetto tipo di trasmissione tra REMS, la **REM-Policy-IT** prevede dei flussi ibridi "facoltativi" **non propri della REM baseline** ma legati alla realtà locale regolata dalla **REM-Policy-IT** che consentono, quando previsti dal **REMSP**, un eventuale dialogo con servizi non-REM (indicati come **TUC2** e **TUC3** in **Table 1** ed illustrate nelle **Figure 6** e **Figure 8** del § 2.4.2.1).

The operational model used in **REM-Policy-IT** is primarily that of the canonical **REM baseline** one represented by the simple 4-corner model **without** options like multihop, re-enveloping of the REM dispatch etc. (see points D at pag. 28 and F at pag. 31 of § 4.3.1 of the basic document). The flows and the intended events are therefore those illustrated in the following scenarios and summarized in **Table 1**. Actually, the canonical transmission between registered users (represented as "ensured"), and referred as **TUC1** in **Table 1**, is shown in the following **Figure 1** (and from **Figure 2** to **Figure 5** for the error conditions, represented as "failing").

Along with the aforementioned transmission type between REMS, the **REM-Policy-IT** foresees two hybrid "optional" flows **don't exactly inside the REM baseline** but related to the local reality regulated by the **REM-Policy-IT** that allow, when provided by the **REMSP**, possible interactions with non-REM services (referred to as **TUC2** and **TUC3** in **Table 1** and illustrated in the **Figure 6** and **Figure 8** of § 2.4.2.1).

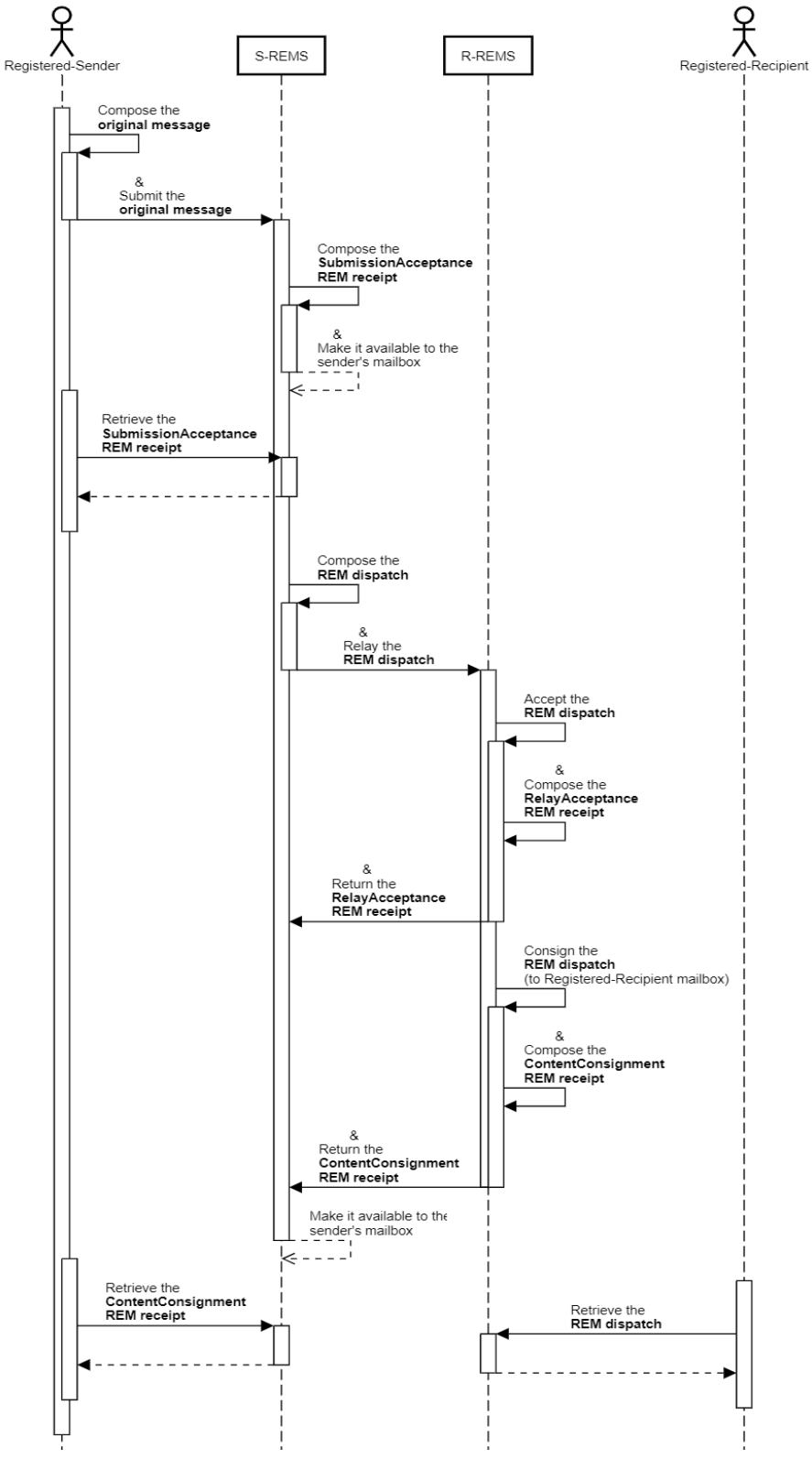


Figure 1 – 4-Corner model: Intra-REM "canonical/ensured" flow between registered users (TUC1)

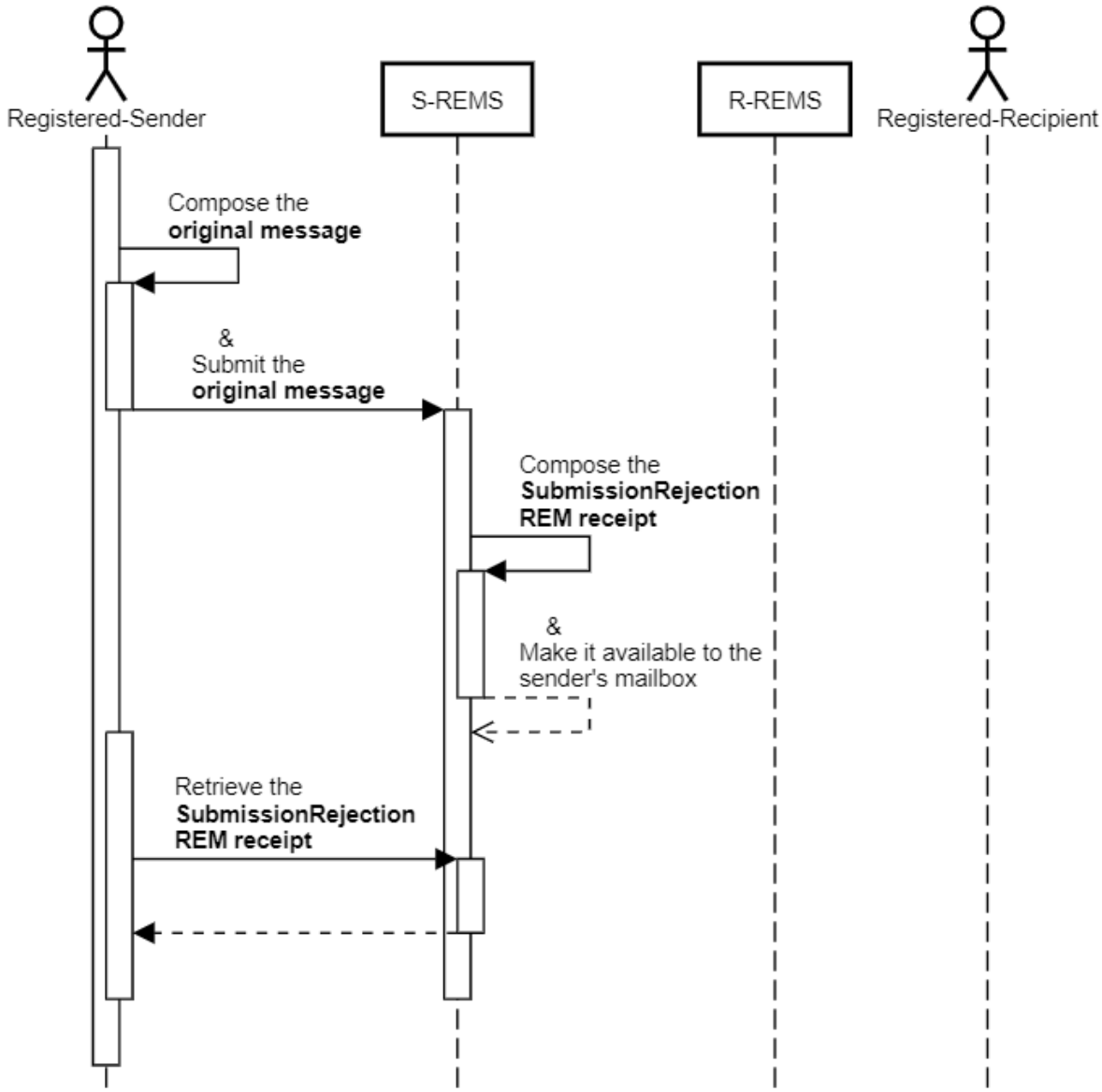


Figure 2 – 4-Corner model: Intra-REM "canonical/failing" flow – SubmissionRejection (TUC1)

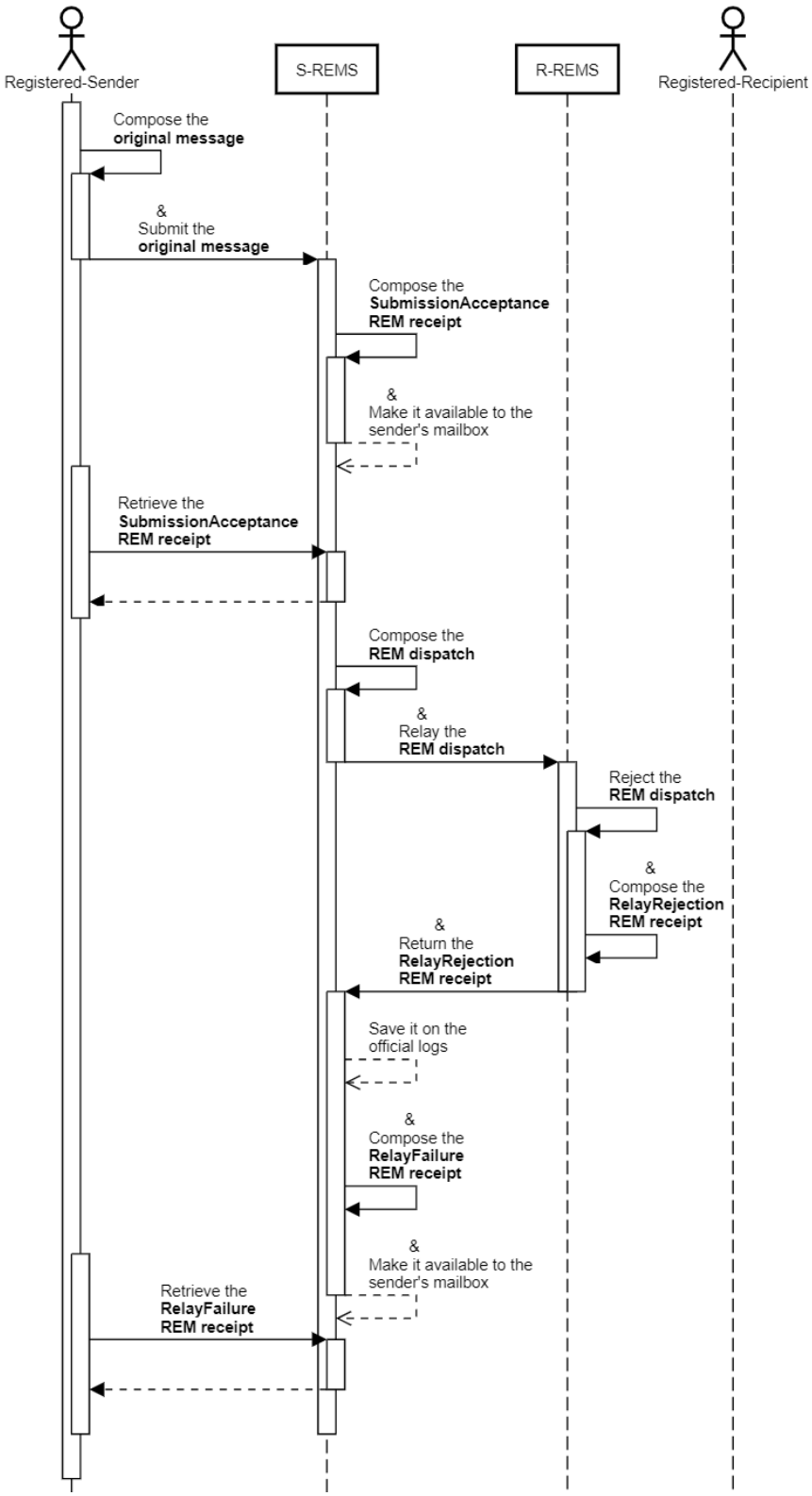


Figure 3 – 4-Corner model: Intra-REM "canonical/failing" flow – RelayRejection & Failure (TUC1)

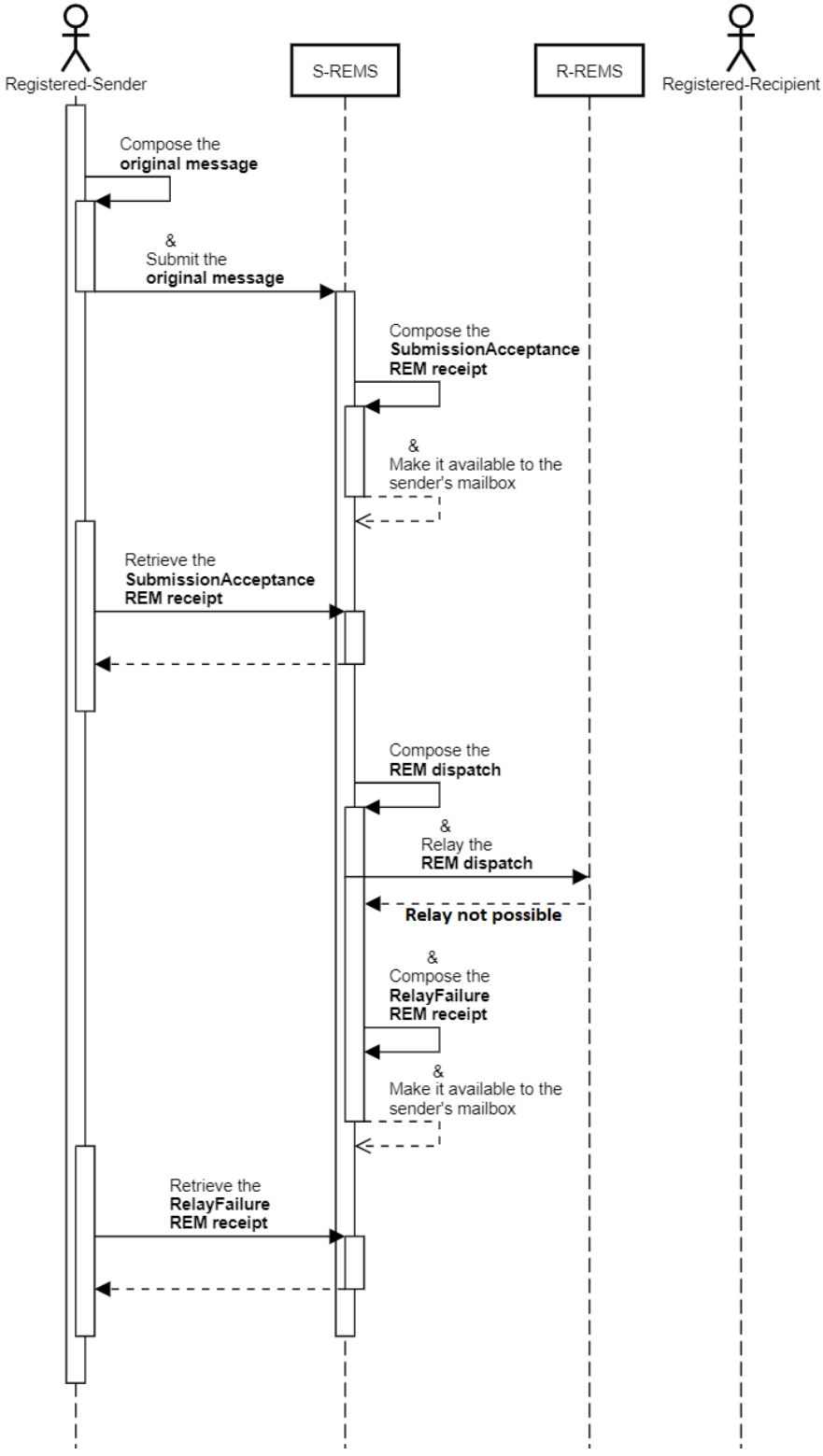


Figure 4 – 4-Corner model: Intra-REM "canonical/failing" flow – RelayFailure (TUC1)

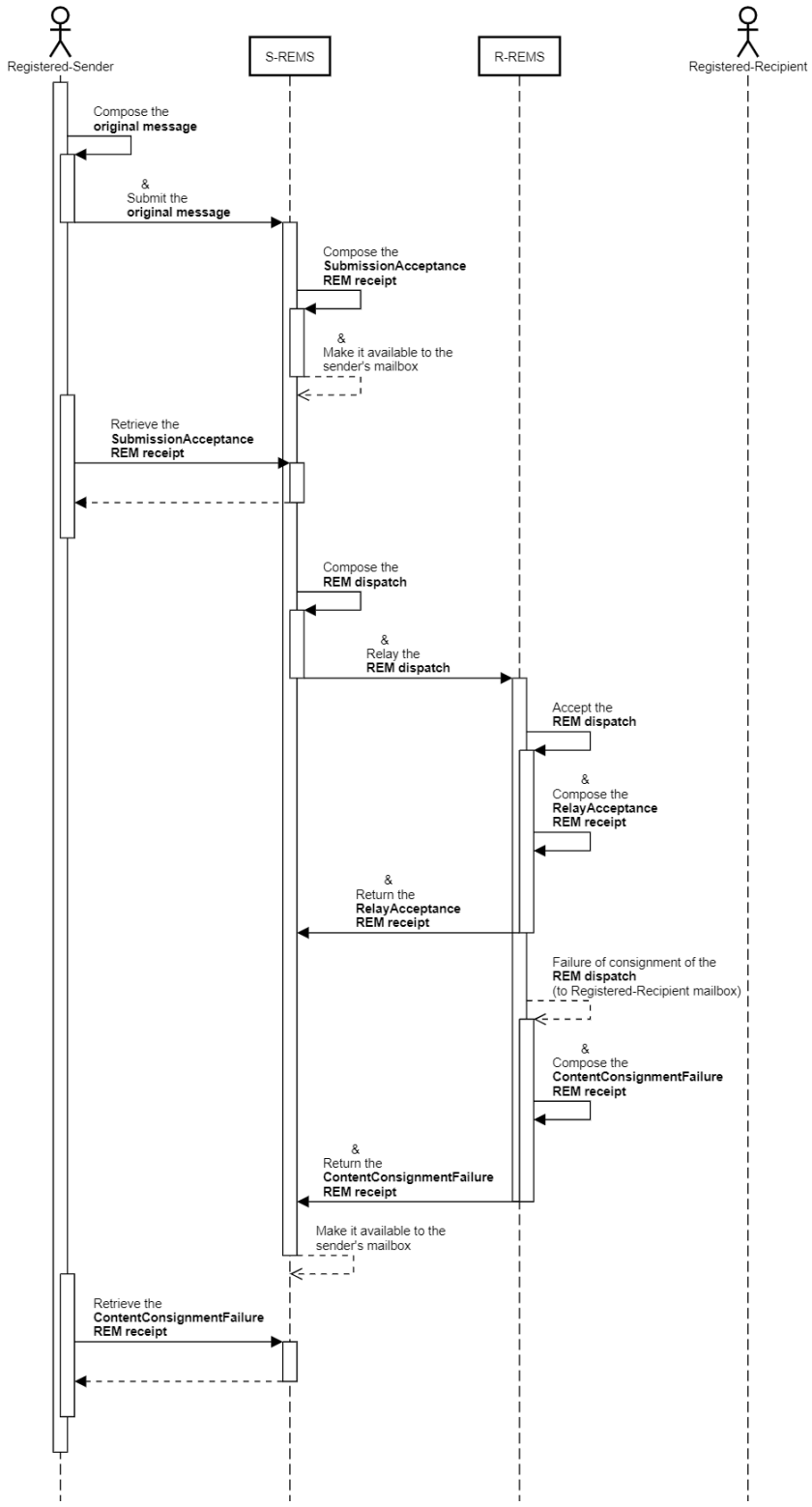


Figure 5 – 4-Corner model: Intra-REM "canonical/failing" flow – ContentConsignmentFailure (TUC1)

Caso particolare R-REMS=S-REMS: una semplificazione agli schemi precedentemente riportati è rappresentata dall'operazione di "relay" quando i REMSP mittente e ricevente coincidono. Così come stabilito in EN 319 522-2 **[6]** (dove è chiaramente indicato: <<*ERDS* ***Relay interface*** *(ERDS RI): interface that supports ERD message relay between* ***different*** *electronic registered delivery services*>>) le operazioni di relay devono essere effettuate solo quando i provider REM mittente e ricevente sono differenti. Ne consegue che, per le comunicazioni tra mittenti e destinatari registrati presso lo stesso provider, la trasmissione che inizia con l'evento di **SubmissionAcceptance** si chiude direttamente con l'evento **ContentConsignment** (in caso di successo) o **ContentConsignmentFailure** (in caso di errore). Pertanto, l'eventualità di utente-ricevente inesistente è gestita, in questo caso, con una **ContentConsignmentFailure**(**RD21**) come indicato in EN 319 532-4 **[4]**, Clause C.4.5.3 Table C.25 item i) e NOTE 2.

In **Table 3** sono riportati gli eventi, le evidenze e i messaggi previsti come obbligatori all'interno della REM baseline (intestazione in grigio tabella), i *component*

Particular case R-REMS=S-REMS: a simplification in respect to the schemes above is represented by the "relay" operation when sender and recipient's REMSP are the same. As set out in EN 319 522-2 **[6]** (where is expressly stated: <<*ERDS* ***Relay interface*** *(ERDS RI): interface that supports ERD message relay between* ***different*** *electronic registered delivery services*>>) the relay operations must take place only when the sender and recipient's REMS are different. It follows that, for the communications between senders and recipients registered to the same provider, the transmission starting with the **SubmissionAcceptance** directly closes with either **ContentConsignment** (in case of success) or **ContentConsignmentFailure** (in case of error) event. Therefore, the eventuality of inexistent recipient-user is managed, in this case, with a **ContentConsignmentFailure**(**RD21**) as per EN 319 532-4 **[4]**, Clause C.4.5.3 Table C.25 item i) and NOTE 2.

Table 3 outlines the events, the evidence types and the messages foreseen as mandatory inside the REM baseline (grey header of the table), the ERDS evidence

delle ERDS evidence, gli header e metadati dei REM message (distribuiti nella prima colonna della tabella), e la "cardinalità" prevista in corrispondenza di ogni incrocio (ogni cella della tabella). Questa è rappresentata da un valore secco oppure sotto forma di range di valori. Quando previsto, la cardinalità è ulteriormente declinata in due valori separati dal simbolo '|': quella prevista nella **REM baseline** a sinistra di tale simbolo, e quella raccomandata per tutti gli oggetti (REM messages, ERDS evidence) **emessi** da REMSP aderenti alla **REM-Policy-IT**, a destra dello stesso in accordo alle disposizioni del presente documento. Fare riferimento al § 2.9.2 in merito alle tolleranze da applicare rispetto a REM message provenienti da policy differenti alla **REM-Policy-IT**.

components, the headers and metadata of REM messages (distributed in the first column of the table), and the prescribed "cardinality" at each intersection (any table cell). This is represented by a unique value or in the form of a range of values. In some case, the cardinality is further inflected in two values separated by the '|' symbol: that prescribed in the **REM baseline** on the left, and the cardinality recommended for all the objects (REM messages, ERDS evidence) issued by REMSP belonging to the **REM-Policy-IT**, on the right of such symbol, according to the prescriptions of the present document. Refer to § 2.9.2 regarding the tolerance to apply in respect to REM messages coming from policies different from **REM-Policy-IT**.

Table 3 – Mandatory components for messages/events in REM baseline

Summary table for components, headers, events, flows. Sources: Table 1, Table 13 EN 319 522-1 [5], Table 1 & Figure 1..5 present document										
REM Message types / ERDS evidence events (*) / Operation ID / Type of transmission / Flow illustration		REM SubmissionAcceptance/ SubmissionAcceptance MME1/TUC1/Figure 1	REM dispatch / SubmissionAcceptance MME3/TUC1/Figure 1	REM SubmissionRejection / SubmissionRejection MME2/TUC1/Figure 2	REM RelayAcceptance / RelayAcceptance MME4/TUC1/Figure 1	REM RelayRejection / RelayRejection MME5/TUC1/Figure 3	REM RelayFailure / RelayFailure MME6/TUC1/Figure 3-Figure 4	REM ContentConsignment / ContentConsignment MME7/TUC1/Figure 1	REM ContentConsignmentFailure / ContentConsignmentFailure MME8/TUC1/Figure 5	Implementations
Code	**ERDS evidence component**	**Presence constraints**								
G01	**EvidenceIdentifier**	1		1	1	1	1	1	1	I-G01
G02	**Evidence(version="EN319522v1.1.1")**	1		1	1	1	1	1	1	I-G02
G03	**ERDSEventId**	1		1	1	1	1	1	1	I-G03
G04	**EventReasons/EventReason/Code** **EventReasons/EventReason/Details** (***)	1 2		1..N|1 2..N|2..M	1 2	1..N|1 2..N|2..M	1..N|1 2..N|2..M	1 2	1..N|1 2..N|2..M	I-G04
G05	**EventTime**	1		1	1	1	1	1	1	I-G05
R01	**EvidenceIssuerPolicyID/PolicyID**	1..N|2		1..N|2	1..N|2	1..N|2	1..N|2	1..N|2	1..N|2	I-R01
R02	**EvidenceIssuerDetails**	1		1	1	1	1	1	1	I-R02
R03	**Signature**	1		1	1	1	1	1	1	I-R03
I01	**SenderDetails/Identity**	0..1|1		0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	I-I01
I02	**SenderDetails/Identifier**	1		1	1	1	1	1	1	I-I02
I05	**RecipientDetails/Identity**	0..N|0		0..N|0	0..N|1..N	0..N|1..N	0..N|1..N	0..N|1..N	0..N|1..N	I-I05
I06	**RecipientDetails/Identifier**	1..N		1..N	1..N	1..N	1..N	1..N	1..N	I-I06
I09	**EvidenceRefersToRecipient**	0		0	0	0	0	1	1	I-I09
I10	**SenderDetails/AssuranceLevelsDetails**	1		1	1	1	1	1	1	I-I10
I12	**RecipientDetails/AssuranceLevelsDetails**	0		0	0	0	0	0	0	I-I12
M01	**MessageIdentifier**	1		1	1	1	1	1	1	I-M01
M02	**UserContentInfo/**AppLayerIdentifier, DigestMethod, DigestValue	1		1	1	1	1	1	1	I-M02
M03	**SubmissionTime**	1		1	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	I-M03
M04	**ForwardedToExternalSystem**	0		0	0	0	0	0	0	I-M04b
M05	**ExternalERDSDetails**	0		0	1	1	1	0	0	I-M05
E01	**Extensions/GeneralEvidenceInfo/Subject**	0..1|1		0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	I-E01s
	Extensions/GeneralEvidenceInfo/**UntrustedPathToRecipient**	0..N		0..N	0..N	0..N	0..N	0..N	0..N	I-E01u
	Extensions/RelayEvidenceInfo/**RelayEvidenceRefersTo**	0		0	0..N	0..N	0..N	0	0	I-E01r
Code	**REM message header/metadata component**	**Presence constraints. Sources: Table 5 EN 319 522-1 [5] (other than the sources on the head above)**								
MD01	**REM-MetadataVersion**	1	1	1	1	1	1	1	1	I-MD01
MD02	**REM-RelayDate**	0	0..1|0	0..1|0	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	I-MD02
MD03	**REM-ExpirationDate**	0	0	0	0	0	0	0	0	I-MD03
MD04	**REM-RecipientAssuranceLevel**	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	I-MD04
MD05	**REM-ApplicablePolicy**	0..N|2	0..N|2	0..N|2	0..N|2	0..N|2	0..N|2	0..N|2	0..N|2	I-MD05
MD06	**REM-ModeOfConsignment**	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	I-MD06
MD07	**REM-ScheduledDelivery**	0	0	0	0	0	0	0	0	I-MD07
MD08	**REM-MD08**	1	1	1	1	1	1	1	1	I-MD08
MD09	**Reply-To**	0..1|0	1	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	0..1|0	I-MD09
MD10	**To**	1	1	1	1	1	1	1	1	I-MD10
MD11	**Message-ID**	1	1	1	1	1	1	1	1	I-MD11
MD12	**In-Reply-To**	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	I-MD12
MD13	**REM-MessageType**	1	1	1	1	1	1	1	1	I-MD13
MD14	**REM-DigestAlgorithm**	1	1	1	1	1	1	1	1	I-MD14
MD14	**REM-DigestValue**	1	1	1	1	1	1	1	1	I-MD14
MD14	**Subject**	1	1	1	1	1	1	1	1	I-MD14s
MD14	**REM-UAMessageIdentifier**	1	1	1	1	1	1	1	1	I-MD14
N/A	**From**	1	1	1	1	1	1	1	1	AP4
N/A	**Bcc**	0	0	0	0	0	0	0	0	I-FBCC
N/A	**Signature**	1	1	1	1	1	1	1	1	PP6
N/A	**REM-EventIdentifier** (as G03)	1	1	1	1	1	1	1	1	I-RM-G03
N/A	**REM-Evidence-ID** (as G01)	1	1	1	1	1	1	1	1	I-RM-G01
N/A	**REM-ReasonIdentifier** (as G04/**Code**)	0..1	0..1	0..1	0..1	0..1	0..1	0..1	0..1	I-RM-G04
N/A	**REM-Section-Type**	2	3	2	2	2	2	2|3 (**)	2	I-HFC-ST

(*) These mandatory events of REM baseline are extended in Table 5 and will be used in: OLR8 – Table 7, Table 8, Table 14, Table 15.

(**) The cardinality 3 in this specific case is to manage, inside REM-Policy-IT, the *original message* attached as an extension of the REM ContentConsignment receipt (see the details at § 2.4.2.5).

(***) The cardinality |2..M, initially suggested to be 2..3, is subject to the current best practice (see § 2.6.1) as illustrated in row PP24 of Table 2.

Operations:

MME1: Submission/Acceptance of original message	**(incorporates a SubmissionAcceptance ERDS evidence)**
MME2: Submission/Rejection of original message	**(incorporates a SubmissionRejection ERDS evidence)**
MME3: Relay/Successful of REM dispatch	**(incorporates a SubmissionAcceptance ERDS evidence)**
MME4: Relay/Acceptance of REM dispatch	**(incorporates a RelayAcceptance ERDS evidence)**
MME5: Relay/Rejection of REM dispatch	**(incorporates a RelayRejection ERDS evidence)**
MME6: Relay/Failure of REM dispatch	**(incorporates a RelayFailure ERDS evidence)**
MME7: Content/Consignment of REM dispatch	**(incorporates a ContentConsignment ERDS evidence)**
MME8: Content/ConsignmentFailure of REM dispatch	**(incorporates a ContentConsignmentFailure ERDS evidence)**

Implementations:

The following prescriptions apply to <u>any</u> ERDS evidence and REM message <u>issued</u> inside REM-Policy-IT taking care to support and ensure interoperability with any ERDS evidence and REM message coming from outside the border or from other policies compliant with REM baseline defined in EN 319 532-4 [4] Annexes B, C and D. Refer to § 2.9.2 regarding the tolerance to apply in respect to REM messages coming from policies different from REM-Policy-IT.

NOTE: to have a more compact text, in many cases the prescriptions below refer to both interaction forms: within REM baseline (cardinality and main references in **Table 3**) and from/to non-ERDS (cardinality and main references in **Table 5**). The leverage of cross-references helps in an easy jump from one point to another (*see **Note** at page 6 of the present annex for details*).

I-G01 / I-RM-G01: Row PP3e of Table 2.

I-G02: The value of the version attribute of the Evidence root element is set according to EN 319 532-4 [4], Clause C.3.4 Table C.18, item b).

I-G03 / I-RM-G03: ERDSEventId element is the URI identifying the event triggering the issuance of the evidence, as defined for G03 *component* in EN 319 522-2 [6], Clause 8.2.3, and it is replicated to the REM-EventIdentifier header of any REM message. The official URIs for these events are the subset specifically selected for the REM baseline (starting from the generic set in Table 2 of EN 319 522-3 [7]) according to EN 319 532-4 [4], Clause 5.4.5.1 Table C.27 and C.28, Clause 5.4.1 Table 7, b) (row N° 2). Such selection is augmented in the REM-Policy-IT for the ordinary e-mail management (i.e., with the events F.1, F.2, F.3). Table 15 and the § 2.5.1 provide the full set of events/URIs foreseen for REM-Policy-IT and further clarification notes (whereas see § 2.4.2.2, for details on the ordinary email management).

I-G04 / I-RM-G04: Row PP24 of Table 2.

I-G05 The value of the EventTime element is an UTC set according to EN 319 532-4 [4], Clause C.3.4 Table C.18 item e), Clause C.4.5.1 Table C.22 item b), Clause C.4.5.2 Table C.23 item b), Table C.24 item b), Clause C.4.5.3 Table C.25 item b). Similarly, it is equally set during interactions from/to non-ERDS systems (see component G05 at Table 5 below).

I-R01: Row PP20 of Table 2.

I-R02 / I-M05: Row PP25 of Table 2.

I-R03: Row PP7 of Table 2.

I-I01: Row PP9 of Table 2. For any ERDS evidence issued inside REM-Policy-IT this component shall be present. In case of messages coming from outside the border or from other policies, this component shall be as per EN 319 522-2

[6], Clause 8.2.10: *<<The source of the information for this component is the S-ERDS. R-ERDS ... shall use sender's identity attributes as provided in an available ERDS evidence or ERDS relay metadata generated by S-ERDS if they want to include this component in the ERDS evidence they produce. If such information is not available to the R-ERDS ..., this component shall not be present in the evidence they produce>>.*

I-I02: The value of the SenderDetails/Identifier element is the sender's email according to EN 319 532-4 [4], Clause C.3.4 Table C.18 item h) sub-item II.

I-I05: Row PP9 of Table 2. For RelayAcceptance, RelayRejection, RelayFailure (but only when it is due to a previous/related RelayRejection), ContentConsignment, ContentConsignmentFailure, ReceivedFromNonERDS ERDS evidence XMLs, issued inside REM-Policy-IT, this component shall be present. In the other cases this component shall be as per EN 319 522-2 [6], Clause 8.2.14: *<<The source of the information for this component is the R-ERDS. S-ERDS ... shall use recipient's identity attributes as provided in an available ERDS evidence generated by R-ERDS if they want to include this component in the ERDS evidence they produce. If such an evidence is not available to the R-ERDS ..., this component shall not be present in the ERDS evidence they produce>>.*

NOTE: for this reason, the cardinality 1..N is prescribed only when such information can be really available to the ERDS evidence issuer.

I-I06: The value of any RecipientDetails/Identifier multivalue element is a recipient's email according to EN 319 532-4 [4], Clause C.3.4 Table C.18 item i) sub-item II.

I-I09: The value of any EvidenceRefersToRecipient multivalue element is a ordinal number, identifying a recipient, according to EN 319 532-4 [4], Clause C.3.4 Table C.18 item o), Clause C.4.5.3 Table C.25 item i) sub-item II.

I-MD01: The value of REM-MetadataVersion header is `EN31953203V010201` as per EN 319 532-3 [3] Table 2.

I-MD02: The value of any REM-RelayDate is an UTC set according to EN 319 532-3 [3] Table 2.

EXAMPLE: `REM-RelayDate: Wed, 01 Dec 2021 21:04:40 +0000 (UTC)`

I-MD03: The REM-ExpirationDate header is absent according to EN 319 532-4 [4], Clause C.4.5.4 Table C.26 item MD03.

I-I10 / I-MD04: This component is composed by:

```
SenderDetails/AssuranceLevelsDetails/GlobalAssuranceLevel/AssuranceLevel
SenderDetails/AssuranceLevelsDetails/GlobalAssuranceLevel/PolicyID
SenderDetails/AssuranceLevelsDetails/AuthenticationDetails/AuthenticationTime
SenderDetails/AssuranceLevelsDetails/AuthenticationDetails/AuthenticationMethod
```

See row PP23 of Table 2 and § 2.4.2.14 for more details.`

I-I12 / I-MD04: Row PP23 of Table 2 and § 2.4.2.14 for more details.

I-MD05: Row PP19 of Table 2.

I-MD06: In the context of the REM baseline and even more inside REM-Policy-IT the REM-ModeOfConsignment header is not used since the REM messages is consigned according to the REM baseline capabilities defined in EN 319 532-4 [4], Table C.8 item c.3.3.7, as per the semantic of MD06 metadata. Anyway, in case of its presence, values different from the following URI can be ignored:

```
http://uri.etsi.org/19522/v1#/consignment/basic
```

I-MD07: The REM-ScheduledDelivery header is absent according to EN 319 532-4 [4], Clause C.4.5.4 Table C.26 item MD07.

I-MD08: The REM-MD08 header is mandatory (as per EN 319 522-2 [6], Clause 6.1 Table 5) and it is defined as per EN 319 532-3 [3], Clause 6.2.1). Its value is a replica of the full email address present in the `From:` header of the original message.

EXAMPLE: `REM-MD08: Sender name <sender@sender-own-domain-only-for-test.it>`

I-MD09: The header "Reply-To" is defined as per EN 319 532-3 [3] Table 3 and the prescription 'AA' at § 4.3.4 of the main document. In case of the ReceivedFromNonERDS event, this header has the same cardinality of the REM dispatch.

I-MD10: The header "To" is defined as per EN 319 532-3 [3] Table 3 and prescription 'X' at § 4.3.4 of the main document.

I-MD12: The header "In-Reply-To" is defined as per EN 319 532-3 [3] Table 3 and prescription 'EE' at § 4.3.4 of the main document.

I-MD13: The value of REM-MessageType element is either the first or second of the following URIs, for REM dispatch or REMS receipt respectively, as per EN 319 522-3 [7], Clause 4.3.5 and according to EN 319 532-3 [3] Table 2, EN 319 532-4 [4], Clause 5.4.1 Table 7, a) (row N° 1).

```
REM-MessageType: http://uri.etsi.org/19522/v1#/ERDMessageType/dispatch
REM-MessageType: http://uri.etsi.org/19522/v1#/ERDMessageType/receipt
```

I-M01 / I-MD11: Row PP3m of Table 2 and § 2.4.2.3 for more details.

I-M02 / I-MD14: Rows PP1 (for DigestMethod and REM-DigestAlgorithm), PP2 (for DigestValue and REM-DigestValue) and PP3o (for AppLayerIdentifier and REM-UAMessageIdentifier) of Table 2.

I-M03: According to the REM baseline prescriptions defined in EN 319 532-4 [4], Table C.18 , j (row N° 12).

NOTE: In case of ReceivedFromNonERDS event (see Table 5 below), this component is not present (since such time reference is generated outside the ERDS system).

I-M04b: This element is not used for the event of the REM baseline. See I-M04 implementation guidance, at Table 5 below, for the usage of *ForwardedToExternalSystem* during interactions from/to non-ERDS systems.

I-MD14s: (Row PP4 of Table 2), Table 14 and § 2.4.2.10 for more details.

I-E01s: The extension *E01* element is always present at least regarding the *Extensions/GeneralEvidenceInfo/Subject* sub-element. It is an – untouched – replica of the *original message* Subject header, according to the REM baseline prescriptions defined in EN 319 532-4 [4], Clause C.3.2.1 Table C.15 item b) sub-item i. (row N° 2). It is used, inside the REM-Policy-IT, for any REM message issued and also during the interactions from/to non-ERDS systems.

I-E01u: For the REM messages issued under the REM-Policy-IT, the *Extensions/GeneralEvidenceInfo/UntrustedPathToRecipient* sub-element is used according to the REM baseline prescriptions defined in EN 319 532-4 [4], Clause C.3.2.1 Table C.15 item b) sub-item ii. (row N° 2).

I-E01r: For the REM messages issued under the REM-Policy-IT, the *Extensions/RelayEvidenceInfo/RelayEvidenceRefersTo* sub-element is used according to the REM baseline prescriptions defined in EN 319 532-4 [4], Clause C.3.2.2 Table C.16 items b) (row N° 2).

I-HFC-ST: For the REM messages issued under the REM-Policy-IT, the *REM-Section-Type* header as follows.

- REM dispatch / REM ReceivedFromNonERDS:

`REM-Section-Type: rem_message/introduction`	**EN 319 532-4 [4], Clause 5.4.3.1 Table 8 item a)**
`REM-Section-Type: rem_message/original`	**EN 319 532-4 [4], Clause 5.4.4 Table 11 item a)**
`REM-Section-Type: rem_message/xml_evidence`	**EN 319 532-4 [4], Clause 5.4.6 Table 13 item a)**

- REMS receipt:

`REM-Section-Type: rem_message/introduction`	**EN 319 532-4 [4], Clause 5.4.3.1 Table 8 item a)**
`REM-Section-Type: rem_message/xml_evidence`	**EN 319 532-4 [4], Clause 5.4.6 Table 13 item a)**
`REM-Section-Type: rem_message/extension`	**EN 319 532-4 [4], Clause 5.4.5 Table 12 item a) (*)**

(*) Note that the last case (extension) is solely usable in the case of REM ContentConsignment receipts issued under the REM-Policy-IT according to § 2.4.2.5 and as illustrated in Figure 19.

I-FBCC: For the REM messages issued under the REM-Policy-IT, the *Bcc:* header is not allowed. In case of its presence in the *original message* (that represents a clear sign of the will of the sender to use it, independently of the specification of the same addressee in the RCPT TO list) the submission operation MUST be rejected issuing a REM SubmissionRejection receipt, with attached an ERDS evidence according to:

EventReason/Code: `<http://uri.etsi.org/19522/EventReason/S_ERDS_PolicyViolation>`

EventReason/Details: `<RA05>`

EventReason/Details: `<Sender's ERDS provider's policy violation>` *(text reason description obtained from EN 319 522-2 **[6]**, Clause 8.3.3.1 Table 7)*

For any component that is not listed above, refer to the example illustrated at § 2.7 to get the relevant implementation recommendation regarding any ERDS evidence and REM message issued inside REM-Policy-IT.

2.3.2.2 *Firma digitale REM message | REM message digital signature*

Firma digitale effettuata con certificato digitale del REMSP.

Formato: CAdES-B S/MIME EML.

Parametri del CAdES da specificare:

digest algorithm

signature algorithm

key length

Si veda per lo scopo la riga **PP6** della **Table 2**:

Il parametro "signature-policy-identifier" (si veda riga **PP4 Table 2**) è lasciato opzionale nel senso ampio che – indipendentemente dalla sua presenza e dal valore che assume – non ha influenza per gli scopi della REM all'interno della **REM-Policy-IT**.

Digital signature based on the digital certificate of the REMSP.

Format: CAdES-B S/MIME EML.

Parameters of CAdES to specify:

digest algorithm

signature algorithm

key length

See row **PP6** of **Table 2**:

The "signature-policy-identifier" parameter (see row **PP4 Table 2**) is left as optional in the sense that – independently of its presence and from its value – it is not influent for the REMS inside **REM-Policy-IT**.

2.3.2.3 *Firma digitale e time-stamp ERDS evidence | ERDS evidence digital signature and time-stamp*

Firma digitale effettuata con certificato digitale del REMSP.

Formato XAdES-B-T XML.

Parametri del XAdES da specificare:

digest algorithm

signature algorithm

key length

Si veda per lo scopo la riga PP7 della **Table 2**

Digital signature based on the digital certificate of the REMSP.

Format XAdES-B-T XML.

Parameters of XAdES to specify:

digest algorithm

signature algorithm

key length

See row PP7 of **Table 2**

2.3.2.4 Firma digitale Capability and Security Information | Capability and Security Information digital signature

Firma digitale della struttura XML della CSI effettuata dalla **REMID authority**[32] (rappresentata da **AGID**, per la **REM-Policy-IT**) al fine di garantire l'integrità di tutta la catena di Trust in ogni istante ed in generale nel tempo. Integrità che va dal certificato **TLS** fino alla struttura XML che lo contiene e si lega, dal punto di vista crittografico, all'integrità garantita per la **TL**.

File: CapabilityAndSecurityInformation.xml

Formato: XAdES-B-T XML.

Parametri del XAdES da specificare:

digest algorithm

signature algorithm

key length

Digital signature of the CSI XML structure done by the **REMID authority**[32] (represented by **AGID**, for the **REM-Policy-IT**) and to ensure the Trust chain integrity at any time and over the time. Integrity that goes from the **TLS** certificate, through the XML structure containing it, and it binds, from the cryptographic viewpoint, to the integrity ensured for the **TL**.

File: CapabilityAndSecurityInformation.xml

Format: XAdES-B-T XML.

Parameters of XAdES to specify:

digest algorithm

signature algorithm

key length

[32] La firma digitale della presente struttura XML è un requisito "semanticamente" obbligatorio della **REM baseline** in accordo a EN 319 532-4 **[4]**, Clause C.2.3.4.1 Table C.6 item c.3.1.11), da non confondere con la notazione dell'XSD che lo indica "sintatticamente" come opzionale (`<xsd:element ref="ds:Signature" minOccurs="0"/>`). Questa apparente asimmetria è una pratica comune alle varie definizioni formali (così come si può notare anche in quelle per la firma digitale della Trusted List e della ERDS evidence). Ovviamente, quella che va applicata è la prescrizione semantica.

[32] The digital signature of the present XML structure is a "semantically" mandatory requirement of the **REM baseline** according to EN 319 532-4 **[4]**, Clause C.2.3.4.1 Table C.6 item c.3.1.11), not to be confused with the XSD notation that points it as "syntactically" optional (`<xsd:element ref="ds:Signature" minOccurs="0"/>`). This apparently asymmetry is a common practice to the various formal definitions (how it can be noted in in digital signature of the Trusted List and ERDS evidence definition). Obviously, in these cases, the semantic prescription must be applied.

Si veda per lo scopo le righe **PP7** e **PP22** della **Table 2** per i parametri da utilizzare (eccetto che per il certificato digitale che è sotto la responsabilità della **REMID authority**) e l'EN 319 532-4 **[4]**, Clause C.2.3.4.1, item c.3.1.8) sub-item viii. e ix. riguardo la pubblicazione ed il mantenimento dello storico del presente XML.

See rows **PP7** and **PP22** of **Table 2** for the parameters to use (except for the digital certificate, that is under the responsibility of the **REMID authority**) and the EN 319 532-4 **[4]**, Clause C.2.3.4.1, item c.3.1.8) sub-items viii. and ix. regarding the publication and the historical preservation of the present XML.

2.4 Prescrizioni specifiche della REM-Policy-IT | REM-Policy-IT specific prescriptions

2.4.1 Parametri | Parameters

Nella seguente **Table 4** è riportata la specifica, per tutti i REM message emessi all'interno della **REM-Policy-IT**, di parametri "addizionali" rispetto a quelli previsti all'interno della **REM baseline**, e che sfruttano i gradi di libertà della stessa.

In the following **Table 4** is given the specification, for any REM message issued inside the **REM-Policy-IT**, of "additional" parameters in respect to that are envisaged inside the REM baseline, leveraging its degree of freedom.

Table 4 – Additional parameters of the REM-Policy-IT

Id	Element / Parameter	Reference	Implementation
AP1	Return-Path:	EN 319 532-3 **[3]**, Table 3	**Only for REM dispatch issued in the policy**: the same 'email address' value of *From* header of *original message* (i.e. except the 'display name' part of the email address). See also examples at § 2.7
AP2	Received:	EN 319 532-3 **[3]**, Table 3	**Only for REM dispatch**: the REM service level can optionally add some *Received* header inheriting it, in this case, from the *Received* header of *original message*. Whereas the usual SMTP behaviour is expected to be practiced by the **MTA**s for this multivalue Received header. Therefore, all the additional necessary *Received* headers provided by the protocol can be present in both REM dispatch and REMS receipts. See also examples at § 2.7

AP3	charset	EN 319 532-3 **[3]**, Table 6, 7, 10.	**For any REM message:** charset="UTF-8"
AP4	From:	EN 319 532-3 **[3]**, Table 3	**Only for REM dispatch**: It shall be in the form as for the following example: *From: "On behalf of: sender@s-rems-only-for-test.it" <rem-service@s-rems-only-for-test.it>* Where: *<rem-service@s-rems-only-for-test.it>* is the real "signer" service email address of the REMS issuer (it must be also in the **rfc822Name** of the X509v3 Subject Alternative Name extension - **SAN** - of digital certificate used for the digital signature, *see* **PP6 Table 2** *§ 2.3.1).* *"On behalf of: sender@s-rems-only-for-test.it"* is a simple text that is displayed (as display name element of the email address) by any client, giving to the user an immediate visual indication of the original sender address.
AP5	Cc:	EN 319 532-3 **[3]**, Table 3	**Only for REM dispatch**: it shall match the *Cc* header of the *original message*.

2.4.2 Funzionalità comportamenti e formati | Functionalities behaviours and formats

2.4.2.1 Adozione modello 4-corner esteso | 4-corner extended model adoption

Oltre al flusso canonico previsto dalla REM baseline, la **REM-Policy-IT** estende i flussi del 4-corner a trasmissioni ibride **OPZIONALI** da/verso sistemi esterni (non propri della REM baseline) considerati come sistemi di posta ordinaria (si vedano i punti J di pag. 34 del § 4.3.1 ed EEE di pag. 76 del § 4.3.4 del documento base). I flussi ed eventi estesi previsti sono pertanto quelli illustrati nei seguenti scenari. Di fatto, le trasmissioni estese alle **utenze** non registrate, ed indicate come **TUC2** e **TUC3** in **Table 1**, sono quelle riportate nelle seguenti **Figure 6** e **Figure 8** (e **Figure 7** riguardo una condizione di errore) e

In addition to the canonical flow of REM baseline, the **REM-Policy-IT** extends the 4-corner flows to **OPTIONAL** hybrid transmissions from/to external systems (**non** proper of the REM baseline) considered as ordinary email systems (see points J at pag. 34 of § 4.3.1 and EEE at pag. 76 of § 4.3.4 of the basic document). The flows and events considered are therefore those illustrated in the following scenarios. Indeed, the extended transmissions to non-registered users, referred to as **TUC2** and **TUC3** in **Table 1**, are those given at the following **Figure 6** and **Figure 8** (and **Figure 7** regarding an error condition) and summarized in **Table 5**. Such

schematizzate nella seguente **Table 5**. Tale tabella ha formati e contenuti analoghi a quelli della **Table 3** con la differenza che si riferisce ai tre eventi di tipo non-ERDS.

table is formatted and refers to analogues contents of those in **Table 3**, but considering that it refers instead to the three non-ERDS type events.

Table 5 – Extended components for from/to non-ERDS messages/events beyond REM baseline

Summary table for components, headers, events, flows. Sources: Table 1, Table 5, Table 13 EN 319 522-1 [5], Table 1 & Figure 6..14 present doc.					Implementations
REM Message types / ERDS evidence events (*) Operation ID / Type of transmission / Flow illustration		REM RelayToNonERDS/ RelayToNonERDS EME1 / TUC2 / Figure 6	REM RelayToNonERDSFailure / RelayToNonERDSFailure EME2 / TUC2 / Figure 7	REM ReceivedFromNonERDS / ReceivedFromNonERDS EME3 / TUC3 / Figure 8	
Code	ERDS evidence element	Presence constraints			
G01	EvidenceIdentifier	1	1	1	I-G01
G02	Evidence(version="EN319522v1.1.1")	1	1	1	I-G02
G03	ERDSEventId	1	1	1	I-G03
G04	EventReasons/EventReason/Code EventReasons/EventReason/Details (**)	0..1|1 0..N|2..M	0..N|1 0..N|2..M	0..1|1 0..N|2..M	I-G04
G05	EventTime	1	1	1	I-G05
R01	EvidenceIssuerPolicyID	1..N|2	1..N|2	1..N|2	I-R01
R02	EvidenceIssuerDetails	1	1	1	I-R02
R03	Signature	1	1	1	I-R03
I01	SenderDetails/Identity	0..1|1	0..1|1	0..1|0	I-I01
I02	SenderDetails/Identifier	1	1	1	I-I02
I05	RecipientDetails/Identity	0..N|0	0..N|0	0..N|1..N	I-I05
I06	RecipientDetails/Identifier	1..N	1..N	1..N	I-I06
I09	EvidenceRefersToRecipient	0	0	0	I-I09
I10	Sender/AssuranceLevelsDetails	1	1	0	I-I10
I12	Recipient/AssuranceLevelsDetails	0	0	0	I-I12
M01	MessageIdentifier	1	1	1	I-MD11
M02	UserContentInfo/AppLayerIdentifier, DigestMethod, DigestValue	1	1	1	I-M02
M03	SubmissionTime	0..1|1	0..1|1	0..1|0	I-M03
M04	ForwardedToExternalSystem	1	1	1	I-M04
M05	ExternalERDSDetails	0	0	0	I-M05
E01	Extensions/GeneralEvidenceInfo/Subject	0..1|1	0..1|1	0..1|1	I-E01s
	Extensions/GeneralEvidenceInfo/UntrustedPathToRecipient	1..N	1..N	0	I-E01u
	Extensions/RelayEvidenceInfo/RelayEvidenceRefersTo	0..N	0..N	0	I-E01r
Code	REM message header/metadata component	Presence constraints. Sources: Table 5 EN 319 522-1 [5] (other than the sources on the head above)			
MD01	REM-MetadataVersion	1	1	1	I-MD01
MD02	REM-RelayDate	0..1|1	0..1|1	0..1|1	I-MD02
MD03	REM-ExpirationDate	0	0	0	I-MD03
MD04	REM-RecipientAssuranceLevel	0..1|0	0..1|0	0..1|0	I-MD04
MD05	REM-ApplicablePolicy	0..N|2	0..N|2	0..N|2	I-MD05
MD06	REM-ModeOfConsignment	0..1|0	0..1|0	0..1|0	I-MD06
MD07	REM-ScheduledDelivery	0	0	0	I-MD07
MD08	REM-MD08	1	1	1	I-MD08
MD09	Reply-To	0..1|0	0..1|0	1	I-MD09
MD10	To	1	1	1	I-MD10
MD11	Message-ID	1	1	1	I-MD11
MD12	In-Reply-To	0..1	0..1	0..1	I-MD12
MD13	REM-MessageType	1	1	1	I-MD13
MD14	REM-DigestAlgorithm	1	1	1	I-MD14
MD14	REM-DigestValue	1	1	1	I-MD14
MD14	Subject	1	1	1	I-MD14s
MD14	REM-UAMessageIdentifier	1	1	1	I-MD14
N/A	From	1	1	1	AP4
N/A	Bcc	0	0	0	I-FBCC
N/A	Signature	1	1	1	PP6
N/A	REM-EventIdentifier (as G03)	1	1	1	I-RM-G03
N/A	REM-Evidence-ID (as G01)	1	1	1	I-RM-G01
N/A	REM-ReasonIdentifier (as G04/Code)	0..1|1	0..1|1	0..1|1	I-RM-G04
N/A	REM-Section-Type	2	2	3	I-HFC-ST

(*) These events extend the basic ones defined in Table 3 and will be used in: OLR8 – Table 7, Table 8, Table 14, Table 15.
(**) The cardinality |2..M, initially suggested to be 2..3, is subject to the current best practice (see § 2.6.1) as illustrated in row PP24 of Table 2.

Operations:

EME1: Relay/Outflow of REM dispatch	**(incorporates a RelayToNonERDS ERDS evidence)**
EME2: Relay/Outflow Rejection or failure of REM dispatch	**(incorporates a RelayToNonERDSFailure ERDS evidence)**
EME3: Relay/Inflow of non-ERDS content	**(incorporates a ReceivedFromNonERDS ERDS evidence)**

Implementations:

The implementation of any component is according to the presence requirement of Table 5 and exactly according to the same requirements of Table 3 except the following, specific for the three events managed in Table 5. Refer to § 2.9.2 regarding the tolerance to apply in respect to REM messages coming from policies different from REM-Policy-IT.
NOTE: to have a more compact text, in many cases the implementation reference in **Table 5** refers to a prescription valid for both type of interaction: within REM baseline (cardinality and main references in **Table 3**) and from/**to non-ERDS (cardinality** and main references in **Table 5**). The leverage of cross-references helps in an easy jump from one point to another (*see **Note** at page 6 of the present annex for details*).

I-M04: This *component* provides a description, in plain text, of the external system (in respect to the REM baseline circuit) involved in the event. For these three types of events occurring inside the REM-Policy-IT, the ForwardedToExternalSystem element shall assume the following values:

→*[Inflow]*

***Received:* header identifying the external system that generates the ReceivedFromNonERDS event (by sending an message to a REM system), or some other element that can identify the remote system (e.g., in case of absence of the *Received:* header in the message coming from the external system).**

←*[Outflow]*

***MX record* relevant to the external system to which the REM dispatch has to be relayed, for RelayToNonERDS and RelayToNonERDSFailure events, and optionally some other element that can identify the remote system or the successful/unsuccesful completition of the transaction with it (e.g. the SMTP tracking steps or SMTP errors).**

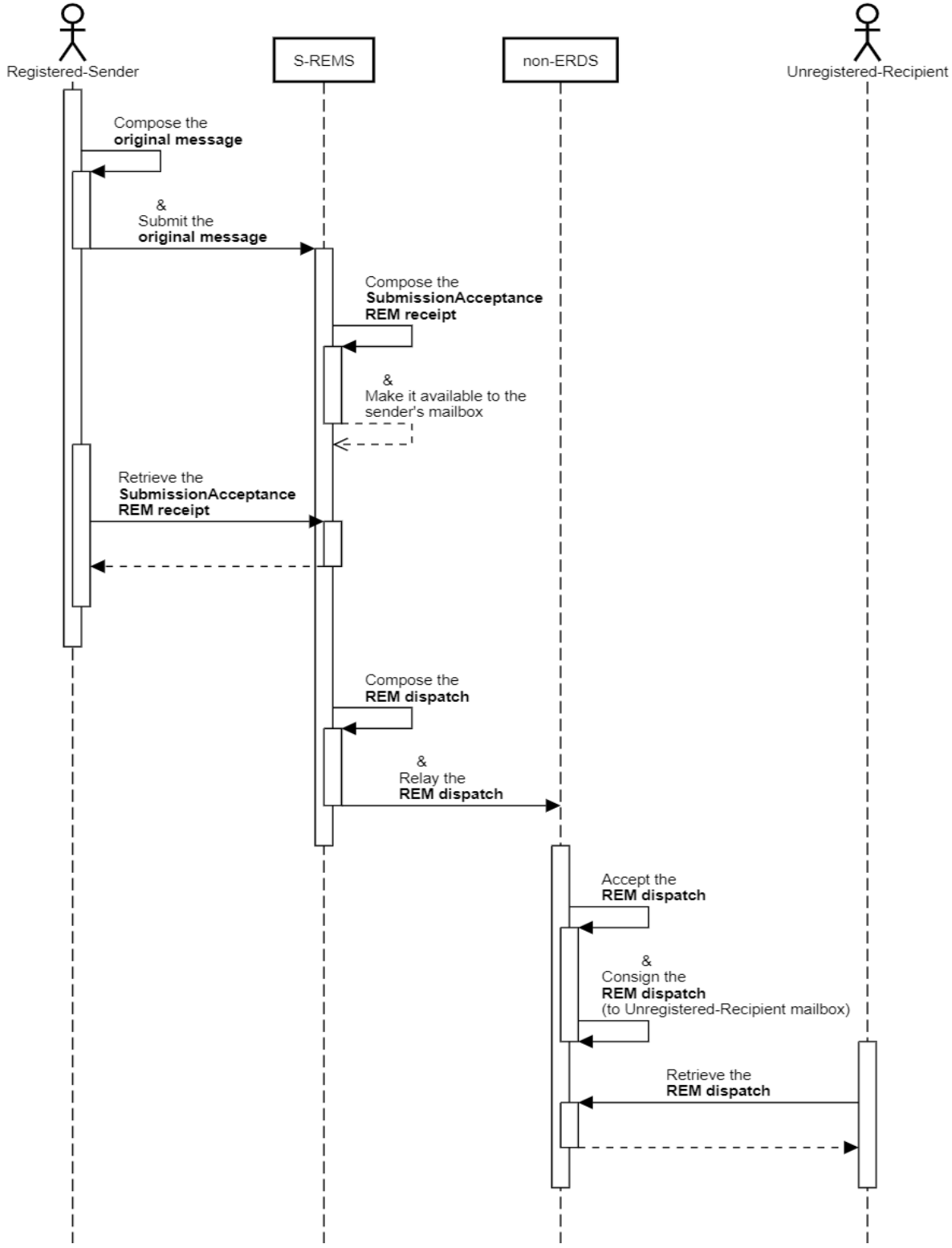


Figure 6 – 4-Corner model: Outflow from registered to unregistered users (TUC2/EME1)

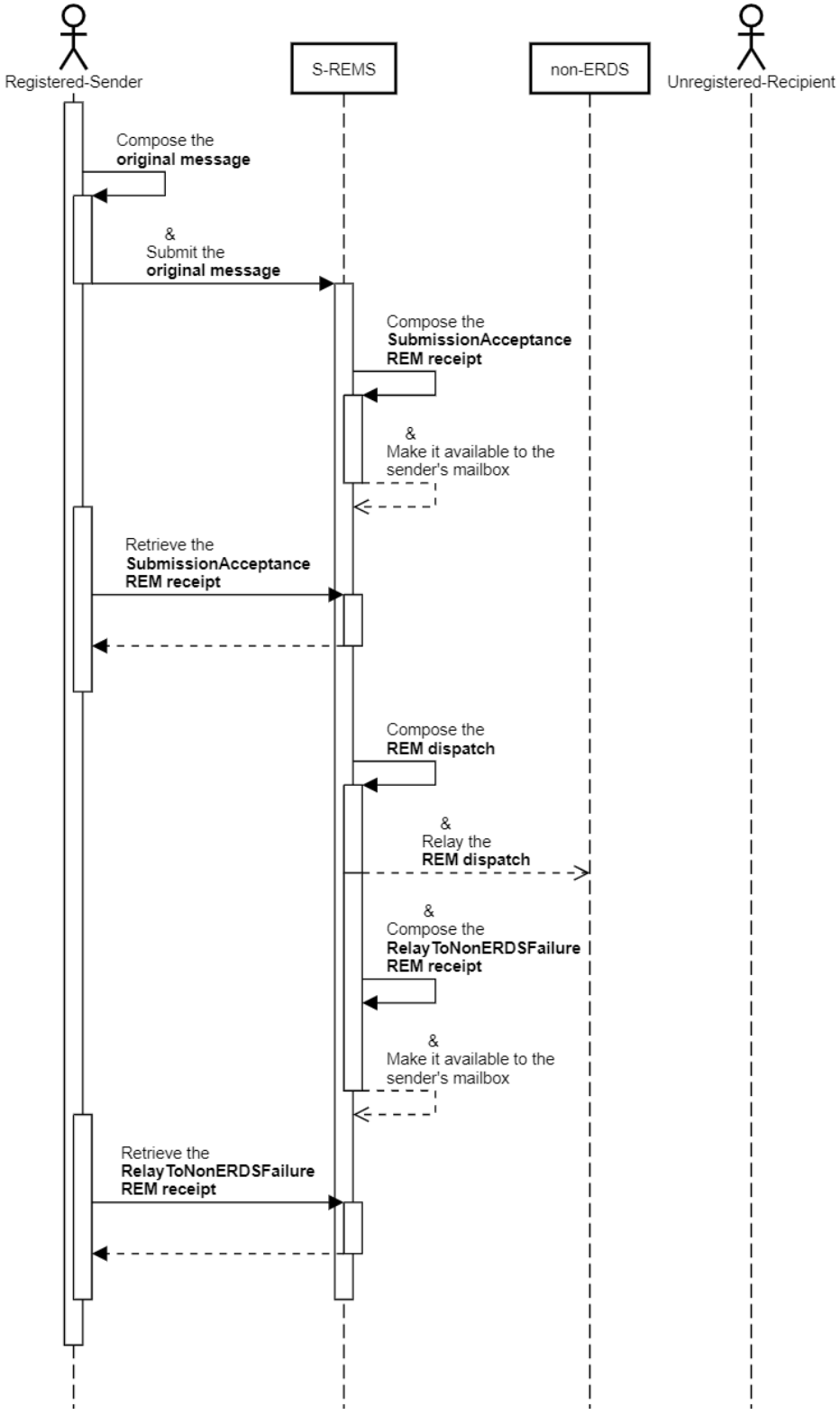


Figure 7 – 4-Corner model: Outflow from registered to unregistered users failure (TUC2/EME2)

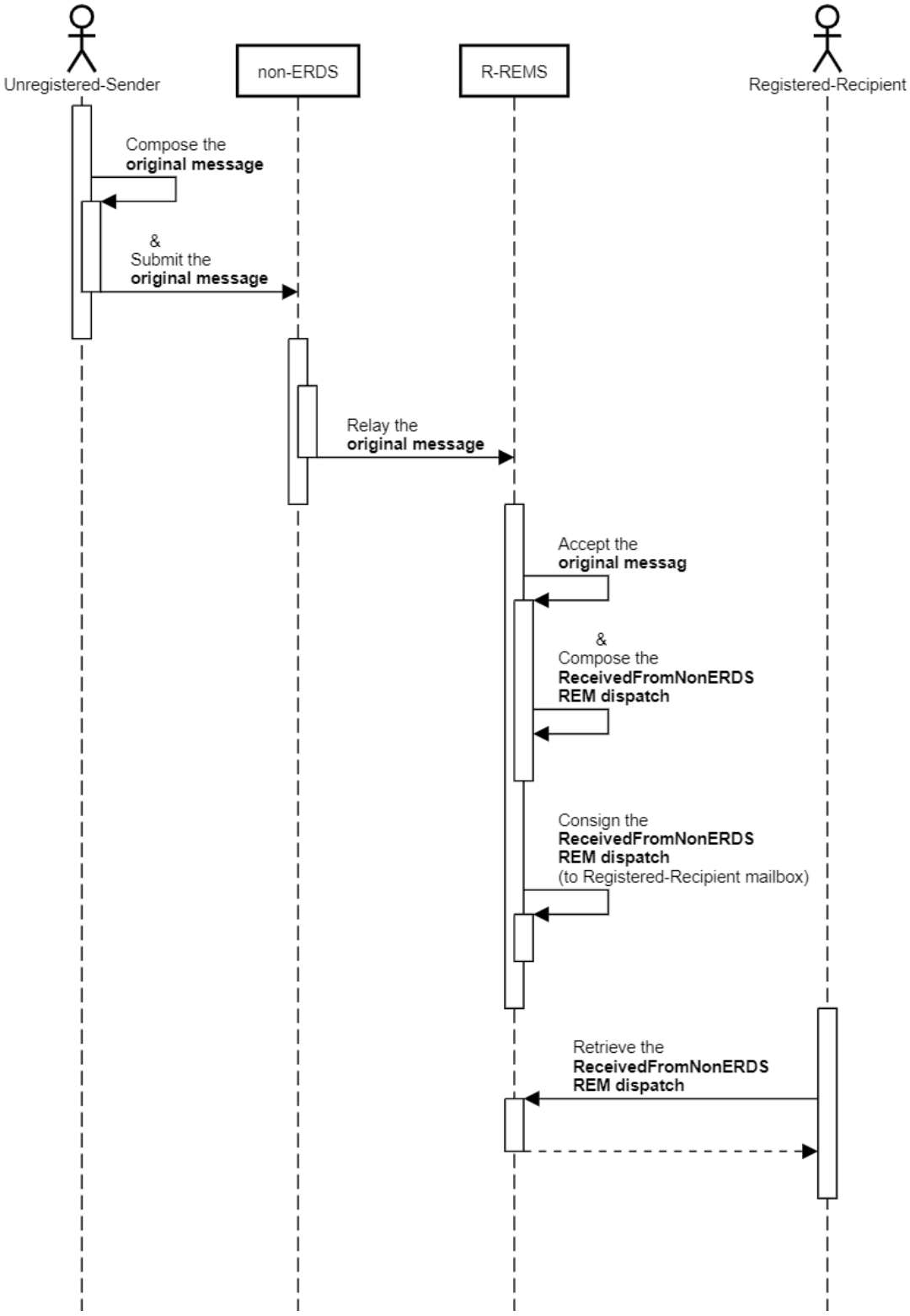


Figure 8 – 4-Corner model: Inflow from unregistered to registered users (TUC3/EME3)

Si noti che le suddette **Figure 6**, **Figure 7** e **Figure 8** intendono fornire la parte più generale dei flussi, mentre le particolarità (es. i sotto flussi opzionali e/o gli errori gestiti) sono riportati in **Figure 9**, **Figure 10**, **Figure 11**, **Figure 12**, **Figure 13** e **Figure 14**.

In riferimento agli scenari canonici di **Figure 1** e **Figure 5**, la colonna ERSD event status in Table 1 dell'EN 319 522-1 **[5]**, Clause 6.1, relativamente agli eventi D.1 ContentConsignment e D.2 ContentConsignmentFailure <<*either D.1 or D2 shall take place (…)*>> prescrive che l'**R-REMS** emetta una REMS receipt o di tipo D.1 o di tipo D.2 (per quanto concerne i soli eventi previsti nella REM baseline). Ci possono comunque essere dei casi in cui ciò non avviene in un tempo prefissato. Questo caso limite, all'interno della **REM-Policy-IT** (e cioè quando l'utenza mittente è appartenente alla suddetta policy) è gestito come comportamento addizionale rispetto alla REM baseline. L'evento è tracciato, in piena trasparenza verso l'utenza, come indicato alla riga **PP26** della **Table 2** attraverso la definizione del timeout **Relay-rcv-ca-wait** e dell'emissione di una REM

Note that **Figure 6**, **Figure 7** and **Figure 8** aim to provide the more general part of the flows, whereas details (e.g., optional sub-flows and/or the managed errors) are described in **Figure 9**, **Figure 10**, **Figure 11**, **Figure 12**, **Figure 13** and **Figure 14**.

With regard to the canonical scenarios of **Figure 1** and **Figure 5**, the ERDS event status column in Table 1 of EN 319 522-1 **[5]**, Clause 6.1, relevant to the D.1 ContentConsignment e D.2 ContentConsignmentFailure events, prescribes that <<*either D.1 or D2 shall take place (…)*>>. This means that **R-REMS** will issue either a D.1 or D.2 REMS receipt (concerning only events foreseen in the REM baseline). Anyway, there can be situations where this does not happen in a pre-defined time. This rare case is managed as an exception inside the **REM-Policy-IT** in respect to the REM baseline (the sender users belong to the aforementioned policy). The event is tracked in a transparently way with regards to the sender. As outlined in row **PP26** of **Table 2** the **Relay-rcv-ca-wait** is defined and the issue of a REM **ContentConsignmentFailure** with the following specific event is foreseen for this particular case:

ContentConsignmentFailure con evento specifico per questo caso: ***RD03 - S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP***.	***RD03 - S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP***.

2.4.2.2 Gestione posta ordinaria | Ordinary e-mail Outflow/Inflow operation

In questa sezione è analizzata la modalità delle trasmissioni ibride tra utenze di sistemi aderenti alla REM baseline (riferita per semplicità anche come **REM** da qui in avanti) da/per utenze di sistemi esterni (si vedano i casi TUC2 e TUC3 in **Table 1** a pag. 16 relativi a comunicazioni da/verso **utenze** non registrate, e le **Figure 6** e **Figure 8** relative a servizi esterni alla REM baseline)[33].

Il **REMID policy** definito dalla **REM-Policy-IT** prevede che ogni **REMSP** abbia possibilità di scelta se consentire o meno la ricezione/invio da/verso sistemi esterni alla REM baseline (anche in modalità selettiva solo *in* o solo *out*).

Conseguentemente a tale scelta, ogni REMSP può consentire o meno alle proprie **utenze**, attraverso opzioni contrattuali o di

This section analyses the case of hybrid transmissions between users of system adhering to the REM baseline (called also, simply **REM** hereinafter) from/to users of external systems (see case TUC2 and TUC3 in **Table 1** at pag. 16 relevant to communications from/to non-registered users, and the **Figure 6** and **Figure 8** relevant to services don't adhering to the REM baseline)[33].

In the **REMID policy**, defined through the **REM-Policy-IT**, every **REMSP** can choose if the receiving/sending from/to systems external to the REM baseline is allowed (also in a selective way only *in* or only *out*).

Consequently to such choice, any REMSP can consent or not its users to further tune, through contractual or self-care

[33] A complemento, gli eventi e le relative ERDS evidence riguardo la ricezione/trasmissione di contenuti da/verso sistemi non-REM (chiamati anche in generale non-ERDS) sono mappati nella Table 1 dell'EN 319 522-1 **[5]**.

[33] As supplement, the events and the related ERDS evidence about the reception/transmission of contents from/to non-REM systems (aka non-ERDS in the general case) are mapped in the Table 1 of EN 319 522-1 **[5]**.

self-care, di effettuare le proprie scelte rispetto alle capacità di ricezione e invio di messaggi da/verso mittenti/destinatari esterni a sistemi aderenti alla REM baseline (es. posta ordinaria cosiddetta non-ERDS).

Esistono quindi di fatto, per una **utenza** REM, le possibilità schematizzate in **Table 6**.

choices, regards the capabilities of receive/send messages from/to external sender/recipients, in respect the REM baseline system (e.g. the so called non-ERDS ordinary e-mail).

Therefore, for a REM user, there are the possibilities summarized in **Table 6**.

Table 6 – Extended messages Inflow/Outflow beyond REM baseline

Id	From REMS to non-ERDS		From non-ERDS to REMS		Operation ID on Table 5	REMS Event or SMTP negative response	Example
	S-REMSP	SenderUser	R-REMSP	RecipientUser			
EMF1	**Y**	**Y**	*	*	EME1	**RelayToNonERDS**	**Figure 9**
					EME2	**RelayToNonERDSFailure**	**Figure 7, Figure 11** or **Figure 12**
EMF2	*	*	**Y**	**Y**	EME3	**ReceivedFromNonERDS**	**Figure 8**, **Figure 13**
EMF3	**Y**	**N**	*	*	EME2	**RelayToNonERDSFailure**	**Figure 10**
EMF4	*	*	**Y**	**N**		Reject or Discard	**Figure 14**
EMF5	**N**	**No choice**	*	*	EME2	**RelayToNonERDSFailure**	**Figure 10**
EMF6	*	*	**N**	**No choice**		Reject or Discard	**Figure 14**

Note:

SenderUser is a user registered to the sender-side REM service provider (S-REMSP) enabled to send REM messages.

RecipientUser is a user registered to the recipient-side REM service provider (R-REMSP) enabled to receive REM messages.

Y in a cell means that, for a *specific flow* the corresponding *entity* has the *option* to **send** or **receive** ordinary email set to **enabled** (e.g., for the *specific* flow = '**From REMS** to ordinary email', the *entity* = '**S-REMSP**' has **enabled** by '**Y**' the *option* allowing to **send** ordinary email).

N in a cell means that, for a specific flow the corresponding entity has the option to **send** or **receive** ordinary email set to **disabled** (e.g., for the *specific* flow = 'From ordinary email **to REMS**', the *entity* = '**RecipientUser**' has **disabled** by '**N**' the *option* to **receive** ordinary email).

No choice in a cell means that, for a specific flow the corresponding user cannot do any choice: the '**N**' at service provider level states that the option to **send** or **receive** ordinary email is set to **disabled** at service level. And this prevails on any user's choice (e.g., for the *specific* flow = '**From REMS** to ordinary email', the *entity* = '**S-REMSP**' has **disabled** by '**N**' the *option* allowing to **send** ordinary email, and **SenderUser** has **No choice** on it).

***** in a cell means that this case is **not appliable** or relevant for such specific combination of flow/service provider/user.

Le colonne 2 e 3 della **Table 6** indicano la configurazione dell'opzione di invio verso sistemi non-ERDS rispettivamente a livello di REMSP e a livello utente mittente (SenderUser). Le colonne 4 e 5 indicano la configurazione dell'opzione di ricezione da

The columns nr. 2 and 3 of **Table 6** denote the configuration, at REMSP and at user (SenderUser) level respectively, allowing to send REM messages towards non-ERDS systems. The columns nr. 4 and 5 denote the configuration, at REMSP and at

sistemi non-ERDS rispettivamente a livello di REMSP e a livello utente (RecipientUser). La configurazione a livello di servizio (**S-REMS** o **R-REMS**) prevale su quella utente. Le altre colonne indicano, in funzione delle suddette configurazioni, come si inquadra il servizio rispetto alla tipologia di flusso, agli eventi e termina con l'ultima colonna dove sono rappresentati i relativi esempi.

Seguono una serie di figure che identificano ogni possibile caso d'uso. Si veda anche punto "J Event related to connections " del § 4.3.1, pag. 34 del documento base.

user level (RecipientUser) respectively, allowing to receive messages from non-ERDS systems. The service level configuration (**S-REMS** or **R-REMS**) prevails on that at user's level. The other columns denote, according to the aforementioned configurations, how the service falls in respect to the flow type, the events and ending with the last column where are represented the relevant examples.

Follows a variety of figures identifying the main possible use cases. See also the point "J Event related to connections " of § 4.3.1, pag. 34 of the basic document.

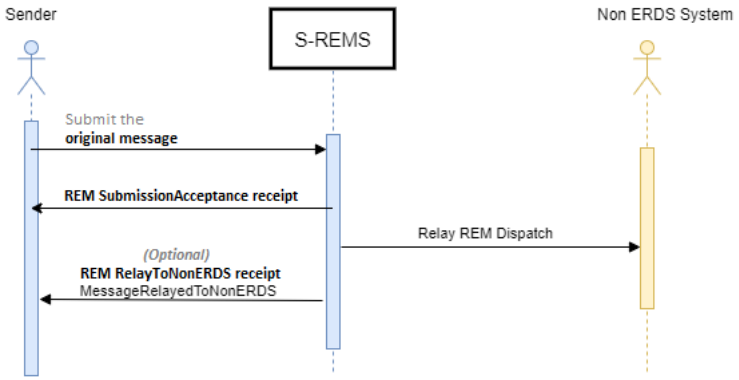


Figure 9 – Successful Outflow sending to non-ERDS systems (EMF1/EME1)

In **Figure 9** è schematizzato il caso in cui il relay verso un sistema non-ERDS ha successo (si veda la **Table 6** alla riga identificata dagli Id **EMF1/EME1**).

The case of successful relay towards a non-ERDS system is outlined in **Figure 9** (see **Table 6** at the row identified by **EMF1/EME1** Ids).

La REMS receipt contenente la **RelayToNonERDS** o la **RelayToNonERDSFailure** ERDS evidence è opzionale. L'utente mittente può richiedere l'opzione (ad es. attraverso le proprie preferenze o quando possibile/comodo anche direttamente nell'Header dell'*original message*) con uno od entrambi i seguenti MIME header. Il default è equivalente a "non-required" quando non altrimenti specificato dall'utente. Quando un tale header è presente nell'*original message* il REMSP aderente alla **REM-Policy-IT** replicherà tale header anche nel REM dispatch.

REM-RelayToNonERDS: evidence-required

REM-RelayToNonERDSFailure: evidence-required

In caso l'opzione sia richiesta, l'S-REMS restituirà al mittente una REM **RelayToNonERDS** receipt per ogni relay andata a buon fine verso un Service Provider destinatario (non appartenente al circuito REM baseline) individuato dal suo **MX record**: ognuna cumulativa per i destinatari di competenza del rispettivo Service Provider di destinazione.

La REMS receipt containing the **RelayToNonERDS** or the **RelayToNonERDSFailure** ERDS evidence is optional. The sender can require such option (e.g. through his/her own preferences or if possible/comfortable even directly inside the Header of the *original message*) with one or both the following MIME header components. The default is "non-required" when it is not specified by the user. The REMSP adhering to **REM-Policy-IT** will replicate such header also in the REM dispatch when it is present in the *original message*.

REM-RelayToNonERDS: evidence-required

REM-RelayToNonERDSFailure: evidence-required

In case the option is required, the S-REMS will return one REM **RelayToNonERDS** receipt for each successful relay towards a target Service Provider (non-belonging to the REM baseline circuit) detected by its **MX record**: each cumulative for the recipients belonging to the related destination Service Provider.

Nel caso di fallimento dell'operazione di relay, invece, l'S-REMS restituirà al mittente una REM **RelayToNonERDSFailure** receipt per ogni **DSN** (Delivery Status Notification bounced e-mail) proveniente dal sistema di posta elettronica ordinaria remoto (non appartenente al circuito REM baseline) che verrà allegata alla suddetta REMS receipt.

Nei casi di errore che non producono o produrranno una DSN (a titolo esemplificativo, ma non esaustivo, errori sincroni permanenti durante la relay, ad es. comandi SMTP non accettati, syntax o connection error, etc. o che comunque producono una "Permanent Negative Completion reply" durante la relay) l'S-REMS restituirà al mittente una ricevuta REM **RelayToNonERDSFailure** per ogni service provider remoto in difetto, con una descrizione dell'errore.

In tutti i casi (positivi, negativi, sincroni e asincroni) si veda anche il caso Outflow delle note implementative della componente **I-M04** della **Table 5**, che prescrive di conservare nell'ERDS evidence il valore dell' **MX record** del service provider cui era destinato l'*original message*, ed opzionalmente altre eventuali informazioni.

In the case of relay failure, instead, the S-REMS will send back to the sender one REM **RelayToNonERDSFailure** receipt for any **DSN** (Delivery Status Notification bounced e-mail) coming from the remote ordinary email system (non-belonging to the REM baseline circuit) that will be attached to the aforementioned REMS receipt.

In the error cases that don't or won't produce a DSN (by way of example, but not limited to, permanent synchronous errors during the relay, e.g. not accepted SMTP commands, syntax or connection errors, etc. or in any case they produce a "Permanent Negative Completion reply" during the relay) the S-REMS will send back to the sender a REM **RelayToNonERDSFailure** receipt for each failing remote service provider, with a description of the error.

In every case (positive, negative synchronous and asynchronous) see also the Outflow case in the implementation notes of **I-M04** components of **Table 5**. It prescribes to preserve the **MX record** value of the service provider to which the *original message* was intended), and optionally, other eventual information.

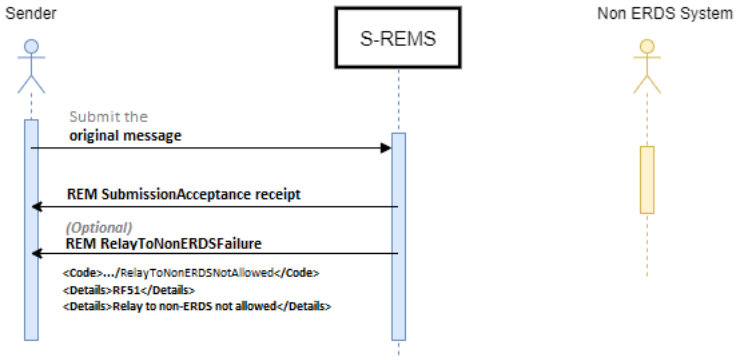


Figure 10 – Not allowed Outflow sending to non-ERDS systems (EMF3/EMF5/EME2)

In **Figure 10** è schematizzato il caso in cui il relay verso un sistema non-ERDS non è permesso a causa delle policy dell'**S-REMS** o delle preferenze utenti configurate (si vedano la prima e terza colonna della **Table 6** alle righe **EMF3** ed **EMF5**, e i codici **RF51** / **RelayToNonERDSNotAllowed** definiti in **Table 15** e nella spiegazione relativa).

The case of deny of relay towards a non-ERDS system is outlined in **Figure 10**. Its refusal is due to the **S-REMS** policy or for the configured user's preferences (see the first and third columns of **Table 6** at the rows **EMF3** and **EMF5**, and the codes **RF51** / **RelayToNonERDSNotAllowed** defined in **Table 15** and in the relevant explanation).

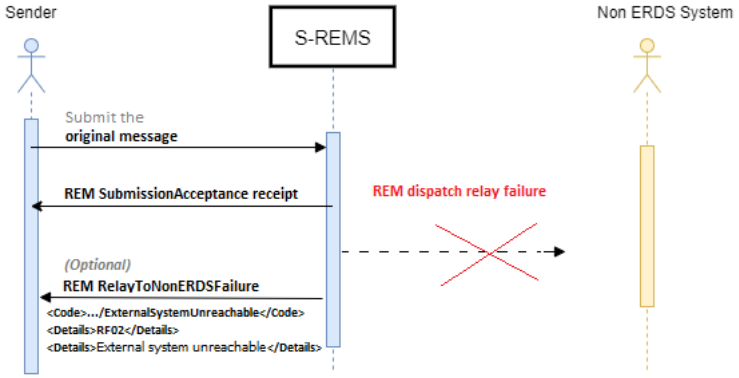


Figure 11 – Failure Outflow sending to non-ERDS systems (EMF1/EME2)

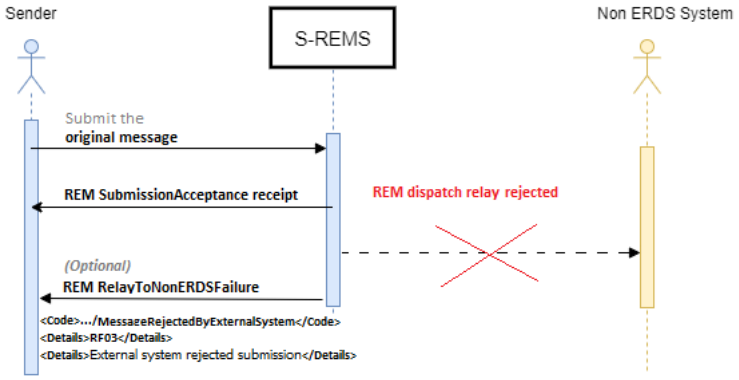


Figure 12 – Rejection Outflow sending to non-ERDS systems (EMF1/EME2)

In **Figure 11** e **Figure 12** sono illustrati due casi di relay verso un sistema non-ERDS non conclusi per due differenti cause. Questi due scenari rientrano nelle configurazioni identificate in **Table 6** alla riga **EMF1/EME2**, ed utilizzano rispettivamente i codici **RF02/ExternalSystemUnreachable** e **RF03/MessageRejectedByExternalSystem** riportati in **Table 15**.

Figure 11 e **Figure 12** outline two cases of uncompleted relay towards a non-ERDS system due to different causes. These two scenarios fall within the configurations identified in **Table 6** row **EMF1/EME2**, and use respectively the codes **RF02/ExternalSystemUnreachable** and **RF03/MessageRejectedByExternalSystem** given in **Table 15**.

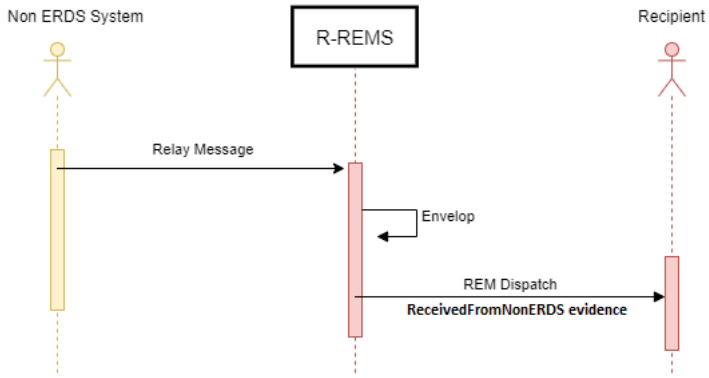


Figure 13 – Successful Inflow receiving from non-ERDS systems (EMF2/EME3)

In **Figure 13** è illustrato il caso in cui vi è un relay da un sistema non-ERDS verso un sistema REM. A seguito delle policy dell'**R-REMS** e delle preferenze utente configurate il messaggio è accettato dall'R-REMS, imbustato come REM dispatch (con allegata una ReceivedFromNonERDS evidence) e consegnato al destinatario. Questo caso rientra nella possibilità identificata alla quarta e quinta colonna (**From non-ERDS to REMS**) della **Table 6** alla riga **EMF2/EME3**, e i codici **RF04/MessageReceivedFromNonERDS** definiti in **Table 15**.

The case where a relay from a non-ERDS system to a REM system occurs is illustrated in **Figure 13**. Due to the **R-REMS** policies and to the configured recipient's preferences the message is accepted by the R-REMS, enveloped as a REM dispatch (with attached a ReceivedFromNonERDS evidence) and delivered to the recipient. This case falls in the possibility identified at the fourth and fifth columns (**From non-ERDS to REMS**) of **Table 6** at row **EMF2/EME3**, and the codes **RF04/MessageReceivedFromNonERDS** defined in **Table 15**.

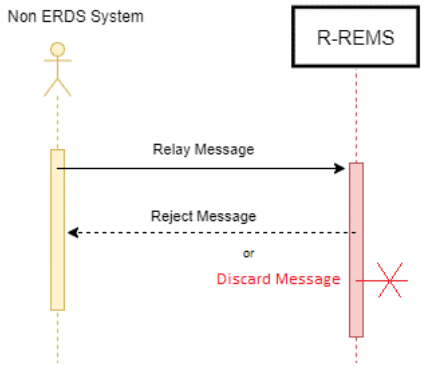


Figure 14 – Rejected/Discarded Inflow receiving from non-ERDS systems (EMF4/EMF6)

In **Figure 14** è schematizzato il caso in cui il relay da un sistema non-ERDS verso un sistema REM è inibito a causa delle policy di blocco dell'**R-REMS** o delle preferenze utente configurate. Il messaggio in ingresso è pertanto rigettato (o scartato senza alcuna

The case where a relay from a non-ERDS system to a REM system is inhibited by the **R-REMS** lock policies or by the configured recipient's preferences is illustrated in **Figure 14**. The incoming message is therefore rejected (or discarded

segnalazione, previa ovviamente chiara indicazione nel manuale operativo e/o nel contratto di servizio) dall'R-REMS. Questo caso rientra nelle possibilità identificate alla quarta e quinta colonna (**From non-ERDS to REMS**) della **Table 6** alle righe **EMF4** ed **EMF6**).

without any feedback, upon explicit and clear indication in the practice statement and/or the service agreement, obviously) by the R-REMS. This case falls in the possibility identified at the fourth and fifth columns (**From non-ERDS to REMS**) of **Table 6** at the rows **EMF4** and **EMF6**).

2.4.2.3 Impostazione Message-ID | Message-ID setting

Come riportato nel § 4.3.4 al punto D di pag. 45 e note [13] e [14], lo standard EN 319 532-3 **[3]**, Clause 4.2 prevede che il REMSP possa aggiungere o modificare, nel processo di imbustamento, alcuni header dell'*original message*. Tali modifiche devono essere limitate alle casistiche di comprovata necessità. Nel caso del MIME header **Message-ID**, l'operazione specificata nel seguito è giustificata dalla necessità di garantire il corretto funzionamento del sistema.

In particolare, è fondamentale garantire l'univocità dell'identificativo di tutti gli *original message* accettati all'interno del sistema dei REMSP, al fine di gestire la corretta tracciatura di tutti i REM message (cioè i REM dispatch e le REMS receipt) afferenti, ognuno di essi, ad un'unica transazione legata all'*original message*. Non potendo fare un affidamento

How is referred in § 4.3.4 on point D of pag. 45 and note[13] and [14], the standard EN 319 532-3 **[3]**, Clause 4.2 foresees that REMSP could add or edit, in the enveloping process, some header of the *original message*. That changes must be proved to be limited to necessity cases. In the case of the **Message-ID** MIME header, the operation specified below is justified by the needs of guarantee the proper functioning of the system.

In particular, it is fundamental to ensure the uniqueness of the identifier of all the *original messages* accepted by the entire REMSPs system, with the scope to guarantee the correct tracking of all the REM messages (i.e., the REM dispatches and the REMS receipts) relevant, everyone, to same transaction related to the *original message*.

certo sulla validità e univocità del Message-ID generato dai client di posta elettronica (che è al di fuori della responsabilità di ogni REMSP), il REMSP deve provvedere, per ogni submission, alla definizione di un nuovo specifico Message-ID univoco (in accordo allo standard). Questo nuovo Message-ID dovrà essere impostato opportunamente dal REMSP, durante il processo di imbustamento, nell'header Message-ID dell'*original message* e del REM dispatch che lo ospiterà.

Mentre, al fine di garantire al mittente l'associazione tra l'*original message* inviato e le relative ricevute, il Message-ID dell'*original message* specificato normalmente dal client (e quando non fatto sarà assegnato automaticamente dall'S-REM) sarà salvato nell'*original message* stesso, nel REM dispatch e nelle varie REMS receipt usando dappertutto l'header:

REM-UAMessageIdentifier.

Per completare la descrizione, si noti che i due suddetti header Message-ID e REM-UAMessageIdentifier saranno anche mappati, rispettivamente, nei due seguenti elementi della ERDS evidence:

- *MessageIdentifier*
- *UserContentInfo/AppLayerIdentifier*

Not being able to rely on the validity and the uniqueness of the Message-ID generated by the e-mail client (that is out of REMSP responsibility), any REMSP has to provision, for every submission, the definition of a new specific unique Message-ID (according to the standard). This new Message-ID must be set appropriately by the REMSP, during the enveloping process, in the Message-Id header of the *original message* and of the REM dispatch that will host it.

While, in order to ensure to the sender the associations between the *original message* submitted and the relevant receipts, the Message-ID of the *original message* specified usually by the e-mail client (and when not done it will be assigned by S-REMS) will be saved in the *original message* itself, in the REM dispatch and in any of the various REMS receipt using overall the header:

REM-UAMessageIdentifier.

To full described the description, note that these headers Message-ID and REM-UAMessageIdentifier will be also mapped, respectively, in the following elements of the ERDS evidence:

- *MessageIdentifier*
- *UserContentInfo/AppLayerIdentifier*

Si riportano, per completezza, alcuni riferimenti dello standard EN 319 532 riguardanti l'argomento:

- EN 319 532-3 **[3]**, Clause 4.2 – Nota 2: il Message-ID è indicato come uno dei possibili header da sostituire (es. nel caso in cui sia assente o anche solo per normalizzarlo ad un identificativo con un formato universalmente riconosciuto).
- EN 319 532-3 **[3]**, Clause 6.2.1: il valore dell'header Message-ID è obbligatorio per tutte le tipologie di REM message e deve essere un UID come definito in IETF RFC 5322 **[17]**, section 3.6.4.
- EN 319 532-3 **[3]**, Clause 6.1: REM-UAMessageIdentifier, nello standard REM, dovrebbe contenere il Message-ID dell'*original message* inviato dall' e-mail **ERD user agent/application** (**ERD-UA**).
- EN 319 532-3 **[3]**, Annex A: il messaggio di esempio riporta, nel Message-ID, l'identificativo sostituito dal S-REMS, e in REM-UAMessageIdentifier quello originale.

Si noti inoltre che, come stabilito nell'EN 319 532-4 **[4]**, Clause C.3.4, Table C.18 item l), il sub-element "UserContentInfo/AppLayerIdentifier" riporta il Message ID dell'*original message*, cioè

Here follows, for completeness, some reference of the ETSI standard EN 319 532 regarding the case under consideration:

- EN 319 532-3 **[3]**, Clause 4.2 – Note 2: the Message-ID is referred to as one possibly header to substitute (e.g. in case is missed or also just to normalize it to an identifier with a universally known format).
- EN 319 532-3 **[3]**, Clause 6.2.1: the value of Message-ID header is mandatory for all typologies of REM message and must be a UID as defined in IETF RFC 5322 **[17]**, section 3.6.4.
- EN 319 532-3 **[3]**, Clause 6.1: REM-UAMessageIdentifier, in the REM standard, has to contain the Message-ID of the *original message* submitted by e-mail **ERD user agent/application** (**ERD-UA**).
- EN 319 532-3 **[3]**, Annex A: the example message contains, in the Message-ID, the identifier replaced by the S-REMS, and in REM-UAMessageIdentifier the original one.

Also note that, as prescribed in EN 319 532-4 **[4]**, Clause C.3.4, Table C.18 item l), the sub-element "UserContentInfo/AppLayerIdentifier" contains the Message-ID of the *original*

quello generato dell'**ERD user agent/application** (**ERD-UA**).

Di conseguenza, per il **REMID policy=REM-Policy-IT** è prescritto che:

- L' S-REMS deve sostituire il Message-ID con un UID come definito in IETF RFC 5322 **[17]**, section 3.6.4
- L'eventuale Message-ID presente nell'*original message* è inserito nel REM dispatch, nelle relative REMS receipt correlate e nell'*original message* tramite l'header REM-UAMessageIdentifier

Fare riferimento al § 2.9.2 in merito alle tolleranze da applicare rispetto a REM message provenienti da policy differenti alla **REM-Policy-IT**.

Da **Figure 15** fino a **Figure 18** sono riportati degli esempi significativi di impostazione dei vari identificativi per ogni tipo di REM message.

message, i.e. that generated by the **ERD user agent/application** (**ERD-UA**).

Consequently, for the **REMID policy=REM-Policy-IT** is prescribed that:

- The S-REMS must replace the Message-ID with an UID defined according to IETF RFC 5322 **[17]**, section 3.6.4
- The possible Message-ID present in the *original message* will be set in the REM dispatch, in any relevant REMS receipt correlate and in in the *original message* through the REM-UAMessageIdentifier header.

Refer to § 2.9.2 regarding the tolerance to apply in respect to REM messages coming from policies different from **REM-Policy-IT**.

A number of significant examples regarding the set of possible identifiers for any type of REM message are illustrated from **Figure 15** up to **Figure 18**.

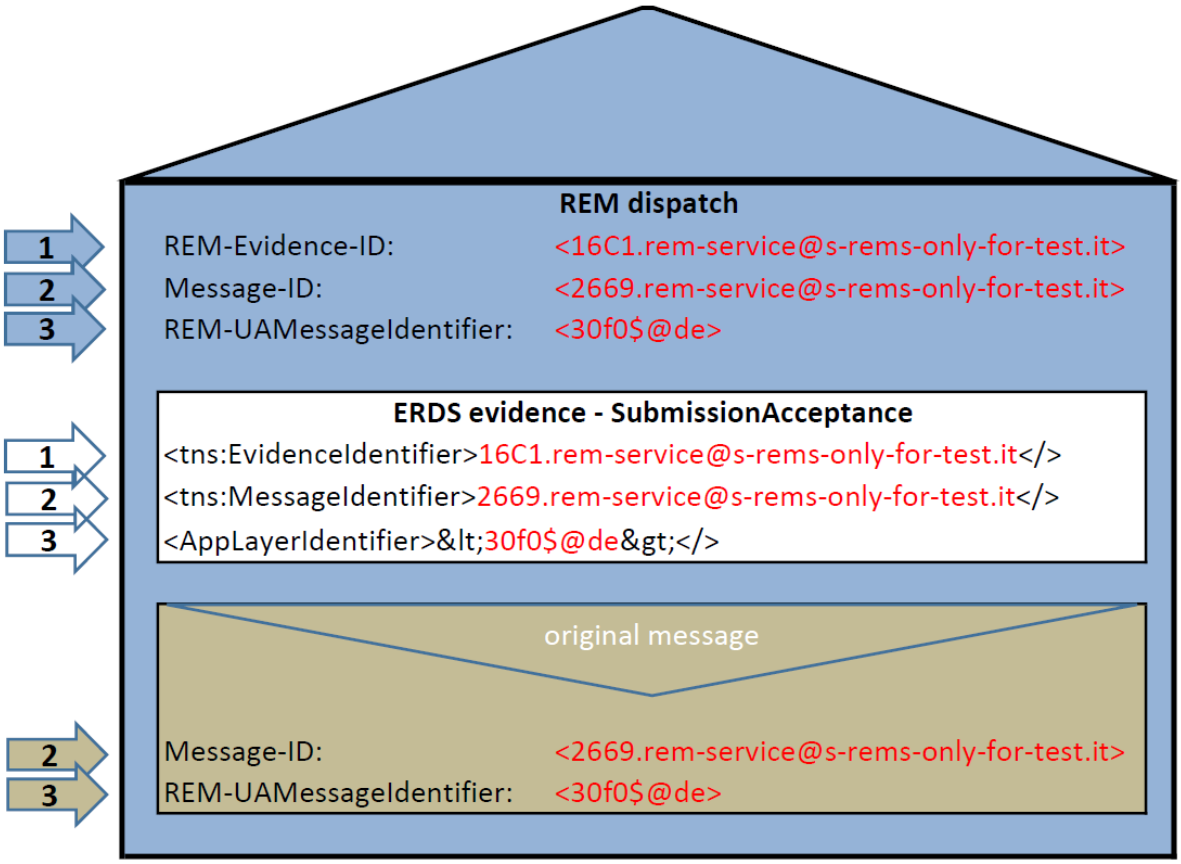


Figure 15 – REM dispatch – message and evidence identifiers

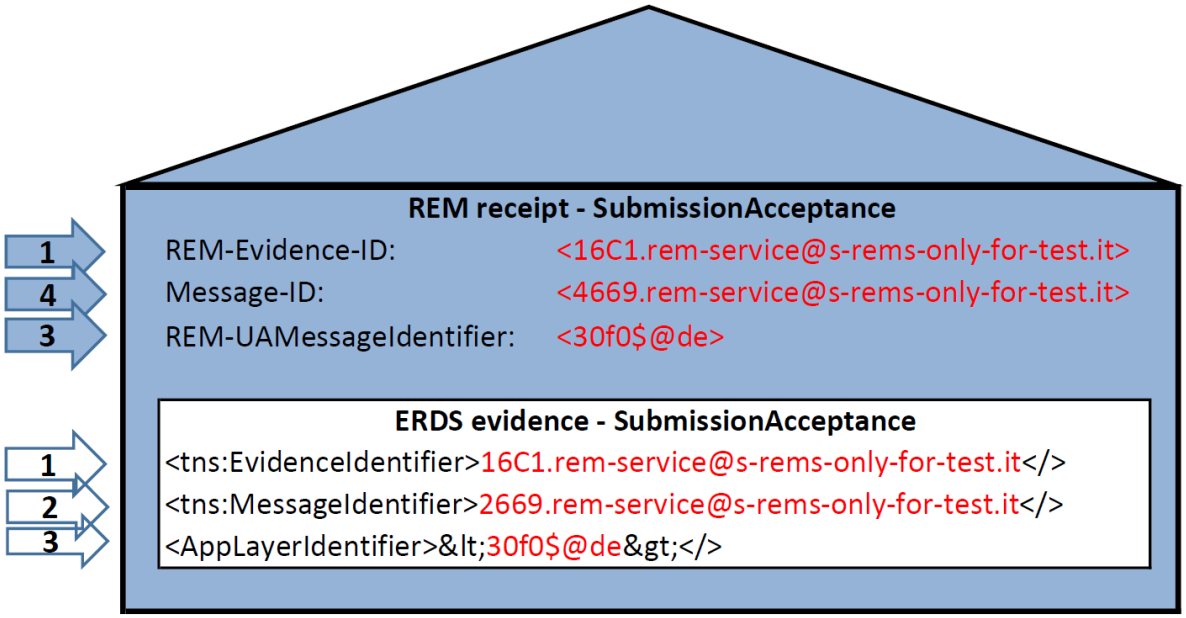


Figure 16 – REMS receipt – SubmissionAcceptance – message and evidence identifiers

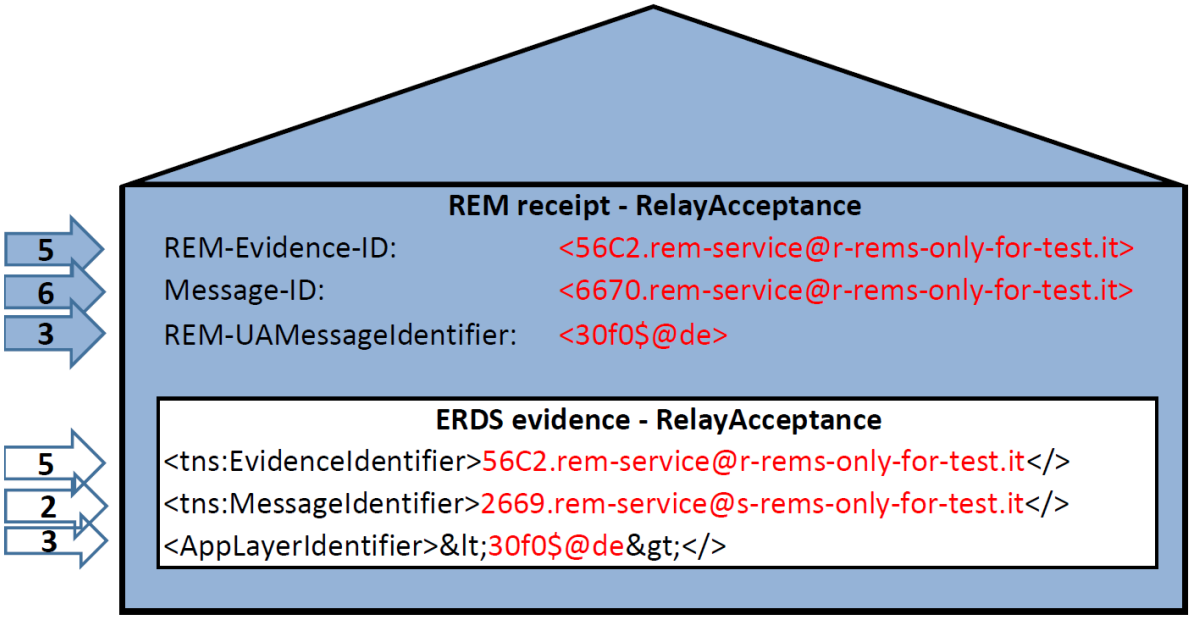


Figure 17 – REMS receipt – RelayAcceptance – message and evidence identifiers

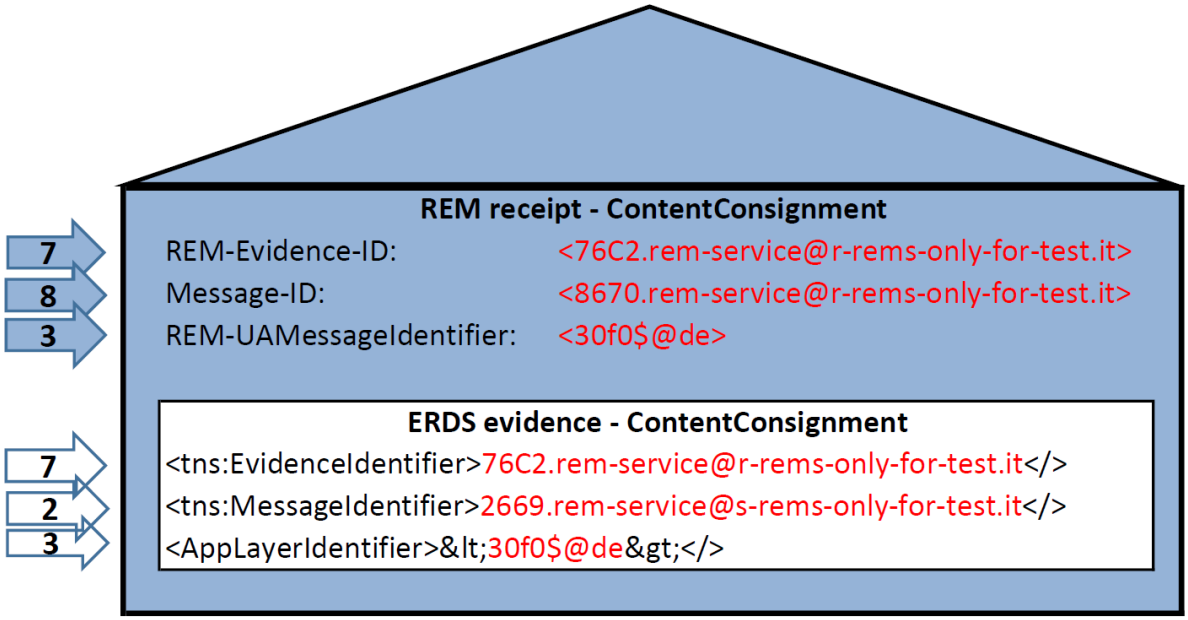


Figure 18 – REMS receipt – ContentConsignment – message and evidence identifiers

2.4.2.4 Gestione log ufficiali | Official log operation

Il log costituisce la registrazione sequenziale e cronologica di eventi generati a seguito di una operazione di una specifica entità (soggetto umano o processo automatico) con finalità di analisi, monitoraggio e verifica.

Come riportato nel § 4.3.1 al punto A di pag. 24, nell'ambito REM, il registro dove vengono tracciate tutte le transazioni relative agli eventi che innescano la conseguente generazione di ogni evidenza ad essi correlata (le cosiddette ERDS evidence) è denominato **official log**.

The log constitutes the sequential and chronological recording of the events generated by an operation of a specific entity (human or automatic process) with the scope of analysis, monitoring and checking.

How is referred in § 4.3.1 on point A of pag. 24, in the REM area, the register where are tracked all the transactions relevant to the events triggering the consequent generation of any related evidence (the so called ERDS evidence) is called **official log**.

Il processo di generazione degli **official log** inizia con la presa in carico dell'*original message* da parte del sender's REMSP. Mentre per il recipient's REMSP, il processo inizia con la ricezione del REM dispatch predisposto ed inviato dall'S-REMS. Tale processo chiude il proprio ciclo di vita con il tracciamento delle ricevute (REMS receipt) innescate da, e connesse con, il flusso seguito dal REM dispatch.

L'**official log** dovrà contenere almeno i dati definiti nella seguente **Table 7**[34]:

The process of generation of the **official log** begins when the sender's REMSP takes in charge the *original message*. While, for the recipient's REMSP, the process starts with the arrival of the REM dispatch prepared and relayed by S-REMS. This process closes its life cycle with the tracking of the receipts (REMS receipt) triggered from, and connected with, the flow followed by the REM dispatch.

The **official log** must contain at least the information defined in following **Table 7**[34]:

[34] Si demanda al provider REM la scelta tecnologica utilizzata per implementare la storicizzazione delle informazioni riportate nell'official **official log**.

[34] It is left to the REMSP the technological choice to use for the implementation and storing of the information recorded in the **official log**.

Table 7 – official log minimum set: records format

Id	Log Element	ERDS evidence map	EN 319 522-2 Code	Note
OLR1	**Message-ID**	MessageIdentifier	M01/MD11	UID (according to msg-id RFC 5322 [17], section 3.6.4) identifying any REM message envelope (see the second header (azure arrows Nr. 2, 4, 6, 8 on the left) in the examples from **Figure 15** up to **Figure 18**). In the case of REM dispatch, it is provided by S-REMS to univocally identify any REM message of the entire transaction related to the *original message*. Therefore, the same identifier is also replicated by reset of the **Message-ID** of *original message* (see brown/azure arrows Nr. 2 on the left of the examples in **Figure 15**). For any REM message it is also copied in the **MessageIdentifier** ERDS evidence element (see white arrows Nr. 2 on the left of the examples from **Figure 15** up to **Figure 18**).
OLR2	**UAMessageId**	UserContentInfo/ AppLayerIdentifier	M02/MD14	Message-ID specified, if any, by the client **ERD user agent/application** (**ERD-UA**), and set to the Application-layer/protocol identifier ERDS element. For any REM message it is set as **REM-UAMessageIdentifier** MIME header and it is also copied in the **AppLayerIdentifier** ERDS evidence element (see row **PP3o** of **Table 2** at § 2.3.1, and the white arrows Nr. 3 on the left of the examples from **Figure 15** up to **Figure 18**)
OLR3	**Evidence-ID**	EvidenceIdentifier	G01	UID identifying any ERDS evidence. For any REM message it is set in the **REM-Evidence-ID** MIME header and it is also copied in the **EvidenceIdentifier** ERDS evidence element (see row **PP3e** of **Table 2** and arrows Nr. 1, 5 and 7 on the left of the examples from **Figure 15** up to **Figure 18**).
OLR4	**EventTime**	EventTime	G05	Date and time of the event in UTC format.
OLR5	**Sender**	SenderDetails/ Identifier	I02	E.g., one e-mail address.
OLR6	**Recipients**	(RecipientDetails/ Identifier)*	I06	List of CSV (*) of e-mail addresses
OLR7	**Subject**	N/A	MD14	The subject of the *original message*
OLR8	**ERDSEventId**	ERDSEventId	G03	See **Table 3, Table 5** and **Table 8** for the full list of allowed values for **REM-Policy-IT**
OLR9	**EventReasons**	(EventReason/**Reason Code**) (EventReason/Details)*	G04	See column 3 of **Table 15** for the full list of allowed short codes values for the **REM-Policy-IT**
OLR10	**SREMSName**	EvidenceIssuerDetails/LegalName	R02	The details of the REMSP that has issued the ERDS evidence.
OLR11	**SREMSAdr**	N/A	N/A	The e-mail address of S-REMS (the same of that present on digital certificate used to sign the ERDS evidence). This is set in the "**From**:" header of any REM message (*see* AP4 row of **Table 4** at § 2.4.1 and **PP6** row of **Table 2** at § 2.3.1).
OLR12	**RREMSAdrs**	N/A	N/A	List of CSV (*) e-mail addresses of R-REMSs (the same of that is found on the **MX record** associated to each recipient's e-mail domain specified in I06 component).
OLR13	**EvidenceRef**	N/A	N/A	Either a reference to the full XML ERDS evidence or a blob with all its structure.
OLR14	**AttachCount**	N/A	N/A	Optionally, for the REM dispatch, the number of attachments of the *original message*, when possible to easily extract them

(*) The "**Reason Code**" contained in the first "Detail" element can fully identify the event (e.g. "**RA02**" is equivalent to "Invalid message format". If some optional "Detail" element is present in the ERDS evidence (see **Row PP24 of Table 2**) its value is saved in the official log (e.g. "**RA02**; *Unspecified recipients*").

Al verificarsi dell'evento, la componente software che ha generato o rilevato l'evento stesso, provvede a collezionare la lista di dati significativi sopra descritti per procedere con la relativa memorizzazione e avendo cura di

Upon the occurrence of the event, the software component generating or detecting the event itself, collects the list of significant data described above to proceed

tracciare le operazioni rilevanti al funzionamento del servizio.

È compito del REMSP assolvere alla funzionalità di memorizzazione e conservazione a lungo termine dell'**official log** per il periodo e le modalità stabilite dal DPCM (si propone una durata di 30 mesi).

Di seguito nella terza colonna della **Table 8** l'elenco degli **Eventi** che devono essere tracciati nell'**official log**. Nella seconda colonna della **Table 15** del § 2.5.1 è riportato lo **short-code** dell'elenco completo degli errori indicato ad essere tracciato nell'**official log**.

with their recording having care to track the operations relevant to the service working.

It is under the responsibility of the REMSP to absolve to the obligation of long-term retention of **official log** for the period and modality stated by the DPCM (it is proposed a period of 30 months).

Following, the third column of **Table 8**, contains the **Event** list that must be tracked in the **official log**. The third column of **Table 15** of § 2.5.1 contains the **short-codes** of the full list of candidate errors to be tracked in the **official log**.

Table 8 – official log: events to Issue (I) / Track (T)

Id	Operation/Element	Log EventId - OLR8	S-REMS	R-REMS	Target	REM baseline
OLE1	**Submission/Acceptance of original message**	**SubmissionAcceptance**	I/T		Sender	Y
OLE2	**Submission/Rejection of original message**	**SubmissionRejection**	I/T		Sender	Y
OLE3	**Relay/Successful of REM dispatch**	**dispatch**	I/T	T	Recipient	Y
OLE4	**Relay/Acceptance of REM dispatch**	**RelayAcceptance**	T	I/T	S-REMS	Y
OLE5	**Relay/Rejection of REM dispatch**	**RelayRejection**	T	I/T	S-REMS	Y
OLE6	**Relay/Failure of REM dispatch**	**RelayFailure**	I/T		Sender	Y
OLE7	**Content/Consignment of REM dispatch**	**ContentConsignment**	T	I/T	Sender	Y
OLE8	**Content/ConsignmentFailure of REM dispatch**	**ContentConsignmentFailure**	T	I/T	Sender	Y
OLE9	**Relay/Escape of REM dispatch**	**RelayToNonERDS**	I/T		Sender	N
OLE10	**Relay/Escape Rejection of REM dispatch**	**RelayToNonERDSFailure**	I/T		Sender	N
OLE11	**Relay/Arrival of non-ERDS content**	**ReceivedFromNonERDS**		I/T	Recipient	N

Note:

I/T TAG in the fourth/fifth columns means that the event is "issued" and "tracked" (only one row in DB is sufficient) by the corresponding entity (e.g., issuer/S-REMS or receiver/R-REMS).

T TAG in the fourth/fifth columns means that the event is only "tracked" by the corresponding entity (e.g., issuer/S-REMS or receiver/R-REMS).

2.4.2.5 Restituzione dell'original message nella ContentConsignment receipt | Return of the original message inside the ContentConsignment receipt

Come riportato al punto "A ERDS and REM data structures." al § 4.3.2, pag. 35 del documento base, lo standard non prevede una ricevuta REM che attesti la consegna del messaggio al destinatario con allegato al proprio interno l'*original message*. La REM ContentConsignment receipt prevede solo il "digest" dell'*original message*. Nell'ambito della **REMID policy=REM-Policy-IT** (e, uniformemente, nel bacino di **utenza** servito dalla suddetta policy) è necessario implementare un flusso che consenta all'utente la possibilità di scegliere se ricevere l'*original message* in allegato alla ContentConsignment.

Le questioni da indirizzare per tale scopo sono:

1) Consentire la possibilità di verifica dell'integrità dell'*original message* contro il suo "**digest**" (presente nelle varie evidenze e quindi anche nella ContentConsignment evidence) in una delle due seguenti modalità:

How per the point "A ERDS and REM data structures." at § 4.3.2, pag. 35 of the basic document, the standard doesn't specify a REMS receipt that ensures the delivery of the message to the recipient with the *original message* attached inside it. Only the "digest" of the *original message* is foreseen in the REM ContentConsignment receipt. In the **REMID policy=REM-Policy-IT** scope (and, uniformly, in the area served by the aforementioned policy) it is possible to implement a flow allowing the possibility for the user to choose if receive the *original message* as an attachment of the REM ContentConsignment receipt.

The questions to address for such purpose are:

1) Allow the option to verify the *original message* integrity against its "**digest**" (present in any evidence and therefore even in the ERDS ContentConsignment evidence) according to one of the following modalities:
   a) When required by the user, allow to save the *original message*, protected

a) Se richiesto dal mittente, dare la possibilità di salvare l'*original message* – mantenuto in forma protetta e incapsulata dentro il REM dispatch – nella **casella** del mittente in un folder di default (si veda sotto per il nome suggerito) o specificato in un apposito header.

b) Se richiesto dal mittente, dare la possibilità che la **ContentConsignment receipt** restituisca indietro al mittente, come allegato, l'*original message* – integro e come medesima sequenza di byte rispetto a quello contenuto nel REM dispatch.

2) Consentire l'uso del servizio senza nessuno dei due punti a) e b) sopra (ad es. per ragioni di performance e/o nei casi in cui non sia ritenuto fondamentale dall'utente avere l'*original message* per controverifica, ma gli sono sufficienti gli attestati di evidenza XML - contenenti il solo digest - forniti normalmente in ogni REMS receipt).

3) Individuare il comportamento di **default**[35] del servizio, quando nessuna scelta è

in the incapsulated form inside the REM-dispatch - in the sender's **mailbox** in a default folder (see below for the name suggested) or in one specified through a MIME header.

b) When required by the user, allow that the **ContentConsignment receipt** returns back to the sender, as an attachment, the *original message* - intact and taken byte per byte - from the REM dispatch.

2) Allow the use of the service without any of the points a) and b) above, (e.g., for performance reasons and/or in case it is not considered fundamental from the user to have the *original message* for counter-testing purposes, but are sufficient the XML evidence attestations - that hold only the digest – normally provided in any REMS receipt.

3) Individuate the **default**[35] behaviour for the service, when no choice is selected by the user (or it is not set in the sender's preferences).

[35] Ovviamente, come best-practice, un comportamento di riferimento può essere impostato dall'utente nelle proprie preferenze che diventa prevalente rispetto a quello del servizio.

[35] As best practice, obviously, a reference behaviour can be set to the user's preferences by the sender and its became prevalent in respect to the service default.

selezionata dall'utente (o nelle sue preferenze).

Le modalità per raggiungere i suddetti obiettivi sono dettagliate nel seguito.

1.a): La funzionalità di "salvataggio" dell'*original message* può essere selezionata dal seguente apposito header:

REM-ContentConsignment: SaveOriginalMessage[;folder=my-sent]

L'utente mittente può richiedere (ad es. attraverso le proprie preferenze o quando possibile/comodo anche direttamente nell'Header dell'*original message*) con questo MIME header *component* specificando, eventualmente, anche il folder dove preferisce i REM dispatch vengano salvati (il folder di default "dispatch-sent" può essere previsto quando non altrimenti specificato dall'utente).

1.b): L'opzione per richiedere la restituzione dell'intero *original message* nella REM ContentConsigment receipt può essere selezionata dal seguente apposito header nell' *original message*, che è necessario che il REMSP replichi anche nel REM dispatch:

REM-ContentConsignment: ReturnOriginalMessage

Follows the details.

1.a): the "save" functionalities of the *original message* can be selected from the following specific header:

REM-ContentConsignment: SaveOriginalMessage[;folder=my-sent]

The sender can require (e.g., through his/her own preferences or if possible/comfortable even directly inside the Header of the *original message*) with such MIME header *component* specifying, possibly, also the preferred folder where all the REM dispatches have to be saved (the default folder "dispatch-sent" can be used when it is not specified by the user).

1.b): The options to require the restitution of the whole *original message* in the REM ContentConsigment receipt can be selected by the following header in the *original message*, that has to be replicated, by the REMSP, also in the REM dispatch:

REM-ContentConsignment: ReturnOriginalMessage

The sender can require the option (e.g., through his/her own preferences or if possible/comfortable even directly inside the Header of the *original message*) with this

L'utente mittente può richiedere l'opzione (ad es. attraverso le proprie preferenze o quando possibile/comodo anche direttamente nell'Header dell'*original message*) con questo MIME header *component*. Nel caso esista il suddetto header, qualsiasi REMSP aderente alla **REM-Policy-IT** deve incorporare l'*original message* nella REM ContentConsigment receipt, indipendentemente da dove provenga il REM dispatch. Ovviamente, è importante essere "resilienti" e non aspettarsi il suddetto comportamento da REMSP esterni alla **REM-Policy-IT**, che non hanno l'obbligo di onorare tale header e possono ovviamente ignorarlo.

La modalità tecnica con cui si allega l'*original message* nella REM ContentConsignment receipt sfrutta il meccanismo delle estensioni MIME definito dallo standard. Si veda anche il punto UU a pag. 71 del documento con le scelte sui criteri di adozione dello standard (documento base da qui in avanti) per altri dettagli. Sono rispettati i requisiti di obbligatorietà definiti nello standard (Table 9 EN 319 532-3 **[3]**). Ma si rendono obbligatorie, quando è richiesto il servizio di "**ReturnOriginalMessage**" dal suddetto header, e solo per le ContentConsignment receipt emesse da REMS

MIME header *component*. In presence of the above-mentioned header, any REMSP adhering to the **REM-Policy-IT** must attach the *original message* in the REM ContentConsigment receipt, independently from when is coming the REM dispatch. Obviously, it is important to be "resilient" and to do not expect this behaviour from REMSP outside the **REM-Policy-IT**, that aren't obliged to honour this header and could ignore it.

Technically speaking, the *original message* is attached in the REM ContentConsignment receipt leveraging the MIME extension mechanism defined in the standard. See also the point UU at pag. 71 of the main part of the present document (basic document hereinafter) for other details. The mandatory requirements defined in the standard (Table 9 EN 319 532-3 **[3]**) are respected. Additionally, when is required the service "**ReturnOriginalMessage**" from the aforementioned header, and only for ContentConsignment receipts issued by REMS belonging to the **REM-Policy-IT**, also the following options:

appartenenti alla **REM-Policy-IT**, anche le seguenti opzioni:

Il parametro <REM_EXTENSION_NAME> deve essere valorizzato con la stringa "**original-message.eml**"

L'header *Content-Transfer-Encoding*: deve essere valorizzato con "**binary**" oppure "**base64**" e

REM-Section-Type: **rem_message/extension**

REM-Extension-Code: **original-message**

Si veda il seguente stralcio di ContentConsignment receipt che esemplifica, in particolare, come viene incapsulato l'*original message* nella suddetta estensione della struttura MIME della ricevuta:

The parameter <REM_EXTENSION_NAME> must match the string "**original-message.eml**"

The header *Content-Transfer-Encoding*: must match the value "**binary**" or "**base64**".

REM-Section-Type: **rem_message/extension**

REM-Extension-Code: **original-message**

See the following excerpt of ContentConsignment receipt exemplifying how the *original message* is encapsulated in the MIME extensions structure of the receipt.

```
Content-Type: application/octet-stream; name=original-message.eml
Content-Transfer-Encoding: binary
Content-Disposition: attachment; filename=original-message.eml
REM-Section-Type: rem_message/extension
REM-Extension-Code: original-message

From: ….
To: …
… hereinafter continue with the original message
```

Figure 19 – REM ContentConsignment – excerpt of original message attachment

Nel caso sia ritenuto fondamentale per delle necessità o usi specifici che lo giustifichino e che dovessero maturare in futuro, attraverso il meccanismo di aggiornamento delle prassi generali (si veda il § 2.6.1), possono essere previste modalità alternative a quella illustrata sopra (ContentConsignment comprendente in allegato l'intero original message). A titolo esemplificativo ma non esaustivo potrebbe essere prevista una ricevuta di

If it is considered essential for specific needs or uses that justify it and which may arise in the future, through the update mechanism of the best practices (see § 2.6.1), alternative methods to that shown above (where the ContentConsignment includes the overall original message as attachment) can be provided. By way of example but not limited to, a ContentConsigment receipt equivalent to the "brief" or "syntetic" "**PEC** consignment

ContentConsignment equivalente alla ricevuta "sintetica" o "breve" della **PEC**, qualora la modalità nativa prevista dalla **REM** (che prevede invece l'hash dell'intero original message) non sia invece considerata sufficiente a coprire eventuali esigenze che dovessero emergere. Ovviamente, occorre sempre tenere presente che, così come in quello già proposto all'inizio del presente paragrafo, anche in questi nuovi casi occorre tenere conto dell'interoperabilità con altre policy differenti dalla **REM-Policy-IT**. Valgono pertanto tutti i ragionamenti fatti prima, in merito alla resilienza e al fatto che tale regola dovrà eventualmente essere rispettata solo all'interno della **REM-Policy-IT**.

receipt" could be provided, if and when the native method provided by the **REM** (which instead foresees the hash of the overall original message) is not considered sufficient to cover possible needs that may arise. Obviously, it should always be considered that, as per the proposal at the beginning of the present paragraph, even in these new cases it is necessary to take into account the interoperability with other policies different from **REM-Policy-IT**. All the reasoning made above, regarding resilience and the fact that this rule is eventually respected only within **REM-Policy-IT** will be, therefore, valid even in these possible new cases.

2.4.2.6 Strutture di base testo accompagnamento dei REM message | Basic introductory text of REM messages

Come indicato nello standard EN 319 532-3 **[3]**, Figure 1 e Figure 2, ogni REM dispatch e REMS receipt prevede un testo in formato TXT e HTML di introduzione per l'utente: *<<A message created by the REMS, to be displayed automatically upon display of the REM message. Text may contain information for the user (see clause 6.2.3.4)>>*. Il contenuto informativo che sia in TXT o nell'equivalente HTML, deve essere identico in entrambi i formati (si vedano anche i punti G di pag. 47 e H di pag. 48 del § 4.3.4 del documento base).

How per the dispositions of EN 319 532-3 **[3]**, Figure 1 e Figure 2, every REM dispatch and REMS receipt foresees an introduction text for the user, in TXT and HTML format: *<<A message created by the REMS, to be displayed automatically upon display of the REM message. Text may contain information for the user (see clause 6.2.3.4)>>*. The informational content of TXT and HTML parts has to be identical for both formats (see also the points G at pag. 47 and H at pag. 48 of § 4.3.4 of the basic document). La **REM-**

La **REM-Policy-IT** prevede che tale testo introduttivo sia espresso almeno nei due linguaggi "italiano" ed "inglese". A tutto vantaggio di un'uniformità di fruizione, sono forniti nel seguito, da **Figure 20** a **Figure 23**, i template raccomandati per la costruzione dei suddetti testi di accompagnamento ad ogni REM message all'interno della **REM-Policy-IT**.

Policy-IT foresees that such introduction text is expressed at least in "Italian" and in "English". For the benefit of a uniformity of fruition, follows from **Figure 20** to **Figure 23** the recommended templates to use, inside the **REM-Policy-IT**, to build the aforementioned accompanying texts of any REM message.

```
Messaggio REM
Il giorno %VAR_DAY% alle ore %VAR_HOUR%
il messaggio: "%VAR_ORIGINAL_SUBJECT%" è stato inviato da "%VAR_SENDER%"
ed indirizzato a:
%VAR_RECIPIENTS_LIST%

Il messaggio originale è incluso in allegato.

Identificativo messaggio: "%VAR_MESSAGE_IDENTIFIER%"
REM service provider: "%VAR_REMS_ISSUER%"

Il titolare della casella mittente "%VAR_SENDER%" è stato identificato come "%VAR_SENDER_NAME%[, %VAR_SENDER_IDENTIFIER%]"

L'allegato SubmissionAcceptance.xml contiene informazioni di servizio sulla trasmissione.

-------------------------------------------------------------------------------------

REM Dispatch
On %VAR_DAY% at %VAR_HOUR%
the message: "%VAR_ORIGINAL_SUBJECT%" was sent by "%VAR_SENDER%"
and addressed to:
%VAR_RECIPIENTS_LIST%

The original message is attached.

Message identifier: "%VAR_MESSAGE_IDENTIFIER%"
REM service provider: "%VAR_REMS_ISSUER%"

The owner of the sender mailbox "%VAR_SENDER%" was identified as "%VAR_SENDER_NAME%[, %VAR_SENDER_IDENTIFIER%]"

The SubmissionAcceptance.xml attachment contains service information on the transmission.
```

Figure 20 – REM dispatch – Introduction template – TXT format

NOTE: the square brackets above [] are metacharacters indicating the entire part that could be not present when the element `%VAR_SENDER_IDENTIFIER%` is not included.

```
  <h1>Messaggio REM</h1>
  <p>Il giorno %VAR_DAY% alle ore %VAR_HOUR%</p>
  <p>il messaggio: "<B>%VAR_ORIGINAL_SUBJECT%</B>" è stato inviato da "<a href="mailto:%VAR_SENDER%">%VAR_SENDER%</a>"<BR>ed
indirizzato a:<BR>
  %VAR_RECIPIENTS_LIST%
  </p>

  Il messaggio originale è incluso in allegato.

  <p>Identificativo messaggio: <a href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a><BR>
  REM service provider: "%VAR_REMS_ISSUER%"</p>

  <p>Il titolare della casella mittente "%VAR_SENDER%" è stato identificato come "%VAR_SENDER_NAME%[,
%VAR_SENDER_IDENTIFIER%]"</p>

  L'allegato SubmissionAcceptance.xml contiene informazioni di servizio sulla trasmissione.

  <HR/>

  <h1>REM Dispatch</h1>
  <p>On %VAR_DAY% at %VAR_HOUR%</p>
  <p>the message: "<B>%VAR_ORIGINAL_SUBJECT%</B>" was sent by "<a href="mailto:%VAR_SENDER%">%VAR_SENDER%</a>"<BR/>and
addressed to:<BR>
  %VAR_RECIPIENTS_LIST%
  </p>

  The original message is attached.

  <p>Message identifier: <a href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a><BR>
  REM service provider: "%VAR_REMS_ISSUER%"</p>

  <p>The owner of the sender mailbox "%VAR_SENDER%" was identified as "%VAR_SENDER_NAME%[, %VAR_SENDER_IDENTIFIER%]"</p>

  The SubmissionAcceptance.xml attachment contains service information on the transmission.
```

Figure 21 – REM dispatch – Introduction template – HTML format

NOTE: the square brackets above [] are metacharacters indicating the entire part that could be not present when the element **%VAR_SENDER_IDENTIFIER%** is not included.

```
Ricevuta di %VAR_EVENT_NAME%
Il giorno %VAR_DAY% alle ore %VAR_HOUR%
il messaggio: "%VAR_ORIGINAL_SUBJECT%" inviato da "%VAR_SENDER%"
ed indirizzato a:
%VAR_RECIPIENTS_LIST%

%VAR_RECEIPT_DESCRIPTION_IT%

Identificativo messaggio: "%VAR_MESSAGE_IDENTIFIER%"
REM service provider: "%VAR_REMS_ISSUER%".

-----------------------------------------------------------------------------------------

Receipt of %VAR_EVENT_NAME%
On %VAR_DAY% at %VAR_HOUR%
the message: "%VAR_ORIGINAL_SUBJECT%" sent by "%VAR_SENDER%"
and addressed to:
%VAR_RECIPIENTS_LIST%

%VAR_RECEIPT_DESCRIPTION_EN%

Message identifier: "%VAR_MESSAGE_IDENTIFIER%"
REM service provider: "%VAR_REMS_ISSUER%".
```

Figure 22 – REMS receipt – Introduction template – TXT format

```
<h1>Ricevuta di %VAR_EVENT_NAME%</h1>
<p>Il giorno %VAR_DAY% alle ore %VAR_HOUR%</p>
<p>il messaggio: "<B>%VAR_ORIGINAL_SUBJECT%</B>" inviato da "<a
href="mailto:%VAR_SENDER%">%VAR_SENDER%</a>"<BR>ed indirizzato a:<BR>
%VAR_RECIPIENTS_LIST%
</p>
<p>%VAR_RECEIPT_DESCRIPTION_IT%</p>

<p>Identificativo messaggio: <a
href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a><BR>
REM service provider: "%VAR_REMS_ISSUER%".</p>

<HR/>

<h1>Receipt of %VAR_EVENT_NAME%</h1>
<p>On %VAR_DAY% at %VAR_HOUR%</p>
<p>the message: "<B>%VAR_ORIGINAL_SUBJECT%</B>" sent by "<a
href="mailto:%VAR_SENDER%">%VAR_SENDER%</a>"<BR>and addressed to:<BR>
%VAR_RECIPIENTS_LIST%
</p>
<p>%VAR_RECEIPT_DESCRIPTION_EN%</p>

<p>Message identifier: <a href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a><BR>
REM service provider: "%VAR_REMS_ISSUER%".</p>
```

Figure 23 – REMS receipt – Introduction template – HTML format

La **Table 9** contiene la descrizione dei place holder utilizzati all'interno dei template. Ciascun elemento è valorizzato in funzione dell'evento che ha determinato la produzione del REM message.

The **Table 9** contains the description of any place holder used inside the templates. Every element is instantiated according to the event determining the creation of the REM message.

Table 9 – Introduction text: templates place holders

Id	Place holder	REM dispatch	REMS receipt	Value (aligned to the relevant evidence)
TPH1	**%VAR_DAY%**	Y	Y	dayOf(<EventTime>) format: dd-mm-yyyy
TPH2	**%VAR_HOUR%**	Y	Y	hourOf(<EventTime>) format: HH:MM:SS (+/- 4-digit-zone-offset)
TPH3	**%VAR_ORIGINAL_SUBJECT%**	Y	Y	subjectOf(original message)
TPH4	**%VAR_SENDER%**	Y	Y	emailOf(sender)
TPH5	**%VAR_RECIPIENTS_LIST%**	Y	Y	emailListOf(recipients)
TPH6	**%VAR_MESSAGE_IDENTIFIER%**	Y	Y	valueOf(<tns:MessageIdentifier>)
TPH7	**%VAR_EVENT_NAME%**		Y	significantPartOf(tns:ERDSEventId)
TPH8	**%VAR_RECEIPT_DESCRIPTION_IT%**		Y	itTextualDescriptionOf(event)
TPH9	**%VAR_RECEIPT_DESCRIPTION_EN%**		Y	enTextualDescriptionOf(event)
TPH10	**%VAR_REMS_ISSUER%**	Y	Y	valueOf(<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="eIp:**LegalNameType**">NAME-OF-THE-REMSP</saml:AttributeValue>)
TPH11	**%VAR_SENDER_NAME%**	Y	N	The name of the **owner** (or **registered holder)** of the sender's mailbox (*) as either the *Given Name* and *Family Name* (separated by a single whitespace) in case of natural person or the *Legal Name* of the legal person (**). See also EN 319 532-4 **[4]**, Clause C.3.4 Table C.18 item h) sub-item I NOTE 4.
TPH12	**%VAR_SENDER_IDENTIFIER%**	Y (recommended)	N	The person semantics identifier of the **owner** (or **registered holder)** of the sender's mailbox (*) as the *Tax identification number* for both natural person and legal person (***).

(*) See the sections about **Registered users** and **Identified users** in § 2.2 for further details on relationships between each of the parties involved.

(**) EXAMPLE: *Mario Rossi* in case of **natural person**; *Bianchi & Verdi S.p.A.* or *Ministero ABC* in case of **legal person**.

(***) If the **owner** is a **natural person**, when the `%VAR_SENDER_IDENTIFIER%` is included, any identifier in such subject field is composed according to the standard EN 319 412-1 **[12]**, Clause 5.1.3, REQs NAT-5.1.3-02, NAT-5.1.3-03)

EXAMPLE: *TINIT-RSSMRA99M24L219Z*

If the **owner** is a **legal person** (for instance like an enterprise, or public administration or another institution or organization **with** or without a **VAT** or a **NTR)**, when the `%VAR_SENDER_IDENTIFIER%` is included, any identifier in such subject field is composed according to the standard EN 319 412-1 **[12]**, Clause 5.1.4, REQs LEG-5.1.4-02, LEG-5.1.4-03)

EXAMPLE 1: *VATIT-12345678900*
EXAMPLE 2: CF:IT-12345678900

where:

CF:	stands for CF/codice-fiscale Italian national scheme, followed by a colon ":"
IT-	stands for IT/ISO 3166-1 Italian country code, followed by a hyphen-minus "-"
12345678900	stands for the identifier/codice-fiscale according to the Italian national scheme.

Il place holder **%VAR_RECIPIENTS_LIST%** può contenere, per ogni indirizzo email, altri elementi quali il displayName e/o la tipologia dell'utente quando nota (es. "EXTERNAL").

La **Table 10** contiene i testi raccomandati a sostituire il place holder **%VAR_RECEIPT_DESCRIPTION_IT%** presente all'interno dei template. La valorizzazione è in funzione del reason code associato all'evento che ha determinato la produzione del REM message.

In alcuni REM message sono presenti ulteriori place holder quali **%REM_SERVICE_NAME%** e **%REM_RECIPIENT%** che devono essere sostituiti rispettivamente con il nome del REMSP e con l'indirizzo e-mail ricevente di competenza.

The **%VAR_RECIPIENTS_LIST%** place holder can contain, for each email address, other attributes like displayName and/or "type of user" when known (e.g. "EXTERNAL").

The **Table 10** contains the text that will substitute the **%VAR_RECEIPT_DESCRIPTION_EN%** place holder present inside the templates. Its instantiation is according to the event determining the creation of the REM message.

Some REM messages have further place holders like **%REM_SERVICE_NAME%** and **%REM_RECIPIENT%** that have to be substituted by the competent REMSP name and recipient's e-mail address.

Table 10 – Introduction text: textual Description of the event

Id	ERDSEventId	Reason code	itTextualDescriptionOf	enTextualDescriptionOf
TDE1	**SubmissionAcceptance**	RA01	è stato accettato dal sistema REM (Codice RA01).	was accepted by the REM system (Code RA01).
TDE2	**SubmissionRejection**	RA02	è stato rifiutato dal sistema REM a causa di un formato non valido (Codice RA02).	was rejected by the REM system due to an invalid format (Code RA02).
		RA03	è stato rifiutato dal sistema REM a causa di presenza malware (Codice RA03).	was rejected by the REM system due to the presence of malware (Code RA03).

		RA05	è stato rifiutato dal sistema REM a causa di violazione della policy (Codice RA05).	was rejected by the REM system due to the policy violation (Code RA05).
		RA06	è stato rifiutato dal sistema REM a causa di un malfunzionamento generale (Codice RA06).	was rejected by the REM system due to a general malfunction (Code RA06).
TDE3	**RelayAcceptance**	RB01	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato preso in carico dal REM service ricevente per il/gli utente/i di sua competenza (Codice RB01).	and relayed to the %REM_SERVICE_NAME% REM service provider was accepted by the recipient REM service for the user(s) of its competence (Code RB01).
TDE4 TDE5	**RelayRejection** **RelayFailure**	RB02	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato a causa del formato non valido (Codice RB02).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to the invalid format (Code RB02).
		RB03	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato per Malware (Codice RB03).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to Malware (Code RB03).
		RB04	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato per firma digitale non valida (Codice RB04).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to invalid digital signature (Code RB04).
		RB05	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato per certificato digitale non valido (Codice RB05).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to invalid digital certificate (Code RB05).
		RB06	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato per violazione della policy (Codice RB06).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to policy violation (Code RB06).
		RB07	non è stato inoltrato al REM service provider %REM_SERVICE_NAME% per un malfunzionamento generale (Codice RB07).	was not relayed to the %REM_SERVICE_NAME% REM service provider due to a general malfunction (Code RB07).
		RB08	non è stato inoltrato al REM service provider %REM_SERVICE_NAME% perché non identificabile (Codice RB08).	was not relayed to the %REM_SERVICE_NAME% REM service provider because it is not identifiable (Code RB08).
		RB09	non è stato inoltrato al REM service provider %REM_SERVICE_NAME% perché non raggiungibile (Codice RB09).	was not relayed to the %REM_SERVICE_NAME% REM service provider because it is unreachable (Code RB09).
		RB10	non è stato inoltrato per destinatario sconosciuto presso il REM service provider %REM_SERVICE_NAME% (Codice RB10).	was not relayed for unknown recipient to the %REM_SERVICE_NAME% REM service provider (Code RB10).
		RB21	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato per utente destinatario non registrato presso il REM service provider (Codice RB21).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to unregistered recipient to the REM service provider (Code RB21).
		RB22	non ha prodotto nei tempi previsti le informazioni di evidenza di inoltro verso il REM service provider %REM_SERVICE_NAME% (Codice RB22).	was not produced in the required time the evidence of relay to the %REM_SERVICE_NAME% REM service provider (Code RB22).
TDE6	**ContentConsignment**	RD01	è stato consegnato nella mailbox del destinatario %REM_RECIPIENT% (Codice RD01).	was consigned in the recipient's mailbox %REM_RECIPIENT% (Code RD01).
TDE7	**ContentConsignmentFailure**	RD03	non ha prodotto nei tempi previsti le informazioni di evidenza di consegna nella mailbox del destinatario, %REM_RECIPIENT%, presso il REM service provider %REM_SERVICE_NAME% (Codice	was not produced in the required time the evidence of consignment in the recipient's mailbox, %REM_RECIPIENT%, to %REM_SERVICE_NAME% REM service provider (Code RD03).

			RD03).	
		RD04	non è stato consegnato nella mailbox del destinatario %REM_RECIPIENT%, presso il REM service provider %REM_SERVICE_NAME%, a causa di mancanza di spazio in casella (Codice RD04).	was not consigned in the recipient's mailbox %REM_RECIPIENT%, to %REM_SERVICE_NAME% REM service provider, due to quota issues on the mailbox (Code RD04).
		RD05	non è stato consegnato nella mailbox del destinatario %REM_RECIPIENT%, presso il REM service provider %REM_SERVICE_NAME%, a causa di un malfunzionamento generale (Codice RD05).	was not consigned in the recipient's mailbox %REM_RECIPIENT%, to %REM_SERVICE_NAME% REM service provider, due to a general malfunction (Code RD05).
		RD06	non è stato consegnato nella mailbox del destinatario %REM_RECIPIENT%, presso il REM service provider %REM_SERVICE_NAME%, a causa di un tipo messaggio non ammesso (Codice RD06).	was not consigned in the recipient's mailbox %REM_RECIPIENT%, to %REM_SERVICE_NAME% REM service provider, due to message type not allowed (Code RD06).
		RD21	non è stato consegnato nella mailbox del destinatario %REM_RECIPIENT% per destinatario non registrato presso il REM service provider %REM_SERVICE_NAME% (Codice RD21).	was not consigned in the recipient's mailbox %REM_RECIPIENT% due to unregistered recipient to the %REM_SERVICE_NAME% REM service provider (Code RD21).
TDE8	**RelayToNonERDS**	RF01	è stato inoltrato verso un sistema esterno alla REM (Codice RF01).	was relayed to a non-REM external system (Code RF01).
TDE9	**RelayToNonERDSFailure**	RF02	nel tentativo di inoltro verso un sistema esterno alla REM ha riportato una condizione di errore perché non raggiungibile (Codice RF02).	in the attempt to relay towards a non-REM external system was returned an error condition because it is unreachable (Code RF02).
		RF03	nel tentativo di inoltro verso un sistema esterno alla REM ha riportato una condizione di errore dovuta al rifiuto del messaggio (Codice RF03).	in the attempt to relay towards a non-REM external system was returned an error condition due to the refusal of the message (Code RF03).
		RF51	non è stato inoltrato verso un sistema esterno alla REM perché questa operazione non è ammessa a causa delle configurazioni del servizio o delle preferenze utente (Codice *RF51*).	was not relayed towards a non-REM external system because this operation is not allowed due to the service configuration or the user's preferences (Code *RF51*).
TDE10	**ReceivedFromNonERDS**	RF04	proveniente da un sistema esterno alla REM è stato accettato dal sistema REM (Codice RF04).	coming from a non-REM external system was accepted by the REM system (Code RF04).

(*) Similarly to what is recommended for the official logs (see row **OLR9** of **Table 7**) the "**Reason Code**" - contained in the text of fourth and fifth columns above in the form of *(Codice XXXX)* and *(Code XXXX)* - is further enriched with additional explanatory text, separated by a semicolon, if some optional "Detail" element is present in the ERDS evidence (see row **PP24** of **Table 2** and the text outlined in green in the following example).

Example: … *was rejected by the REM system due to an invalid format (Code RA02; Unspecified recipients)*.

Gli eventi **TDE4** e **TDE5** in **Table 10** vanno considerati assieme dal punto di vista degli error code (e sono quindi nella stessa riga della tabella). Infatti, ad esempio, l'errore dovuto al

The events **TDE4** and **TDE5** in **Table 10** are considered together from the error code viewpoint (and so they are in the same row of the table). In fact, as an example, the error

codice **RB21** (**MessageNotAcceptedForUnregisteredRecipient**) può essere inserito in ERDS evidence emessa su entrambi gli eventi di relay reject/failure. Un primo esempio di questo caso è quello di un REM dispatch inviato ad un utente inesistente presso l'**R-REMS**. Questo emette una REM relayRejection receipt con codice **RB21** per l'**S-REMS** e a seguito di questa, l'S-REMS emette una REM relayFailure receipt, con lo stesso codice, verso l'utente mittente. Un caso analogo si ha nella gestione della rilevazione di malware lato REMSP ricevente (si vedano le **Figure 30** e **Figure 31**).

due to the code **RB21** (**MessageNotAcceptedForUnregisteredRecipient**) can be used in ERDS evidence issued on the occurrence of both reject/failure relay events. A first example of this case is that of a REM dispatch sent to a unregistered user to a **R-REMS**. It issues a REM relayRejection receipt for **S-REMS** with error code **RB21** and, in turn, the S-REMS issues a REM relayFailure receipt, with the same code, for the sender. A similar case is that of malware detection management at recipient's REMSP (see **Figure 30** and **Figure 31**).

2.4.2.7 *Autenticazione su client di posta elettronica di mercato | Authentication using marketplace e-mail client*

Introduzione

Una considerevole fetta dell'esperienza utente del servizio **PEC** è oggi ampiamente basata sulla fruizione attraverso client di posta elettronica standard.

Al fine di garantire la più ampia diffusione dei servizi REM è stato necessario rendere disponibile una modalità di fruizione del servizio che consenta elevati standard di sicurezza e contemporaneamente renda possibile l'accesso attraverso i protocolli classici della posta elettronica (SMTP/POP3/IMAP4).

Considerando che le modalità prescritte nello standard EN 319 521 **[8]**, Clause 5.2.2, punti a), b) e c) non risultano ancora sufficientemente diffuse nei vari prodotti di mercato, è stata sfruttata l'ulteriore modalità definita al punto d) del suddetto standard, per individuare una soluzione alla suddetta criticità adottabile nell'ambito della **REM-Policy-IT** e soggetta alle security practice nazionali che ne possono limitare l'uso (si veda il § 2.6.1). Di seguito è descritta la soluzione individuata.

Introduction

A considerable part of the **PEC** service user experience is today largely based on a fruition through the standard e-mail client.

In order to guarantee an ever-growing spread of the REM services it was necessary to make available the access through the traditional e-mail protocols (SMTP/POP3/IMAP4). This in order to allow, at the same time, highest security standards and to guarantee an ever-growing spread of the REM services.

The options prescribed in the standard EN 319 521 **[8]**, on the points a), b) and c) of Clause 5.2.2 aren't still sufficiently widespread in the various e-mail clients present on the market. Due to this lack of availability, the point d) of the Clause 5.2.2 of the aforementioned standard has been leveraged to identify a substantial solution to this issue applicable inside the **REM-Policy-IT** and subject to the national security practices that can restrict its usage (see § 2.6.1). Follows the illustration of the solution.

Soluzione

L'utente si deve innanzitutto autenticare in modo "forte" accedendo ad una applicazione fornita dal REMSP di riferimento - utilizzando una delle modalità previste nei punti a), b) e c) dello standard EN 319 521 **[8]**, Clause 5.2.2 - facendosi rilasciare un *token* di sicurezza (detto anche **Application Password**); tale *token* sarà inserito in un qualsiasi client di posta elettronica standard, in luogo del campo "*password*", abilitandolo così ad accedere al servizio REM attraverso l'uso esclusivo e protetto dei classici protocolli (ad es. SMTP/IMAP4 o POP3 quando fornito dal REMSP).

Le security practice da adottare (si veda il § 2.6.1) stabiliranno la lunghezza ed il periodo di validità del token (ad esempio 6 mesi), superato il quale il token dovrà essere rigenerato con il medesimo meccanismo o in alternativa con un altro meccanismo che fornisca le medesime garanzie in termini di sicurezza.

Si noti che questa modalità di accesso è applicabile limitatamente ai client utente o gli applicativi che per accedere al servizio REM possono utilizzare esclusivamente i protocolli standard (i.e. POP3, IMAP4, SMTP over SSL/TLS) per i quali non è possibile l'implementazione o l'adozione di meccanismi di autenticazione multi-fattore (**MFA**) [36]. La

Solution

The user must first authenticate in a "strong" way using an application provided by own REMSP - using one of the modalities prescribed at the points a), b), and c) of the standard 319 521 **[8]**, Clause 5.2.2 – obtaining a security *token* (also called **Application Password**). Such *token* will be configured in any standard e-mail client, at the place of the "*password*", enabling the user to access the REM service through an exclusive and protected use of the canonical e-mail protocols (e.g., SMTP/MAP4 or POP3 when provided by the REMSP).

The security practice to adopt (see § 2.6.1) will state the length and the validity period of the token (e.g., 6 months) that, after witch, a new generation of the token, with the same mechanism - or alternatively, with another mechanism that provides the same assurances - will be required.

Note that this access mode is applicable limitedly to user's clients or applications that use exclusively standard protocols to access to the REM service (i.e., SMTP, IMAP4, POP3 over SSL/TLS) for which isn't possible the implementation or the adoption of multi-factor authentication mechanisms (**MFA**)[36].The solution above is not appliable

soluzione sopra descritta non è applicabile agli applicativi "web mail", alle "API o alle app mobile proprietarie" come strumento per l'accesso alle caselle REM (si veda invece il § 2.4.2.13 che illustra delle soluzioni più appropriate basate sull'**OAuth 2.0 Authorization Framework**, per questi scopi ed in caso di accessi **M2M**).

Esempio

Viene fornito qui di seguito un esempio su come è possibile farsi rilasciare un token di sicurezza per l'accesso di un client/applicativo al servizio REMS (cioè attraverso POP3/IMAP4/SMTP over SSL/**TLS**).

1. L'utente accede ad un servizio (es. un pannello tecnico) messo a disposizione dal REMSP per la gestione dell'**utenza** e del servizio (si veda **Figure 24**).
2. L'accesso al suddetto servizio avviene tramite Strong Authentication.

In questo esempio è utilizzata una classica **MFA** (o 2FA) con username/password, seguita

to applications like "web mail" or "custom API" or "mobile apps" as mechanism to access to the REM mailboxes (see § 2.4.2.13 that shows the most suitable solutions based on the **OAuth 2.0 Authorization Framework**, for these purposes and in cases of **M2M** accesses, instead).

Example

An example on how a security token for a client application it would access to the REM service (i.e., through SMTP/IMAP4/POP3 over SSL/**TLS**) it is provided below.

1. The user logs in to a service (eg technical panel) provided by the REMSP for users and service preferences managing (see **Figure 24**).
2. The access to the aforementioned services is take place through Strong Authentication.

In this example a classic **MFA** (or 2FA) with username/password, followed by a

[36] Ad esempio, sistemi di autenticazione informatica corrispondenti al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115.

[36] For example, authentication systems corresponding to the Level of Assurance LoA3 of the ISO/IEC DIS 29115 standard.

da un secondo step che prevede l'inserimento di una "one time password" (si veda **Figure 25**) generata tramite device sicuro (o in alternativa sono possibili anche altre modalità ormai consolidate come notifica push su specifico device ecc.).

Si noti che la modalità di accesso al suddetto pannello tecnico deve essere una tra quelle previste dall'EN 319 521 **[8]**, Clause 5.2.2 (e riportate qui di seguito per comodità):

a) multi factor authentication mechanisms (**MFA**);

b) mutual **TLS** authentication, which includes advanced user's certificate;

c) advanced electronic signature

All'interno del pannello tecnico l'utente ha a disposizione una sezione specifica per abilitare l'accesso dei propri client di posta elettronica basati su protocolli standard (SMTP/IMAP4/POP3, e una volta abilitata tale opzione, l'utente ha la possibilità di generare un'**Application Password** sufficientemente robusta (nell'esempio indicata come "Client password"), che verrà utilizzata per l'accesso al REM service tramite i suddetti client (si veda **Figure 26**).

Si noti che in qualunque momento l'utente deve avere la possibilità di disabilitare l'opzione, inibendo quindi l'accesso ai client

second step which requires the input of a " one-time password" (see **Figure 25**) is used. It is required the generation of the "one-time password" by secure device (or alternatively, other now familiar ways like push notification on specific device etc. are possible).

Note that the way to access to the aforementioned technical panel must be one of the options of EN 319 521 **[8]**, Clause 5.2.2 (and summarized below for information):

a) multi factor authentication mechanisms (**MFA**);

b) mutual **TLS** authentication, which includes advanced user's certificate;

c) advanced electronic signature;

Inside the technical panel the user has a specific section to enabling the access of own e-mail client based on SMTP, POP3, IMAP4 standard protocols. Once enabled such option, the user can generate a enough robust **Application Password** ("Client password" in the example), that will be used to access to the REM service through the enabled clients (see **Figure 26**).

Note that, at any time the user must have the possibility to disable this option, by

secondo questa modalità. Inoltre, in qualunque momento, anche il REMSP, nel caso in caso di eventi critici come la sospetta compromissione della casella, può disabilitare l'opzione.

In merito alle proprietà dell'**Application Password**, ne deve essere definita una con policy idonea che rispetti linee guida e best practice a livello nazionale ed internazionale (si veda il § 2.6.1 riguardo la security practice da adottare).

L'**Application Password** così ottenuta può essere applicata, tramite copia/incolla, nel classico client di posta elettronica standard che si intende utilizzare per accedere al servizio REM (si veda **Figure 27**).

Segue l'esempio completo.

inhibiting the client access according to this method. Furthermore, at any moment, even the REMPS, in case of some critical event like the suspect of compromising of the mailbox, can disable the option.

Concerning the properties of the **Application Password**, there must be defined one with a suitable policy respecting the guidelines and best practices at national and international level (see § 2.6.1 regarding the security practices to adopt).

The **Application Password**obtained in this way can be applied, through copy/past, in the usual standard e-mail client to use to access to the REM service (see **Figure 27**).

Follows the complete example.

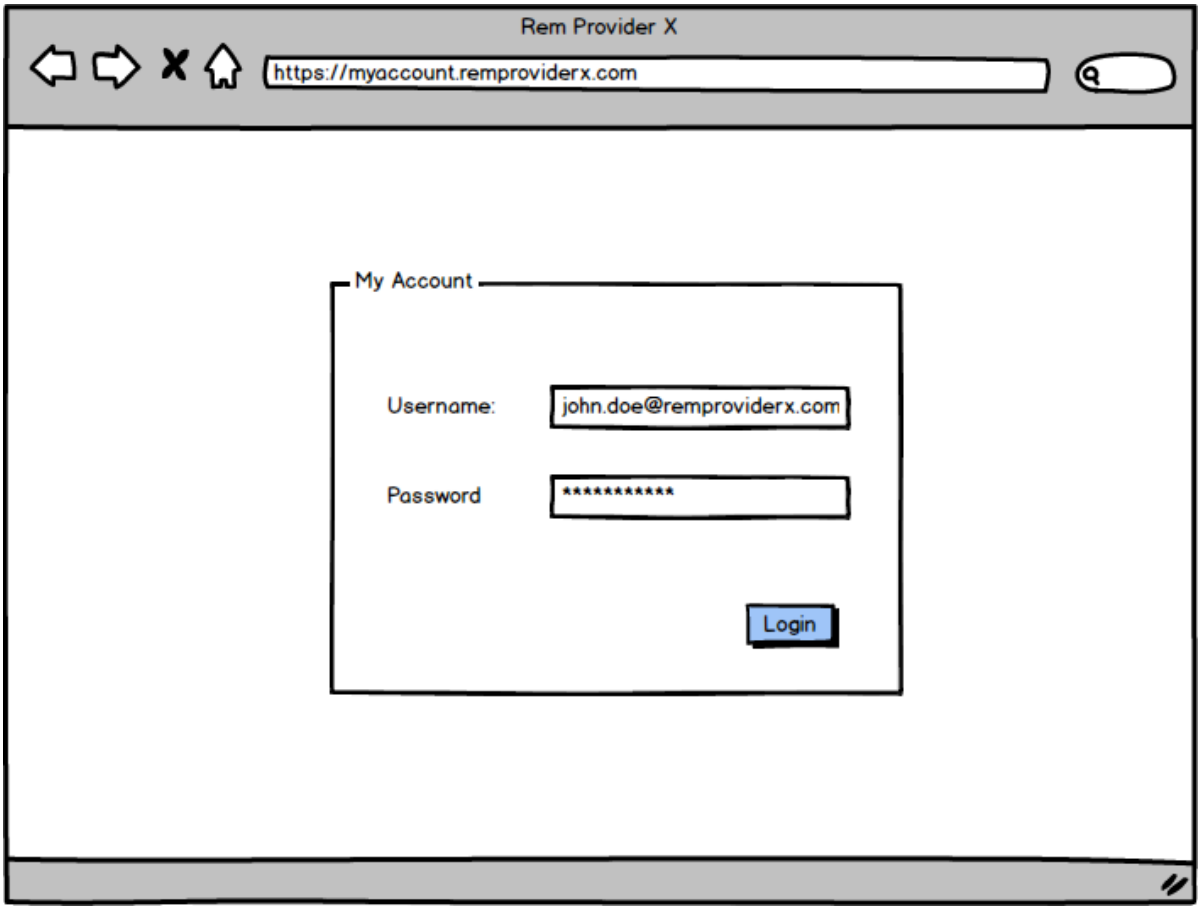


Figure 24 – User's login to the token generation service (panel)

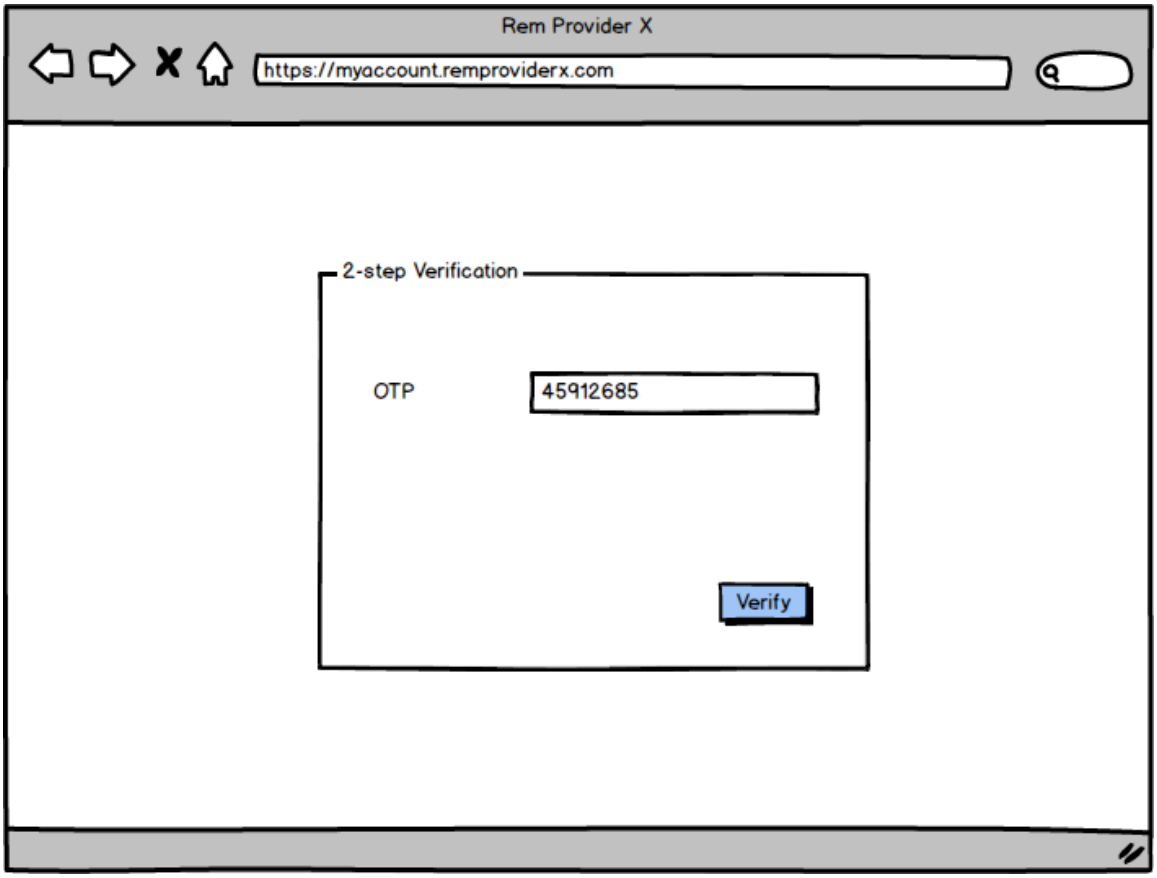


Figure 25 – Verification of the OTP for the multifactor authentication (MFA)

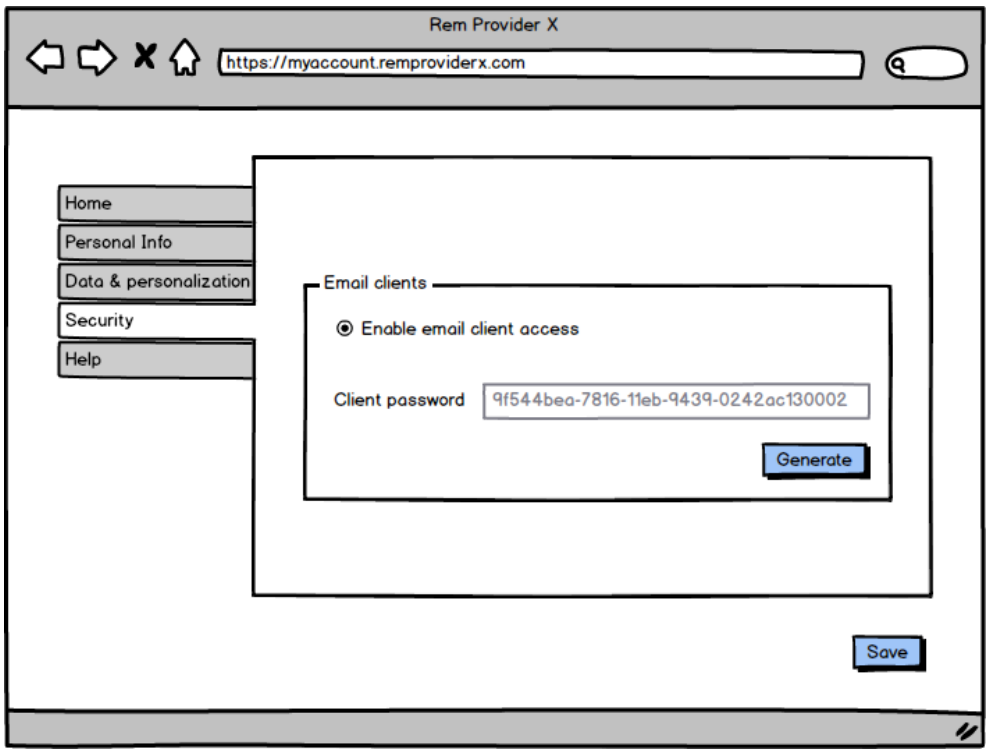


Figure 26 – Enabling client access and token generation to use as Application Password (client password)

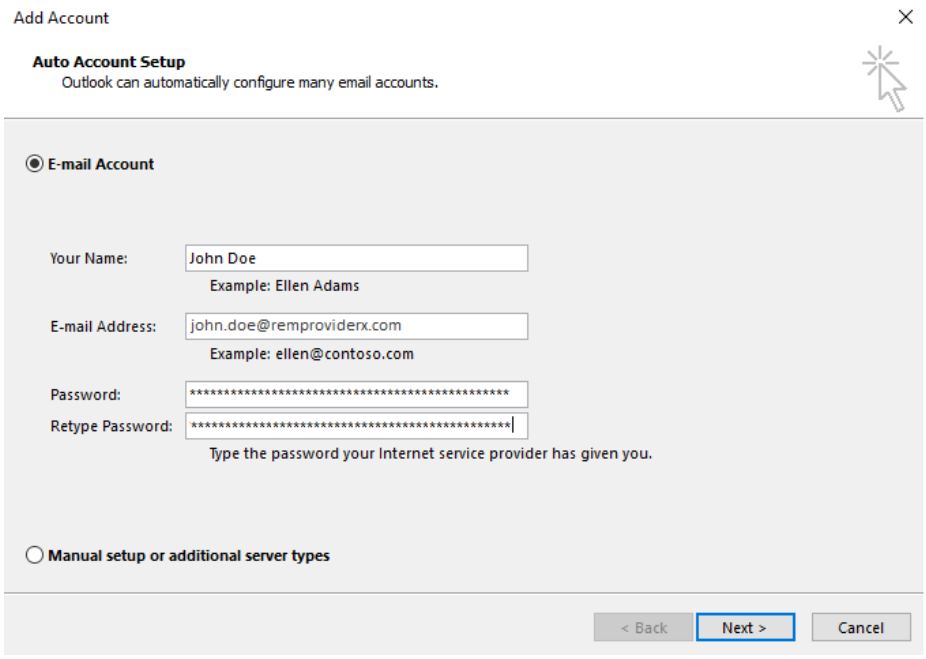


Figure 27 – Updating the password with the secure token generated on the panel

2.4.2.8 *Accurato monitoraggio del DNS | Accurate monitoring of DNS*

Il corretto monitoraggio del **DNS** è una pratica fondamentale per diagnosticare eventuali problemi, prevenire attacchi mirati e identificare prontamente violazioni di sicurezza.

Visto che la REM baseline prevede che il protocollo **DNS** sia alla base del Routing dei messaggi, è fondamentale che il REMSP adotti le corrette misure di sicurezza e monitoraggio dei sistemi/servizi basati sul **DNS** - si veda EN 319 532-4 **[4]**, Clause 5.3.5 item a).

Uno degli attacchi più comuni a cui è soggetto il DNS è ad esempio il DNS Poisoning. Questo attacco consiste nell'inserimento, da parte degli attaccanti, di informazioni false all'interno della cache del DNS Resolver. In questo modo gli attaccanti possono ridirigere la vittima verso una versione malevola di un determinato servizio, al fine ad esempio di sottrarre dei dati.

Si riportano di seguito alcune misure minime per la sicurezza del DNS, ferma restando la raccomandazione di seguire, congiuntamente, linee guida riconosciute a livello internazionale come, ad esempio, NIST Special Publication 800-81-2 **[13]** (Secure Domain Name System - Deployment Guide).

The correct monitoring of the **DNS** is a fundamental practice to detect possible problems, to prevent targeted attacks and to identify, as soon as possible, security violations.

Since the REM baseline requires that the routing of messages is based on **DNS** protocol, it is fundamental that the REMSP adopts the appropriated security measures and monitoring of the systems/services based on **DNS** - see EN 319 532-4 **[4]**, Clause 5.3.5 item a).

One of the most common attacks to the DNS occur is the DNS Poisoning. This threat consists in the injection, from some attacker, of false information inside the DNS resolver cache. In this way, the attacker can redirect the victim toward malicious version of determined service, as an example to subtract some data.

Follows some security measure for the DNS security, but taking care the recommendation to follow, jointly, international recognized guidelines like for example NIST Special Publication 800-81-2 **[13]** (Secure Domain Name System - Deployment Guide).

• Utilizzare un DNS Resolver privato opportunamente protetto da accessi esterni.

• Loggare e monitorare le attività principali relative al DNS.

• Configurare il DNS Resolver in modo che sia il più protetto possibile da influenze esterne (es. attacchi di tipo cache poisoning):

- utilizzare source port random;
- utilizzare query id random e non predicibili;
- abilitare il cache locking.

Per quanto riguarda la sicurezza delle comunicazioni tra **S-REMS** e **R-REMS** è **fondamentale** che il sender's REMSP abbia la **certezza** di contattare la ***Relay interface*** del **recipient's REMSP** (il cui indirizzo - **MX record** - è ottenuto tramite il **DNS**).

Per questa ragione il certificato digitale del *Transport Layer Security* (**TLS**) della ***Relay interface*** dell'R-REMS è "ancorato" in maniera "forte" alla Trusted List. Ciò avviene attraverso il meccanismo chiamato CapabilityAndSecurityInformation referenziato dalla **TL** - si veda EN 319 532-4 **[4]**, Clause C.2.3.4.4 item c.3.4.1) and NOTE 1, item c.3.5.1) and NOTE 2. Inoltre, la **REM-Policy-IT** prevede che il file

• Use of a private DNS Resolver properly protected from external access.

• Logging and monitoring of the main activities relevant to the DNS.

• Configure the DNS Resolver in way that it is protected from outside influence (e.g. cache poisoning attacks) as much as possible:

- using source port random;
- using random and not predictable query id;
- enabling cache locking.

Regarding the security of the communication between **S-REMS** and **R-REMS** it **fundamental** that the sender's REMSP is **certain** to contact the ***Relay interface*** of **recipient's REMSP** (whose address - **MX record** - is obtained through the **DNS**).

For this purpose, the *Transport Layer Security* (**TLS**) digital certificate of the R-REMS ***Relay interface*** is "anchored" in a "strong" way to the Trusted List. That is obtained through the CapabilityAndSecurityInformation mechanism that is referenced from the **TL** - see EN 319 532-4 **[4]**, Clause C.2.3.4.4 item c.3.4.1) and NOTE 1, item c.3.5.1) and NOTE 2. Furthermore, the **REM-Policy-IT** requires

CapabilityAndSecurityInformation.xml di ciascun REMS (contenente il certificato digitale **TLS** della ***Relay interface***) sia firmato digitalmente in accordo a quanto prescritto nel § 2.3.2.4.

Ed ovviamente, come specificato più nel dettaglio nel § 2.4.2.15, sempre per la stessa ragione di **certezza** di contattare la ***Relay interface*** del **recipient's REMSP**, il **TLS handshake** tra REMSP **DEVE** ovviamente **ATTIVARSI** nella sua completezza. In altre parole, il **TLS** DEVE ESSERE **RICHIESTO** (lato S-REMS) e **ONORATO** (lato R-REMS); e casomai non fosse così, il tentativo di handshake deve essere immediatamente **ABORTITO** (es. con alert fatal handshake failure; si veda nota[37] a pag. **Errore. Il segnalibro non è definito.**). Questo requisito è chiaramente implementabile, trattandosi di comunicazione regolata attraverso la ***Relay interface*** di **entità "trusted"** (e non utenti qualsivoglia). Come rimarcato al capoverso precedente, il certificato digitale **TLS** è protetto in quanto inserito nel file `CapabilityAndSecurityInformation.xml` (che è firmato digitalmente come prescritto nel § 2.3.2.4). Si noti che la relativa chiave è da proteggere così come avviene per i certificati digitali **TLS** di analoghi servizi (si veda il § 2.4.2.15).

that the file CapabilityAndSecurityInformation.xml of any REMS (containing the ***Relay interface*** **TLS** digital certificate) is digitally signed according to the prescriptions of § 2.3.2.4.

And of course, as detailed in § 2.4.2.15, always for the same purpose of **certainty** to contact the ***Relay interface*** of **recipient's REMSP**, the **TLS handshake** between REMSP **MUST** obviously **TAKE PLACE** in its completeness. In other words, the **TLS** MUST BE **REQUESTED** (S-REMS side) and **HONORED** (R-REMS side); whereas if it does not occur, the handshake attempt must be immediately **ABORTED** (e.g., through a fatal handshake failure alert; see note[37] at pag. **Errore. Il segnalibro non è definito.**). This requirement is clearly feasible, since it refers to a communication regulated through the ***Relay interface*** of **"trusted" entities** (and not whatever users). As pointed out in the previous paragraph, the **TLS** digital certificate is protected as it inserted in the `CapabilityAndSecurityInformation.xml` file (which is digitally signed as prescribed in § 2.3.2.4). Note that the relevant key has to be protected similarly as for **TLS** digital certificate of same type of services (see § 2.4.2.15).

Ulteriori misure potranno essere man mano predisposte in accordo alle evoluzioni delle security practice nazionali che ne potranno ampliare e perfezionare l'attuazione (si veda il § 2.6.1). A titolo esemplificativo, il recente standard IETF RFC 8460 **[19]** offre preziosi spunti che possono essere trasposti nel campo del monitoring del **DNS** nella REM, così come usato nella REM baseline.

Further measures can be gradually arranged according to the national security practices evolutions that can even more fine-tune and improve the application. By way of example, the recent IETF RFC 8460 **[19]** standard offers valuable ideas on DNS monitoring that can be transposed in REM, according to the actual usage of **DNS** in REM baseline (see § 2.6.1).

2.4.2.9 Gestione e messaggi malevoli | Management of messages with Malware

In questa sezione vengono descritte le pratiche adottate dalla **REM-Policy-IT** per la gestione dei messaggi con contenuto malevolo. Tali pratiche sono in linea con quanto previsto da EN 319 522-2 **[6]** e EN 319 532-3 **[3]** e non impattano l'interoperabilità con REMSP che non adottino la **REM-Policy-IT**.

Inoltre, nella specifica della REM baseline (EN 319 532-4 **[4]**, Clause C.4.5.1, C.4.5.2 e C.4.5.3, nell'item h) sub-item I. e II.) è riportata la seguente nota alla quale la presente sezione dà una risposta

<<NOTE 1: In both cases I. and II. above, there can be additional rules in local REMID policy that dispose particular preservations and/or practices on the REM dispatch in case of "security violations and threats" that are specified in the policy

The present section describes the practices used in **REM-Policy-IT** for managing messages with content affected by malware. These practices are compliant with EN 319 522-2 **[6]** and EN 319 532-3 **[3]** and do not introduce interoperability impacts towards REMSPs not adopting the **REM-Policy-IT**.

Furthermore, in the REM baseline specification (EN 319 532-4 **[4]**, Clause C.4.5.1, C.4.5.2 and C.4.5.3, in the item h) sub-items I. and II.) there is also the following note to which the present section gives an answer.

<<NOTE 1: In both cases I. and II. above, there can be additional rules in local REMID policy that dispose particular preservations and/or practices on the REM dispatch in case of "security violations and threats" that are specified in the policy

(see clause C.2.3.5). Anyway, any of this "additional" practice doesn't break the interoperability>>

I REMSP aderenti alla **REM-Policy-IT** devono verificare che i messaggi inviati/ricevuti non contengano malware.

I controlli vanno quindi sempre effettuati come segue:

- in fase di invio: verificando che l'*original message* sottomesso dal mittente all'S-REMS non abbia contenuto malevolo (=> controllo a carico del sender's REMSP);
- in fase di ricezione: verificando che il REM dispatch trasmesso dall'S-REMS all'R-REMS non abbia contenuto malevolo => controllo a carico del recipient's REMSP).

I REMSP, per l'identificazione dei malware, possono avvalersi di differenti soluzioni di Protezione Anti-Malware in successione, in osservanza alle "security-practice" vigenti (si veda § 2.6.1).

La gestione del Malware (che quando rilevato dagli appositi sistemi è gestito come indicato nel seguito) segue un flusso differente a seconda che la rilevazione venga effettuata dal sender's REMSP o dal recipient's REMSP, come evidenziato in **Figure 29** e **Figure 32**.

Ogni evento relativo alla rilevazione dei Malware è gestito tramite la generazione di una o più REMS receipt, ognuna, a sua volta,

(see clause C.2.3.5). Anyway, any of this "additional" practice doesn't break the interoperability>>

The REMSPs adhering to the **REM-Policy-IT** must verify that the messages sent/received do not contain any malware.

These checks must be done as follows:

- Sending phase: checking that the *original message* submitted by the sender to S-REMS doesn't contain malicious content (=> this is a control under the responsibility of the sender's REMSP);
- Incoming phase: checking that the REM dispatch transmitted from S-REMS to R-REMS doesn't contain malicious content (=> this is a control under the responsibility of recipient's REMSP).

The REMSPs, can use multiple Anti-Malware Protection solutions in series, for malware detection, in observance of the "security-practices" in force (see § 2.6.1).

Malware management (that when detected by the appropriate antiabuse systems it is managed by following the step below) follows a different flow depending on the detection occurs at sender's REMSP or at recipient's REMSP, as outlined in **Figure 29** and **Figure 32**.

Every event related to a Malware detection is managed through the generation of one or more REMS receipts,

contenente l'ERDS Evidence appropriata in accordo ai dettagli che seguono.

Malware rilevato dal sender's REMSP

Nel caso di Malware rilevato dal sender's REMSP, è generata una REMS receipt con allegata una ERDS Evidence caratterizzata come dal seguente stralcio esemplificativo ed i valori della **Table 11**.

L'evento di **SubmissionRejection** viene restituito al mittente tramite REMS receipt.

each, in turn, containing the appropriate ERDS Evidence according to the following details.

Malware detected by the sender's REMSP

In case of Malware detected by the sender's REMSP, a REMS receipt with attached an ERDS Evidence is generated as for the following excerpt and the values of **Table 11**.

The **SubmissionRejection** is sent back to the sender through a REMS receipt.

```
<tns:Evidence …>
    ...
    <tns:ERDSEventId>http://uri.etsi.org/19522/Event/SubmissionRejection</tns:ERDSEventId>
    <tns:EventReasons>
        <tns:EventReason>
            <Code>http://uri.etsi.org/19522/EventReason/MalwareFound</Code>
            <Details>RA03</Details>
            <Details>Malware found in ERD original message</Details>
            <Details>...(*)</Details>
        </tns:EventReason>
    </tns:EventReasons>
    ...
</tns:Evidence>
```

Figure 28 – SubmissionRejection for Malware ERDS evidence excerpt

Table 11 – S-REMS - Values to use for Malware (direct case)

Id	Element:	Value	Reference
MDD1	ERDSEventId:	http://uri.etsi.org/19522/Event/**SubmissionRejection**	EN 319 522-3 **[7]**, Table 2
MDD2	EventReason/Code	http://uri.etsi.org/19522/EventReason/**MalwareFound**	EN 319 522-3 **[7]**, Table 3
MDD3	EventReason/Details	**RB03**	EN 319 522-2 **[6]**, Table 8
MDD4	EventReason/Details	Malware found in ERD *original message*	EN 319 522-2 **[6]**, Table 8
MDD5	EventReason/Details	Further details	Free custom text (optional) **(*)**

(*) E.g., details on malware. See also Row PP24 of Table 2.

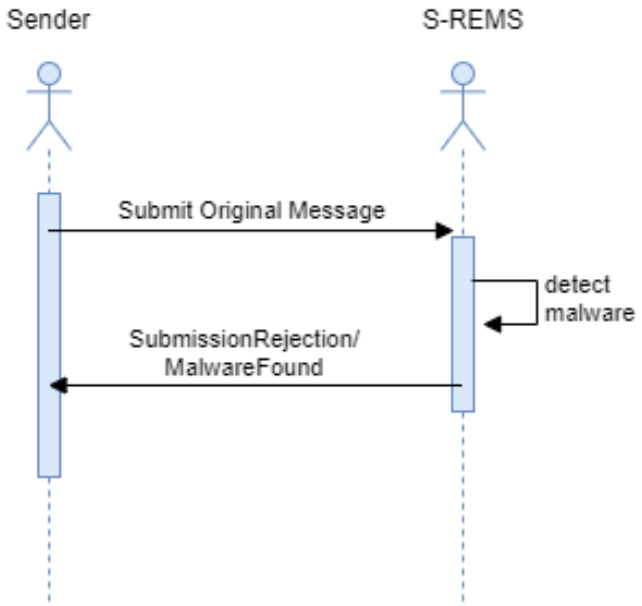


Figure 29 – Malware detected by S-REMS

Malware rilevato dal recipient's REMSP

Nel caso di Malware rilevato dall'REMSP del destinatario, questo genera una prima ricevuta/evento verso il sender's REMSP (*RelayRejection*) che, a sua volta, trasmette una REMS receipt al mittente stesso (*RelayFailure*).

Di seguito le caratteristiche principali della ERDS evidence restituita dal recipient's REMSP al sender's REMSP come illustrato nello stralcio esemplificativo di **Figure 30** e i valori in **Table 12**.

Malware detected by recipient's REMSP

In case of Malware detected by the recipient's REMSP, a first receipt/event is generated towards the sender's REMSP (*RelayRejection*) that, in turn, sends another REMS receipt to the sender itself (*RelayFailure*).

Following there are the main ERDS evidence characteristics sent back from the recipient's REMSP to the sender's REMSP as exemplified in the excerpt in **Figure 30** and with the values in **Table 12**.

```
<tns:Evidence …>
    ...
    <tns:ERDSEventId>http://uri.etsi.org/19522/Event/RelayRejection</tns:ERDSEventId>
    <tns:EventReasons>
        <tns:EventReason>
            <Code>http://uri.etsi.org/19522/Event/R_ERDS_MessageRejectedForMalware</Code>
            <Details>RB03</Details>
            <Details>ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for:
Malware found in ERD message</Details>
            <Details>...(*)</Details>
        </tns:EventReason>
    </tns:EventReasons>
    ...
</tns:Evidence>
```

Figure 30 – RelayRejection for Malware ERDS evidence excerpt

Table 12 – R-REMS - Values to use for Malware (indirect case)

Id	Element:	Value	Reference
MID1	ERDSEventId:	http://uri.etsi.org/19522/Event/**RelayRejection**	EN 319 522-3 **[7]**, Table 2
MID2	EventReason/Code	http://uri.etsi.org/19522/EventReason/**R_ERDS_MessageRejectedForMalware**	EN 319 522-3 **[7]**, Table 3
MID3	EventReason/Details	**RB03**	EN 319 522-2 **[6]**, Table 8
MID4	EventReason/Details	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Malware found in ERD message	EN 319 522-2 **[6]**, Table 8
MID5	EventReason/Details	Further details	Free custom text (optional) **(*)**

(*) E.g., details on malware. See also Row PP24 of Table 2.

```
<tns:Evidence …>
    ...
<tns:ERDSEventId>http://uri.etsi.org/19522/Event/RelayFailure</tns:ERDSEventId>
    <tns:EventReasons>
        <tns:EventReason>
            <Code>http://uri.etsi.org/19522/Event/R_ERDS_MessageRejectedForMalware</Code>
            <Details>RB03</Details>
            <Details>ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for:
Malware found in ERD message</Details>
            <Details>...(*)</Details>
        </tns:EventReason>
    </tns:EventReasons>
    ...
</tns:Evidence>
```

Figure 31 – RelayFailure for Malware ERDS evidence excerpt

Table 13 – S-REMS - Values to use for Malware (indirect case)

Id	Element:	Value	Reference
MID6	ERDSEventId:	http://uri.etsi.org/19522/Event/**RelayFailure**	EN 319 522-3 **[7]**, Table 2
MID7	**EventReason/Code**	http://uri.etsi.org/19522/EventReason/**R_ERDS_MessageRejectedForMalware**	EN 319 522-3 **[7]**, Table 3
MID8	EventReason/Details	**RA03**	EN 319 522-2 **[6]**, Table 7
MID9	EventReason/Details	ERD message successfully relayed to, but rejected by, the Recipient's ERDSP for: Malware found in ERD message	EN 319 522-2 **[6]**, Table 8
MID10	EventReason/Details	Further details	Free custom text (optional) **(*)**

(*) E.g., details on malware. See also Row PP24 of Table 2.

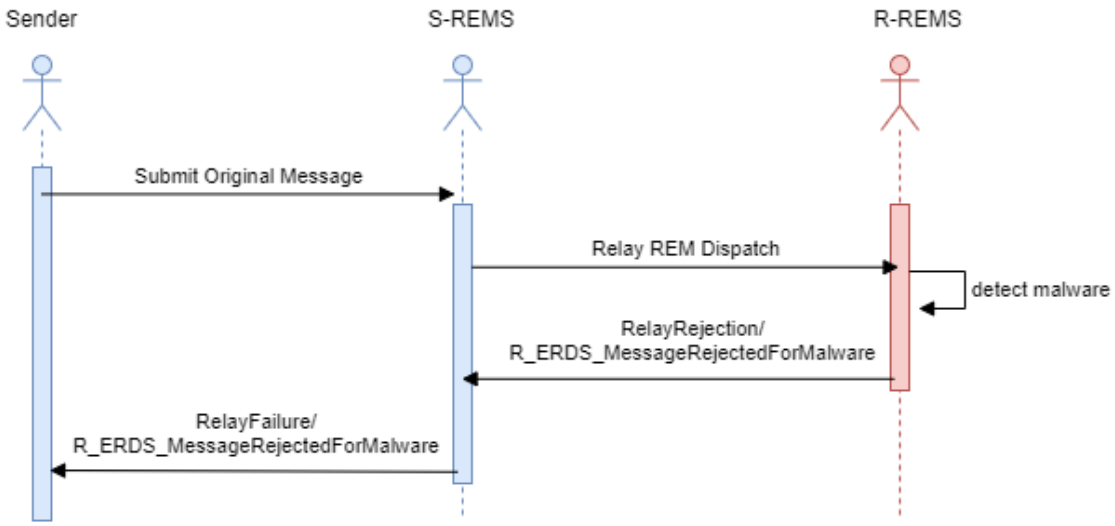


Figure 32 – Malware detected by R-REMS

2.4.2.10 Formato Subject e nome XML ERDS evidence | Subject format and ERDS evidence XML name

Come riportato al punto "Z REMS relay metadata MIME Header Fields Table 3: Subject" al § 4.3.4, pag. 59 del documento base, il **REMID policy** definito dalla **REM-Policy-IT** prevede la copia del subject dell'*original message* su tutti i REM message ad esso correlati. Tale riproduzione è distinta da un apposito prefisso, come da raccomandazione dello standard (si veda EN 319 532-3 **[3]**, Table 3). Inoltre, è parimenti prevista una rielaborazione del subject anche per i flussi da/verso sistemi esterni alla **REM baseline**, con delle regole definite e valide all'interno della **REM-Policy-IT**.

Tali regole prevedono una corrispondenza diretta tra il nome dell'evento generatore del REM message e l'ERDS evidence allegata (si veda il punto "EEE REM EVIDENCE NAME" al § 4.3.4, pag. 76 del documento base). La seguente **Table 14** definisce il mapping completo.

How per the point "Z REMS relay metadata MIME Header Fields Table 3: Subject" at § 4.3.4, pag. 59 of the basic document, the **REMID policy** defined through the **REM-Policy-IT** requires a copy of the subject of the original *message* to any REM message related to it. Such reproduction is distinguished through a specific prefix as per the standard recommendation (see EN 319 532-3 **[3]**, Table 3). In addition, it is similarly defined a mapping of the subject also for messages exchanged from/to systems external to the **REM baseline**, with rules defined and valid inside the **REM-Policy-IT**.

Such rules define a direct mapping between the event name generator of the REM message and the attached ERDS evidence (see point "EEE REM EVIDENCE NAME" at § 4.3.4, pag. 76 of the basic document). See **Table 14** for the full mapping.

Come indicato in **Table 3,** code **E01,** implementazione **I-E01s**, si tenga anche in considerazione che il subject dell'*original message* deve essere riprodotto "intatto" all'interno dell'ERDS evidence nell'apposita estensione, così come specificato nella **REM baseline** in EN 319 532-4 **[4]**, Clause C.3.2.1, item b) and Figure C.3.

Furthermore, as per **Table 3,** code **E01,** implementation **I-E01s**, consider also that the subject of the *original message* must be set "untouched" inside the appropriate ERDS evidence extension, as specified in the **REM baseline** in EN 319 532-4 **[4]**, Clause C.3.2.1, item b) and Figure C.3.

Table 14 – Subject and Evidence formats in REM-Policy-IT

Id	Subject:	REM_EVIDENCE_NAME	Note
SEF1	**REM SubmissionAcceptance**: <orig subj>	**SubmissionAcceptance**.xml	REMS receipt for the sender
SEF2	**REM SubmissionRejection**: <orig subj>	**SubmissionRejection**.xml	REMS receipt for the sender
SEF3	**REM dispatch**: <orig subj>	**SubmissionAcceptance**.xml	REM dispatch for the recipient(s)
SEF4	**REM ContentConsignment**: <orig subj >	**ContentConsignment**.xml	REMS receipt for the sender
SEF5	**REM ContentConsignmentFailure**: <orig subj >	**ContentConsignmentFailure**.xml	REMS receipt for the sender
SEF6	**REM RelayAcceptance**: <orig subj >	**RelayAcceptance**.xml	REMS receipt for S-REMS
SEF7	**REM RelayRejection**: <orig subj >	**RelayRejection**.xml	REMS receipt for S-REMS
SEF8	**REM RelayFailure**: <orig subj >	**RelayFailure**.xml	REMS receipt for the sender
SEF9	**REM EXTERNAL**: <orig subj >	**ReceivedFromNonERDS**.xml	REM dispatch for the recipient(s)
SEF10	**REM RelayToNonERDS**: <orig subj >	**RelayToNonERDS**.xml	REMS receipt for the sender
SEF11	**REM RelayToNonERDSFailure**: <orig subj >	**RelayToNonERDSFailure**.xml	REMS receipt for the sender

2.4.2.11 Certificati digitali | Digital certificates

Le firme digitali degli esempi allegati (si veda § 2.7) sono state realizzate utilizzando una catena gerarchica di tre certificati digitali in accordo alle seguenti convenzioni.

- Utilizzato lo stesso certificato digitale "foglia" per firmare sia gli XML che rappresentano ERDS evidence (firma **XAdES-B-T**), sia gli EML che rappresentano i REM message (firma **S/MIME CAdES-B-B**), e deve avere l'extension X509v3 Subject Alternative Name (**SAN**) come indicato in **PP6** della **Table 2** § 2.3.1 e **AP4** della **Table 4** § 2.4.1.

The digital signature of the attached examples (see § 2.7) are based on a hierarchical chain of digital certificates according to the following conventions.

- Used the same "leaf" digital certificate to sign both the XMLs representing any ERDS evidence (**XAdES-B-T** digital signature), and the EMLs representing any REM message (**S/MIME CAdES-B-B** digital signature), and must have the extension X509v3 Subject Alternative Name

- Tale certificato "foglia" è l'ultimo di una catena di tre certificati composti da una *root CA* e una *intermediate CA* (in accordo alla struttura riportata nella best practice della **REM baseline** in EN 319 532-4 **[4]**, Clause D.2.2.2).

La suddetta struttura è esemplificata in **Figure 33** e **Figure 34**. Si noti che in **Figure 34** (ad es. per le CPS extension) sono riportate esclusivamente delle policy utilizzate per gli ESEMPI, che quindi non rappresentano un vincolo per il certificato che utilizzerà il **REMSP**. Gli esempi di certificati digitali di **Figure 34** sono una rappresentazione ottenuta mediante l'opzione *text form* (`-text`) dell'utility `openssl x509` che ha l'intento di agevolare il lettore nell'individuazione immediata di tutti i parametri essenziali. Tale rappresentazione va però interpretata in accordo alle convenzioni che l'`openssl x509` utilizza nel formato *text form* (es. l'estensione *X509v3 Subject Alternative Name* - **SAN -** che sappiamo essere di tipo **`rfc822Name`,** è convenzionalmente rappresentata dal tag **`email:`** ma con la medesima semantica).

(**SAN**) as outlined in **PP6 Table 2** § 2.3.1 and **AP4** of **Table 4** § 2.4.1.

- Such "leaf" certificate is the last of a chain of three certificates composed by a *root CA* and an *intermediate CA* (according to the best practice of the **REM baseline** in EN 319 532-4 **[4]**, Clause D.2.2.2).

This structure is exemplified in **Figure 33** and **Figure 34**. Note that **Figure 34** (e.g. in CPS extensions) illustrates only the policies used for the EXAMPLES, which not represent a strong requirement for the certificate that will be used by the **REMSP**. The digital certificate examples in **Figure 34** are a pretty print representation obtained by the *text form* (`-text`) option of `openssl x509` utility, aiming to make it easier for the reader in the immediate detection of all certificate essential parameters. This representation has to be interpreted according to the conventions that `openssl x509` uses in the *text form* output (e.g., the *X509v3 Subject Alternative Name* extension - **SAN** - which is of type **`rfc822Name`** is conventionally represented by the tag **`email:`** but with the same semantic).

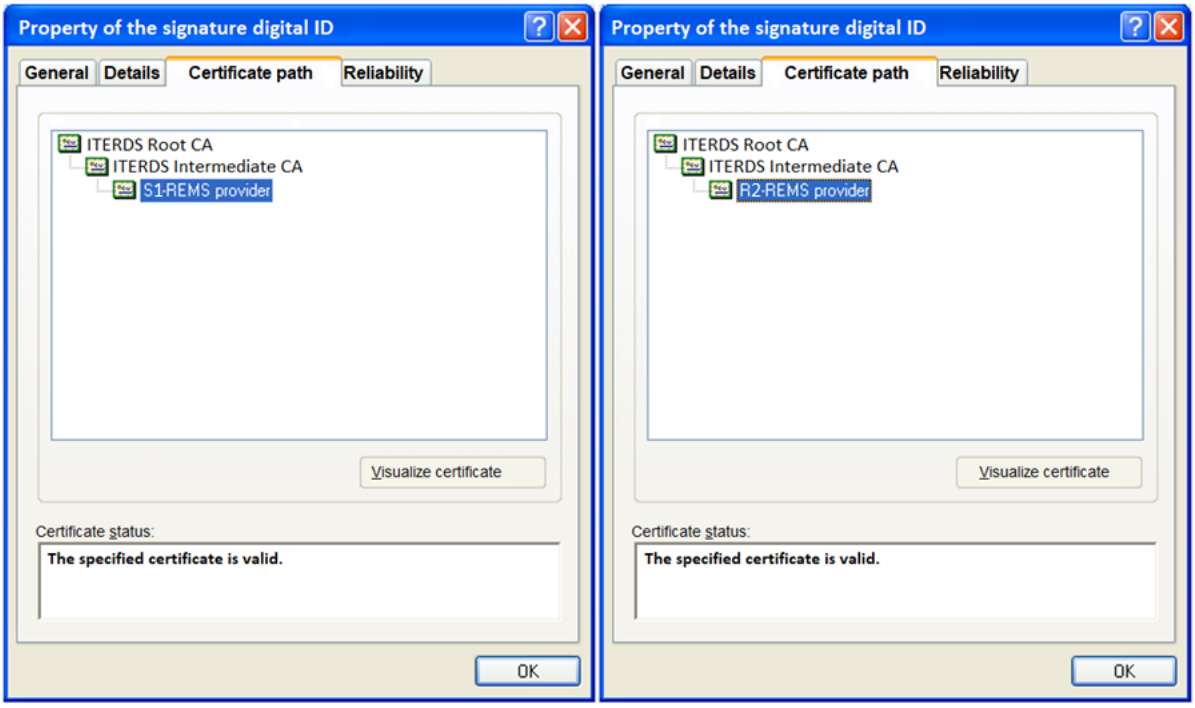


Figure 33 – Digital certificates: hierarchical chain for S-REMS and R-REMS

ITERDS_REM_test_services_S1-REMS_provider.crt

```
            Issuer: C=IT, O=ITERDS, OU=ITERDS test services, CN=ITERDS Intermediate CA
            Subject: C=IT, O=ITERDS, OU=ITERDS test services, CN=S1-REMS provider
            X509v3 extensions:
                X509v3 Subject Key Identifier:
                    ...
                X509v3 Authority Key Identifier:
                    keyid:...

                X509v3 Key Usage: critical
                    Digital Signature
                X509v3 Extended Key Usage:
                    E-mail Protection
                X509v3 Subject Alternative Name:
                    email:rem-service@s1-rems-only-for-test.it
                X509v3 Certificate Policies:
                    Policy: 0.4.0.19522.1.1
                      CPS: http://uri.etsi.org/19522/v1#/ERDSEvidence/certificate-policy
                      User Notice:
                        Organization: IT AgID supervision authority
                        Number: 1
                        Explicit Text: Test certification policy example defined for ERDS evidence by
supervision authority of country IT
                    Policy: 0.4.0.19532.1.1
                      CPS: http://uri.etsi.org/19532/v1#/REMbaseline/certificate-policy
                      User Notice:
                        Organization: IT AgID supervision authority
                        Number: 1
                        Explicit Text: Test certification policy example defined for REM baseline by
supervision authority of country IT
                    Policy: 0.4.0.19532.1.1
                      CPS: https://eidas.agid.gov.it/REM/rem-policy-it#certificate-policy
                      User Notice:
                        Organization: IT AgID REMID authority
                        Number: 1
                        Explicit Text: Test certification policy example defined for REM-Policy-IT by
REMID authority of country IT
```

ITERDS_REM_test_services_R2-REMS_provider.crt

```
            Issuer: C=IT, O=ITERDS, OU=ITERDS test services, CN=ITERDS Intermediate CA
            Subject: C=IT, O=ITERDS, OU=ITERDS test services, CN=R2-REMS provider
            X509v3 extensions:
                X509v3 Subject Key Identifier:
                    ...
                X509v3 Authority Key Identifier:
                    keyid:...

                X509v3 Key Usage: critical
                    Digital Signature
                X509v3 Extended Key Usage:
                    E-mail Protection
                X509v3 Subject Alternative Name:
                    email:rem-service@r2-rems-only-for-test.it
                X509v3 Certificate Policies:
                    Policy: 0.4.0.19522.1.1
                      CPS: http://uri.etsi.org/19522/v1#/ERDSEvidence/certificate-policy
                      User Notice:
                        Organization: IT AgID supervision authority
                        Number: 1
                        Explicit Text: Test certification policy example defined for ERDS evidence by
supervision authority of country IT
                    Policy: 0.4.0.19532.1.1
                      CPS: http://uri.etsi.org/19532/v1#/REMbaseline/certificate-policy
                      User Notice:
                        Organization: IT AgID supervision authority
                        Number: 1
                        Explicit Text: Test certification policy example defined for REM baseline by
supervision authority of country IT
                    Policy: 0.4.0.19532.1.1
                      CPS: https://eidas.agid.gov.it/REM/rem-policy-it#certificate-policy
                      User Notice:
                        Organization: IT AgID REMID authority
                        Number: 1
                        Explicit Text: Test certification policy example defined for REM-Policy-IT by
REMID authority of country IT
```

ITERDS_test_services_Intermediate_CA.crt

```
Issuer: C=IT, O=ITERDS, OU=ITERDS test services, CN=ITERDS Root CA
Subject: C=IT, O=ITERDS, OU=ITERDS test services, CN=ITERDS Intermediate CA
    X509v3 Key Usage:
        Certificate Sign, CRL Sign
    X509v3 Subject Key Identifier:
        ...
    X509v3 Authority Key Identifier:
        keyid:...

    X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
    X509v3 Certificate Policies:
        Policy: 0.4.0.19522.1.1
          CPS: http://uri.etsi.org/19522/v1#/ERDS/certificate-policy
            Organization: IT AgID supervision authority
            Number: 1
            Explicit Text: Test certification policy example defined for ERDS services by
supervision authority of country IT
        Policy: 0.4.0.19522.1.1
          CPS: http://uri.etsi.org/19522/v1#/ERDSEvidence/certificate-policy
            Organization: IT AgID supervision authority
            Number: 1
            Explicit Text: Test certification policy example defined for ERDS evidence by
supervision authority of country IT
```

ITERDS_test_services_Root_CA.crt

```
Issuer: C=IT, O=ITERDS, OU=ITERDS test services, CN=ITERDS Root CA
Subject: C=IT, O=ITERDS, OU=ITERDS test services, CN=ITERDS Root CA
X509v3 extensions:
    X509v3 Key Usage:
        Certificate Sign, CRL Sign
    X509v3 Subject Key Identifier:
        ...
    X509v3 Authority Key Identifier:
        keyid:...

    X509v3 Basic Constraints: critical
        CA:TRUE
```

Figure 34 – Digital certificates: Main properties (test certificates used for the EXAMPLES)

Per il servizio di produzione, la **REM-Policy-IT** prevede che la catena di certificati realizzi un sistema di *cross-certification* che vede ovviamente coinvolta la EU Trusted List (**TL** da qui in avanti). Come evidenziato in **Figure 35** le proprietà fondamentali sono:

- classica *catena di certificati* digitali a tre livelli: *root CA, intermediate CA, certificato foglia di firma*;
- presenza della *root CA* nella lista dei certificati di root *pre-installati* nei più

The **REM-Policy-IT** requires that, for the production service, the digital certificate chain is part of a *cross-certification* system, involving the EU Trusted List (**TL** hereinafter). As outlined in **Figure 35** the main properties are:

- canonical three level digital *certificate chain*: *root CA, intermediate CA, digital signature leaf certificate*;
- presence of the *root CA* in the set of root certificates *pre-installed* in the more

comuni Browser e Sistemi Operativi come *usability trust anchor*;

- presenza del *certificato "foglia"* che firma digitalmente le ERDS evidence e i REM message all'interno della **TL**, come *qualification trust anchor*.

common Browsers and Operating Systems, as *usability trust anchor*;

- Presence of the *leaf certificate* used to digital sign any ERDS evidence and the REM messages inside the **TL**, as *qualification trust anchor*.

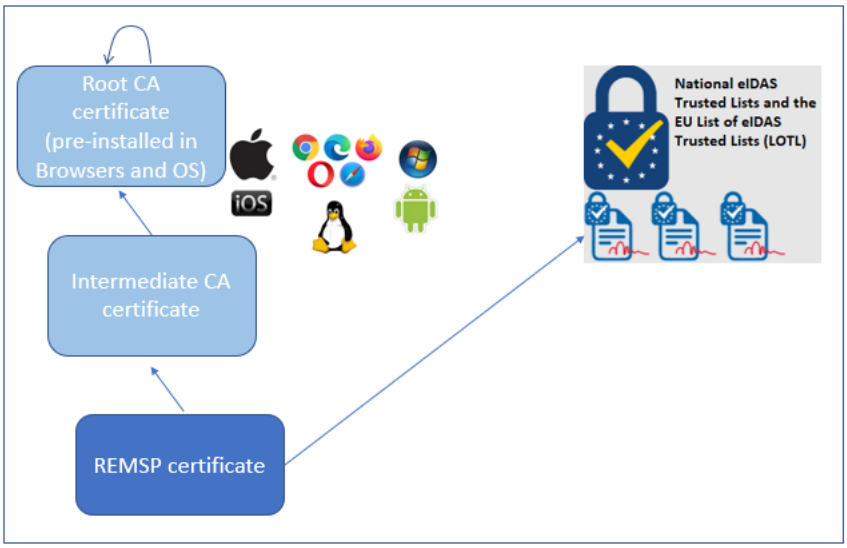


Figure 35 – Digital certificates: cross-certification system

Per realizzare il *qualification trust anchor* è necessario che il certificato "foglia" venga assicurato nell'*element* <ServiceDigitalIdentity> della **TL** così come specificato nella REM baseline in EN 319 532-4 **[4]**, Clause C.2.3.3.2, item b.2.3.1).

Mentre come *usability trust anchor*, nel caso in cui il certificato dell'*intermediate CA* non sia tra quelli *pre-installati* nei più comuni Browser e Sistemi Operativi OS questo viene

To realize the *qualification trust anchor* is necessary that the "leaf" certificate is ensured in the <ServiceDigitalIdentity> *element* of the **TL** as specified in REM baseline in EN 319 532-4 **[4]**, Clause C.2.3.3.2, item b.2.3.1).

Whereas, as *usability trust anchor* and to allow the re-composition of the entire chain, the *intermediate CA* certificate is attached to digital signature together the *leaf certificate*,

allegato alla firma digitale assieme al certificato "foglia" per permettere la ricomposizione dell'intera catena.

Si noti che il certificato utilizzato dal REMSP per la firma digitale dei REM message e delle ERDS evidence ha una durata limitata. All'approssimarsi della scadenza tale certificato dovrà essere sostituito con uno nuovo. Durante le interazioni tra i REMSP deve essere considerato valido solo l'ultimo certificato emesso per un determinato REMSP. Si pone tuttavia il problema della verifica della firma dei REM message e delle ERDS evidence sottoscritte con i vecchi certificati, e quindi più in generale della memorizzazione dello storico dei certificati utilizzati nel tempo da un REMSP per le suddette firme digitali.

La REM baseline prevede che il certificato di firma dei REM message e delle ERDS evidence XML sia all'interno della **TL**, nella sezione dedicata alla definizione del servizio REM (TSPService con identificativo tipologia di servizio http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q).

Allo stesso modo, per la memorizzazione dei certificati utilizzati in precedenza verranno utilizzati gli elementi TSPService della **TL** di tipo http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q, ma **senza** la sezione ServiceSupplyPoints (contenente i riferimenti alla ***Relay interface*** e

when it is not among the *pre-installed* certificates in the more common Browsers and Operating Systems.

Note that the certificate used by any REMSP to sign REM Messages and any ERDS evidence has a limited period of validity. When the certificate is about to expire, it must be replaced with a new one. During the interactions between REMSPs, only the last certificate issued for each REMSP has to be taken into account.

However, there could be the need of verify REM messages and ERDS evidence signed with old digital certificates, and more generally of keeping track of the history of all certificates used over time by a REMSP for the aforementioned digital signatures.

The REM baseline foresees that the certificate used to sign REM Messages and ERDS evidence XMLs is placed within the **TL** in the section containing the REM Service Definition (TSPService identifier: http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q).

Similarly, for keeping track of certificates used previously, they will be used TSPService **TL** elements with type http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q, but **without** the ServiceSupplyPoints section (containing the references to the ***Relay***

ai CapabilityAndSecurityMetadata). In questo modo una sola entry con TSPService di tipo REM/Q sarà quella candidata alla gestione del dialogo tra REMSP, come definito nelle specifiche della Common Service Interface, mentre le altre saranno utilizzate per memorizzare lo storico dei certificati utilizzati in precedenza.

Questo metodo è quello tecnico "operativo" adottato nell'ambito della **REM-Policy-IT** che consente di mantenere la continuità di servizio. Accanto a questo ve ne potrà essere uno formale (che potrà eventualmente essere definito nel dettaglio nelle note relative alle security practice nazionali, e utile al consolidamento dell'informazione storica della Trusted List) in sintonia alle best practice degli altri paesi europei. Entrambi i metodi sono soggetti agli aggiornamenti delle security practice nazionali che potranno perfezionarne l'attuazione (si veda il § 2.6.1)

interface and the Capability and Security Metadata). In this way, only a single entry of TSPService with REM/Q type will be available to handle the interaction with other REMSPs, as defined in the specification of the Common Service Interface, while the others will be used only to store the history of the certificates previously valid.

The method above is the "operational" and technical one allowing to maintain, inside the **REM-Policy-IT**, a full continuity of service.

Along with this there can be a more conventional and "formal" one (possibly detailed in the national security practice notes, and useful to consolidate the historical information of the Trusted List), in harmony with the other European Member States best practices. Both methods are subject to the updates of the national security practices that can further fine-tune the application (see § 2.6.1).

```
...
<TrustServiceProvider>
  <TSPInformation>
...
  </TSPInformation>
  <TSPServices>
    <!-- Service definition with currently valid certificate and Service Supply Points -->
    <TSPService>
      <ServiceInformation>
        <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q</ServiceTypeIdentifier>
        <ServiceName>
          <Name xml:lang="en">S1-REMS provider</Name>
          <Name xml:lang="it">Fornitore di servizio S1-REMS</Name>
        </ServiceName>
        <ServiceDigitalIdentity>
          <DigitalId>
            <X509Certificate> MIIGzTCCBLWgAwIBAgIESDbQhjANBgkqh...</X509Certificate> <!-- Current
Certificate-->
          </DigitalId>
          <DigitalId>
             <X509SubjectName>C=IT, O=ITERDS, OU=ITERDS test services, CN=S1-REMS provider</X509SubjectName>
          </DigitalId>
          <DigitalId>
            <X509SKI>PyP2u81PfEeMyO5AlGZlqj3oZz4=</X509SKI>
          </DigitalId>
        </ServiceDigitalIdentity>
        <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
        <StatusStartingTime>2022-05-11T20:30:00Z</StatusStartingTime>
        <SchemeServiceDefinitionURI>
        <!--[OMISSIS]-->
        </SchemeServiceDefinitionURI>
        <ServiceSupplyPoints>  <!–ServiceSupplyPoint present ==> Current Certificate-->
          <ServiceSupplyPoint>smtp://mx.s1-rems-only-for-test.it:25</ServiceSupplyPoint>
          <ServiceSupplyPoint>https://s1-rems-only-for-
test.it/CapabilityAndSecurityMetadata.xml</ServiceSupplyPoint>
        </ServiceSupplyPoints>
        <TSPServiceDefinitionURI>
        <!--[OMISSIS]-->
        </TSPServiceDefinitionURI>
      </ServiceInformation>
      <ServiceHistory>
        <!--[OMISSIS]-->
      </ServiceHistory>
   </TSPService>
        <!--[OMISSIS]-->
   <!-- Service definition with expired certificate. There is no ServiceSupplyPoints section -->
   <TSPService>
      <ServiceInformation>
        <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q</ServiceTypeIdentifier>
        <ServiceName>
          <Name xml:lang="en">S1-REMS provider</Name>
          <Name xml:lang="it">Fornitore di servizio S1-REMS</Name>
        </ServiceName>
        <ServiceDigitalIdentity>
          <DigitalId>
            <X509Certificate>XWJDNTIzCg==</X509Certificate> <!-- Expired certificate-->
          </DigitalId>
          <DigitalId>
             <X509SubjectName>C=IT, O=ITERDS, OU=ITERDS test services, CN=S1-REMS provider</X509SubjectName>
          </DigitalId>
```

```
          <DigitalId>
            <X509SKI>Upb9sDkiSRvtym6wwly1PGCEbk8=</X509SKI>
          </DigitalId>
        </ServiceDigitalIdentity>
        <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
        <StatusStartingTime>2021-10-03T08:30:00Z</StatusStartingTime>
        <SchemeServiceDefinitionURI>
        <!--[OMISSIS]-->
        </SchemeServiceDefinitionURI>
        <TSPServiceDefinitionURI>
        <!--[OMISSIS]-->
        </TSPServiceDefinitionURI>
      </ServiceInformation>
      <ServiceHistory>
        <!--[OMISSIS]-->
      </ServiceHistory>
    </TSPService>
<TSPServices>
```

Figure 36 – TrustedList – management of expired certificates for service continuity

2.4.2.12 Policy generali di identificazione | General policy of identification

Le policy relative all'identificazione fanno riferimento agli standard e alle norme vigenti e sempre nel rispetto delle prassi di sicurezza nazionali che ne possono limitare o estendere ulteriormente l'uso (si veda il § 2.6.1). Si vedano per più dettagli lo standard EN 319 521 **[8]**, Clause 5.2.1 "initial identity verification" e il § 2.2 nelle sezioni Utenza Registrata, Identificata e Autenticata.

Policies relating to identification refer to standards and regulation in force and always in compliance with national security practices that can limit or further extend their use (see § 2.6.1). For more details see the standard EN 319 521 **[8]**, Clause 5.2.1 "initial identity verification" and § 2.2 in Registered, Identified and Authenticated Users sections.

2.4.2.13 Policy generali di autenticazione | General policy of authentication

Nell'ambito dei **servizi elettronici di recapito certificato qualificato** (detti anche

In the context of **qualified electronic registered delivery service** (also called **QERDS**, in **ETSI** terminology), authentication

QERDS in terminologia **ETSI**) i metodi di autenticazione rivestono un ruolo essenziale. Fornire delle procedure ed esemplificazioni con l'auspicio di facilitarne la comprensione, oltreché dare l'opportunità di valutarne allo stesso tempo l'affidabilità e l'aderenza ai requisiti di sicurezza correnti, può contribuire alla diffusione e l'uso del servizio. Fruire per lo scopo dei più evoluti, ampiamente impiegati e riconosciuti meccanismi (siano essi o parte di essi anche solo standard de facto) rappresenta un ulteriore contributo al raggiungimento degli obiettivi cui ambiscono le policy di sicurezza (congiuntamente a quelli ovvi di un più ampio e diffuso possibile utilizzo del servizio).

La sezione **Utenza autenticata** al § 2.2 ed in più la nota[27] a pag. 14 forniscono già una prima panoramica rispetto a questo tema. Mentre il § 2.4.2.7 descrive una più semplice soluzione individuata per l'autenticazione da client di posta elettronica di mercato basata su un'**Application Password**.

Altre soluzioni che fanno riferimento agli standard di settore e che facilitino l'esperienza complessiva sono possibili, oltre che auspicabili. Ovviamente sempre nel rispetto delle norme vigenti e delle prassi di sicurezza nazionali che ne possono limitare o estendere

methods play an essential role. Providing procedures and examples with the hope of facilitating understanding, as well as giving the opportunity to evaluate at the same time their reliability and adherence to current security requirements, can contribute to the diffusion and use of the service. The use, for the purpose, of the most advanced, widely used, and recognized mechanisms (be they or part of them even de facto standards) represents a further contribution to the achievement of the objectives aimed at security policies (together with the obvious ones of a wider and more widespread possible use of the service).

The **Authenticated users** section in § 2.2 and the note[27] at pag. 14 already provide a first overview of this topic. While a simpler and most practical solution identified for the authentication from market e-mail client, based on an **Application Password**, is described in § 2.4.2.7.

Other solutions that refer to industry standards and that facilitate the overall experience are possible, as well as, desirable. All of this obviously always in compliance with current regulations and national security practices which may limit or further extend their use (see § 2.6.1). The resulting advantages are significantly appreciable

ulteriormente l'uso (si veda il § 2.6.1). I vantaggi che ne conseguono risultano significativamente apprezzabili sia che si acceda al servizio in modo interattivo ma soprattutto quando si accede in modo non interattivo (**M2M**) - ad esempio attraverso un'applicazione software (detta anche **ERD user agent/application** o **ERD-UA**, in terminologia **ETSI**, per i servizi **QERDS**).

In tali casi (ad analoghi livelli di sicurezza rispetto alla soluzione tramite **Application Password** illustrata al § 2.4.2.7) attraverso lo standard di settore **OAuth 2.0** è possibile semplificare significativamente la gestione delle credenziali nel tempo; ad esempio, automatizzando il processo di generazione e rinnovo di quelle **M2M** (operazione che diversamente si renderebbe necessario effettuare manualmente, con cadenza periodica).

Il meccanismo generale, descritto a titolo esemplificativo in modo schematico e ad alto livello nel seguito, sfrutta principi e potenzialità di alcuni flussi specifici implementabili sulla base dell'**OAuth 2.0 Authorization Framework**. Viene tratta anche ispirazione dalle esperienze di utilizzo, così come anche dai casi d'uso specifici maturati nell'ambito e-mail messaging (applicate dai Big Tech IT provider, ad esempio, mediante il

whether the service is accessed in interactive way but above all when accessed in non-interactive way (**M2M**) - for example through a software application (also called **ERD user agent/application** or **ERD-UA**, in **ETSI** terminology, for **QERDS**).

In such cases (at similar level of security of **Application Password** solution illustrated at § 2.4.2.7) through the **OAuth 2.0** industry standard it is possible to significantly simplify the credentials' management over time; for instance by automating the generation and renewal process of the **M2M** ones (operation that would otherwise be necessary to carry out manually, on a periodic basis).

The general mechanism, described by way of example and in a schematic and high-level way below, exploits the principles and potential of some specific flows that can be implemented on the basis of the **OAuth 2.0 Authorization Framework**. Inspiration is also drawn from experiences of use, as well as from specific use cases developed in the e-mail messaging field (applied by Big Tech IT providers, for instance, through the so called **XOAUTH2**). In fact, the standard **OAuth 2.0**, foresees that profiling and extensions can be

cosiddetto **XOAUTH2**). Infatti, come rimarcato nella Sezione 1.8 dello standard **OAuth 2.0**, lo stesso prevede che possano essere effettuate delle profilature ed estensioni per consentirne un più ampio ed interoperabile utilizzo. Il presente esempio si inquadra proprio in quest'ottica, selezionando e dando una lettura specifica a quelle caratteristiche che possono essere utili per i servizi oggetto di questo documento.

Non si entra pertanto nel dettaglio delle fasi di inizializzazione e registrazione dell'applicazione software **ERD-UA** (o anche "client" in terminologia **OAuth**) cui fornire l'autorizzazione all'uso del servizio. Infatti, queste possono seguire i consueti schemi assimilabili e comuni a varie tipologie anche di altri servizi o rispondere ad esigenze particolari del servizio che si intende offrire.

Di significativo si evidenzia che, in accordo allo schema **OAuth 2.0**, il flusso di autorizzazione all'accesso ed uso del servizio propone - da parte diretta di, o anche attraverso e per mezzo di, un'applicazione software (il **client**/**ERD-UA**) - delle credenziali diverse da quelle utilizzate per l'autenticazione dell'utente. Esse sono denominate Access Token (in terminologia **OAuth**), e per mezzo di queste credenziali, l'applicazione può accedere in modo sicuro a caselle del servizio

issued to allow for a wider and more interoperable use, as noted in Section 1.8 of the same. The present example it is framed precisely in this perspective, selecting and giving a specific reading of those characteristics that can be useful for the services pertaining the subject matter hereof.

Therefore, details about initialization and registration phases of the **ERD-UA** (or even "client" in **OAuth** terminology) to which provide authorization of use of the services are not provided here. In fact, these can follow the usual schemes similar and common to various types of other services or respond to particular needs of the services planned to offer.

Significantly, it is highlighted that, according to the **OAuth 2.0** schema, the authorization flow for access and use of the service foresees – directly by, or even through and by mean of, a software application (the **client**/**ERD-UA**) – different credentials from those used for user's authentication. They are called Access Token (in **OAuth** terminology), and using these credentials, the application can securely access the service's **mailboxes** on

per conto dell'utente cui le caselle stesse sono associate.

In concreto, per l'accesso ai servizi oggetto del presente documento, l'applicazione software (o **client/ERD-UA**) durante l'inizializzazione può essere configurata a disporre di una specifica autorizzazione (detta Authorization Grant, in terminologia **OAuth**). Con tale autorizzazione, fornita, ad esempio **su *base cliente***, possono essere richieste le effettive credenziali (cioè l'**Access Token**) con cui poi l'applicazione può accedere alla **casella** o alle caselle a cui l'**Authorization Grant** è associata. Non si entra qui oltre nel dettaglio di come avviene la configurazione che associa l'**Authorization Grant** al cliente, agli utenti e alle caselle che si possono autorizzare, e per cui sarà possibile richiedere delle credenziali di accesso (**Access Token**). Questo fa parte dei processi di onboarding utenza da parte del service provider. Si può comunque immaginare che il rilascio dell'**Authorization Grant** avvenga attraverso un'apposita procedura da seguire all'inizio e successivamente ad ogni rinnovo della stessa (che può aver luogo in tempi sostanzialmente lunghi).

Le credenziali rilasciate all'applicazione software (o **client/ERD-UA**) con le modalità indicate sopra (ad esempio su base cliente),

behalf of the user to whom the mailboxes are associated.

In concrete terms, for access to services pertaining the subject matter hereof, the software application (or **client/ERD-UA**) can be configured, during initialization, to have a specific authorization (called Authorization Grant in **OAuth** terminology). By means of such authorization, provided for instance on a ***customer basis***, can be required the actual credentials (i.e. the **Access Token**) by which the application can then access to the **mailbox**(es) and to which the **Authorization Grant** is associated. Therefore, details about configuration associating **Authorization Grant** with customer, users, and **mailbox**(es) that can be authorized (by the **Access Token**) are not provided here. This is part of the users' onboarding processes executed by the service provider. However, it can be imagined that the release of the **Authorization Grant** occurs through a specific procedure to be followed at the beginning and subsequently at each renewal of the same (which can take place in substantially long time).

The credentials issued to the software application (or **client/ERD-UA**) through the aforementioned methods (for instance on a

possono avere potenzialmente una durata molto lunga (ad es. di mesi o anni), mentre tramite queste verrà rilasciata una credenziale di accesso (o **Access Token**) di validità breve (es. dell'ordine dei minuti), che può essere rinnovata automaticamente secondo i meccanismi previsti dallo standard **OAuth 2.0**.

Nel dettaglio, l'**Authorization Grant** per l'applicazione software (o **client/ERD-UA**) prevista per il presente esempio è di tipo `grant_type=client_credentials`. Ciò significa che il **client/ERD-UA** deve effettuare una richiesta autenticandosi presso la componente **authorization server** prevista dall'**OAuth 2.0** per ottenere le credenziali di accesso (**Access Token**) ad esempio ad una specifica **casella** (indicandola come parametro o input della richiesta, ad esempio nello scope o tramite altro parametro). L'**authorization server** è tipicamente implementato da quello che in gergo è chiamato **Identity Provider** (**IdP**). L'**Authorization Grant** - che in questi casi è anche chiamata **Client Credentials Grant** - è generalmente contraddistinta da tre elementi: (1) `client_id`, (2) `client_secret` e (3) `TLS certificate`. Gli elementi (1) e (2) rappresentano il tipo più classico di **Client Credentials**. L'elemento (3) è necessario per instaurare il **TLS** (essendo la password

customer basis), can have a very long duration (e.g. months or years), while through these a short validity access credential (or **Access Token**) will be issued (e.g. in the order of minutes), which can be automatically renewed according to the mechanisms provided by the **OAuth 2.0** standard.

In detail, the **Authorization Grant** for the software application (or **client/ERD-UA**) provided for this example is of type `grant_type=client_credentials`. It means that the **client/ERD-UA** has to make a request by authenticating itself with the **authorization server** component provided by the **OAuth 2.0** to obtain the access credentials (**Access Token**) for example to a specific **mailbox** (indicating it as a parameter or input of the request, for instance in the scope or via another parameter). The **authorization server** is typically implemented by what is jargon is called **Identity Provider** (**IdP**). The **Authorization Grant** – which in these cases is also called **Client Credentials Grant** – is generally characterized by three elements: (1) `client_id`, (2) `client_secret` and (3) `TLS certificate`. Elements (1) and (2) represent the most common type of **Client Credentials**. Element (3) is necessary to

rappresentata dal `client_secret`, nel caso più semplice, coinvolta nell'autenticazione). Per assicurare l'**authorization server** sulla reale provenienza della richiesta, a meno che ciò non sia ritenuto necessario per dei casi d'uso specifici o che sia coperto da meccanismi differenti, è opportuno avere un **TLS** di tipo mutual (mTLS) – in accordo allo standard IETF RFC 8705 **[23]**. Tutto ciò, parallelamente e come ulteriore vantaggio all'esigenza primaria menzionata sopra, aggiunge a corredo un ulteriore fattore al flusso di autenticazione. Di conseguenza, in tali casi, il `client_secret`, a meno di specifici requisiti prescrittivi delle policy e prassi di sicurezza (si veda il § 2.6.1), non è più tecnicamente necessario.

La richiesta dell'**Access Token** all'**authorization server** è pertanto formata dai suddetti elementi, che costituiscono il **Client Credentials Grant** (o **Authorization Grant**). A questi può essere aggiunto un parametro (ad esempio tramite lo `scope`) che può essere utilizzato per specificare in modo puntuale, se e quando previsto o in caso di ambiguità, l'entità a cui è associato il token (es. la **casella**).

Nell'uso applicativo, quindi, come ulteriormente specificato nello standard IETF RFC 8705 **[23]**, una generica applicazione

establish the **TLS** (being the password represented by the `client_secret`, in the simplest case, involved in the authentication). To ensure the **authorization server** on the real origin of the request, unless this is deemed necessary for specific use cases or is covered by different mechanisms, it is advisable to have a mutual **TLS** type (mTLS) – in agreement to the IETF RFC 8705 **[23]** standard. All this, in addition and as further advantage to the primary need mentioned above, adds a further factor in the authentication flow. Consequently, in such cases, the `client_secret`, unless specific prescriptive requirements of the security policies and practices (see § 2.6.1), is no longer technically necessary.

The request of the **Access Token** to the **authorization server** is therefore made up of the aforementioned elements, which constitute the **Client Credentials Grant** (or **Authorization Grant**). To these may be added a parameter (for instance via the `scope`) which can be used to specify in a timely manner, if and when it is expected or in case of ambiguity, the entities to which the token is associated (e.g. the **mailbox**).

In use from applications, therefore, as further specified in the IETF RFC 8705 **[23]** standard, a generic software application

software (**client/ERD-UA**) richiede attraverso il **Client Credentials Grant** le informazioni essenziali a comporre le credenziali per accedere alla risorsa protetta (ad es. una **casella**). Queste credenziali sono formate a partire dall'**Access Token** e consentono, ad esempio, di accedere alla **casella** indicata nello `scope`. La richiesta è indirizzata all'**authorization server** (cioè l'**Identity Provider** o **IdP**) del fornitore del **servizio elettronico di recapito certificato qualificato**. L'**authorization server** restituisce in risposta l'**Access Token** (contenuto ad esempio all'interno di un token **JWT**) per l'accesso al servizio limitatamente alle caselle associate (implicitamente in fase di registrazione, o perché specificate nello `scope`) al **Client Credentials Grant** stesso.

Una volta inizializzato e configurato il sistema (operazione one-time effettuata al rilascio e ad ogni rinnovo del **Client Credentials Grant**), la richiesta di un nuovo token **JWT** può essere automatizzata senza più necessità dell'intervento umano. Nel caso di accesso al servizio attraverso delle API (es. ReST API) è generalmente sufficiente utilizzare il token **JWT** ricevuto dall'**IdP** così com'è. Mentre, in caso di accesso SMTP/POP3/IMAP4 (ad es. mediante il protocollo **XOAUTH2** - che deve essere ovviamente supportato dal servizio di

(**client/ERD-UA**) requests through the **Client Credentials Grant** the essential information to compose the credentials to access to the protected resource (e.g. a **mailbox**). These credentials are formed starting from the **Access Token**, which allow, for instance, to access the **mailbox** indicated in the `scope`. The request is addressed to the **authorization server** (i.e. the **Identity Provider** or **IdP**) of the **qualified electronic registered delivery service provider**. In response, the **authorization server** returns the **Access Token** (composed for instance of a **JWT** token) for access to the service limited to the **mailboxes** associated (implicitly during the registration phase, or because specified in the `scope`) to the **Client Credentials Grant** itself.

Once the system has been initialized and configured (one-time operation carried out at the release and at each renewal of the **Client Credentials Grant**), the request for a new **JWT** token can be automated without the need for human intervention. In the case of access to the service through API (e.g. ReST API) it is generally sufficient to use the **JWT** token received by the **IdP** as it is. While, in the case of SMTP/POP3/IMAP4 access (e.g. via **XOAUTH2** protocol – which must obviously be supported by the messaging

messaging sul quale è implementato il **servizio elettronico di recapito certificato qualificato**, e al quale si intende accedere), può essere necessario aggiungere al suddetto token **JWT** altri elementi a causa di limitazioni native dei protocolli di accesso. Questi elementi, quali ad es. l'identificativo della casella, permettono al servizio di identificare in modo univoco la risorsa a cui accedere, e non sono tipicamente necessari nel caso API.

Nell'uso interattivo, invece, ma sempre tramite una generica applicazione **client**, il flusso è simile ma non identico a quello **M2M**. Si noti che qui non ci si riferisce, quindi, ai diffusi client di mercato (dove non risulti possibile configurare il protocollo **OAuth 2.0**) per i quali invece continua ad essere valida la soluzione tramite **Application Password** descritta al § 2.4.2.7, ma ad una generica applicazione **client** (**ERD-UA**) che fa da tramite per un accesso interattivo.

Nell'uso in questione, pertanto, il flusso già visto viene preceduto da un'autenticazione multi-fattore (**MFA**) – da parte dell'utente titolato all'uso della **casella** – reindirizzata verso l'**authorization server** che autorizza di fatto la possibilità ad operare successivamente sulla casella stessa. Questo flusso di

server on top of which is implemented the **qualified electronic registered delivery service**, and to which is intended to access to), due to native access protocol limitations, it may be necessary to add other elements to the aforementioned **JWT** token. These elements, such as for example the mailbox identifier, allow the service to uniquely identify the resource to access, and are normally not required in the API case.

Whereas, during ***the interactive use***, but always through a generic **client** application, the flow is similar but not identical to the **M2M** one. Note that here this does not refer, therefore, to the widespread market clients (where is not possible to freely configure the **OAuth 2.0** protocol) for which the **Application Password** solution described at § 2.4.2.7 continues to be valid, but to a generic **client** application (**ERD-UA**) which acts as a mediation device for interactive access.

In the use in question, therefore, the flow already seen is preceded by a multifactor authentication (**MFA**) – by the user entitled to use of the **mailbox** – redirected to the **authorization server** who effectively authorizes the possibility to subsequently operate on the **mailbox** itself.

autorizzazione indicato in **OAuth 2.0** come Authorization Code Grant prevede un'Authorization Request con parametro `response_type=code`. La richiesta ottiene in risposta dall'authorization server un codice di autorizzazione (es. `code: abc123`) da usare per formare l'**Authorization Grant** (cioè il parametro necessario per l'effettiva richiesta dell'**Access Token**). In assenza di errori il flusso autorizzato prosegue come nel caso non interattivo. Si noti che la richiesta dell'**Access Token** avviene senza che le credenziali (nome utente, **casella**, password, etc.) siano comunicate al **client**, cui arriva solo il suddetto codice di autorizzazione.

Nel dettaglio, l'**Authorization Grant** per l'applicazione software (**client/ERD-UA**) prevista nel presente esempio è di tipo `grant_type=authorization_code`. Questa prevede che il **client/ERD-UA** utilizzi il codice di autorizzazione ricevuto in risposta dall'authorization server (nell'es. `code=abc123`) come parametro sostitutivo dello `scope`, usato nel caso non interattivo, nella richiesta di credenziali di accesso (**Access Token**) per la specifica **casella** associata all'utente.

This authorization flow, indicated in **OAuth 2.0** as Authorization Code Grant uses an Authorization Request with `response_type=code` as parameter. The request obtains, in response from the authorization server an authorization code (e.g. `code: abc123`) to use to form the **Authorization Grant** (i.e. the necessary parameter for the actual **Access Token** request). In absence of errors, the authorized flow continues as in the non-interactive case. Note that the **Access Token** request occurs without communicating the credentials (username, **mailbox**, password, etc) to the **client**, which only receives the aforementioned authorization code.

In detail, the **Authorization Grant** for the software application (**client/ERD-UA**) envisaged in this example is of type `grant_type=authorization_code`. This requires the il **client/ERD-UA** to use the authorization code received in response from the authorization server (in the example `code=abc123`) as a substitute parameter for the `scope` used, in the non-interactive case, in the request for access credential (**Access Token**) for the specific **mailbox** associated with the user.

Da qui in avanti, sia che la suddetta applicazione **client** (**ERD user agent/application** – **ERD-UA**) acceda poi al servizio via protocolli standard (SMTP/POP3/IMAP4) che attraverso delle API (es. ReST API), il flusso che ne consegue è praticamente identico a quello descritto nel caso non interattivo, fatta eccezione per quanto già sottolineato riguardo la necessità dell'interazione preventiva con l'utente (autenticazione/autorizzazione) e dell'uso del relativo codice di autorizzazione.

Pertanto, nel caso interattivo, il flusso è suddiviso in due passi dove nel primo si ottiene dall'**IdP** un authorization code, e nel secondo si richiede un **Access Token** che è strettamente legato a monte allo scopo per cui è fornito.

La generazione di un **Access Token** con le suddette proprietà, legate alla presenza dell'authorization code, ma anche assieme alla caratteristica che tale codice è generato a seguito di un'autenticazione **MFA** dell'utente, suggerisce che il certificato **TLS**, seppur presente, non sia obbligatoriamente di tipo mutual (mTLS), a meno di specifici requisiti prescrittivi delle policy e prassi di sicurezza (si veda il § 2.6.1).

From here on, whether the aforementioned **client** application (**ERD user agent/application** – **ERD-UA**) then accesses to the service via standard protocols (SMTP/POP3/IMAP4) or through API (e.g. ReST API), the resulting flow is practically identical to that described in the non-interactive case, exception made for what has already been underlined regarding the need for preventive interaction with the user (authentication/authorization) and the use of the relevant authorization code.

Therefore, in the interactive case, the flow is split into two steps where in the first an authorization code is obtained from the **IdP**, and in the second is requested an **Access Token** which is strictly linked, upstream, to the purpose for which it is provided.

The generation of an **Access Token** with the aforementioned properties, tied to the presence of the authorization code, but also together with the characteristic that this code is generated following a **MFA** authentication of the user, suggests that the **TLS** certificate, although present, is not mandatorily of mutual type (mTLS), unless specific prescriptive requirements of security policies and practices (see § 2.6.1).

Altri approcci o combinazioni con caratteristiche di protezione, semplificazione o possibilità di integrazione possono essere ulteriormente inclusi. Ad esempio l'uso di meccanismi di *Demonstrating Proof Of Possession (DpoP)* definito nello standard IETF RFC 9449 **[24]**, e/o l'uso del metodo di introspezione *Private Key JWT* in accordo alle specifiche IETF RFC 7521 **[25]** e IETF RFC 7523 **[26]** e supportato nell'ambito del protocollo **OpenID Connect**.

Si rimarca infine che, qualunque sia il suo formato, il token ha durata temporale limitata, nell'ordine di minuti o decine di minuti. Alla scadenza del token (evento rappresentato da risposta "unauthorized" al tentativo di accesso), in funzione delle configurazioni e delle implementazioni, l'applicazione software (**ERD user agent/application** – **ERD-UA**) ha la possibilità di richiederne autonomamente uno nuovo.

Si noti inoltre che il disaccoppiamento del flusso e delle fasi di autorizzazione/autenticazione regolato da uno standard mediante l'uso di un **Access Token** rilasciato da un ruolo di autorizzazione specifico denominato **Identity Provider** o **IdP**, permette di implementare – dove richiesto e/o nei casi in cui ciò sia effettivamente possibile e permesso – dei servizi di autenticazione

Other approaches or combinations with security features, simplification or integration possibilities can be further included. For instance, the use of the *Demonstrating Proof Of Possession (DpoP)* mechanism defined in IETF RFC 9449 **[24]** standard, and/or the use of the *Private Key JWT* introspection method according to the IETF RFC 7521 **[25]** and IETF RFC 7523 **[26]** specifications and supported within the **OpenID Connect** protocol.

Finally, it should be noted that, whatever its format, the token has a limited duration, in the order of minutes or tens of minutes. When the token expires (event represented by an "unauthorized" response to an access attempt), depending on the configurations and implementations, the software application (**ERD user agent/application** – **ERD-UA**) has the possibility to independently request a new one.

Also note that the decoupling of the flow and the authorization/authentication phases regulated by standards through the use of an **Access Token**, issued by a specific authorization role called **Identity Provider** or **IdP**, allows to implement – where required and/or in the cases where this is actually possible and permitted – federated authentication services through connection

federata tramite connessione con **IdP** terzi. Ciò rappresenta, inoltre, un approccio aperto ad eventuali adeguamenti che potrebbero arrivare dai regolamenti europei.

with third parties **IdP**.
All this represents also an open approach to any compliance update that could come from European regulations.

2.4.2.14 Policy di gestione del LoA | LoA - Assurance level management policy

Al fine di garantire il massimo grado di interoperabilità (in riferimento soprattutto a quella cross-border), per i tipi di trasmissione tra **utenza** registrata (cioè come indicato nella tipologia **TUC1** in **Table 1**), il livello di assurance (LoA da qui in avanti), richiesto per il sender nel *component* **I10** (AssuranceLevelsDetails) della ERDS evidence come *initial identity verification*, può essere al più di livello 'substantial' (così come prescritto anche nelle capability della REM baseline EN 319 532-4 Clause C.2.3.4.2, Table C.8, item c.3.3.6). Infatti, ci si riferisce all'**utenza** registrata perché durante tale fase può essere effettuata l'*initial identity verification* come disposto nello standard EN 319 521**[8]**, Clause 5.2.1.1 ed in particolare come indicato all'item b). In accordo a tale punto, essendo il livello 'substantial' (o equivalente) il minimo livello accettabile, si deduce che non può essere richiesto, per l'uso del servizio, un livello superiore e nel contempo garantire il massimo

In order to ensure the maximum degree of interoperability (especially with regard to that cross-border), for the types of transmission between registered users **account** (i.e. as per the type **TUC1** in **Table 1**), the level of assurance (LoA hereinafter), required for the sender in the *component* **I10** (AssuranceLevelsDetails) of the ERDS evidence as *initial identity verification*, can be at the most 'substantial' (as well as prescribed also in the capability of the REM baseline EN 319 532-4 Clause C.2.3.4.2, Table C.8, item c.3.3.6). In fact, this is referred to registered users because, during the registration phase, the *initial identity verification* of the users **account** can be done as per the dispositions of the standard EN 319 521**[8]**, Clause 5.2.1.1, and in particular as required at the item b). According to such point, the 'substantial' LoA (or equivalent) is the minimum acceptable. It follows that cannot be required, for the use of the service, a higher level and, meanwhile, to

grado di interoperabilità. Come detto sopra, questo razionale che conduce all'uso del livello 'substantial' è anche in totale accordo con le capability della REM baseline, e vale indipendentemente dal fatto che l'utenza, anche per altre tipologie di servizi, possa risultare registrata mediante un'*initial identity verification* effettuata con assurance level 'high'.

Come ulteriore conseguenza, e per ragioni analoghe, il mittente o il servizio **S-REMS** (sulla base della propria policy, o su specifiche richieste del mittente) non può richiedere un **REM-RecipientAssuranceLevel** all'**utenza** ricevente che sia differente dal livello "substantial". Infatti, "substantial" è il livello stabilito nelle capability della REM baseline, ma è anche il massimo che si può richiedere per assicurare un servizio interoperabile. Per questo il suddetto header è assente nella REM baseline.

have ensured the maximum degree of interoperability. As noted above, this rational that leads to the use of 'substantial' level is in complete agreement with the capability of the REM baseline, and it is valid independently by the fact that the users, even for other type of services, may result registered by an *initial identity verification* done with a 'high' assurance level.

As further consequence, and for similar reasons, the sender or the **S-REMS** (on the base of its policies, or of specific requests from the sender) cannot require a **REM-RecipientAssuranceLevel** to the recipient that is different from the "substantial" level. In fact, "substantial" is the level prescribed in the REM baseline capabilities, but it is also the maximum that can be required to ensure an interoperable service. For that the header above is absent in the REM baseline.

```
<tns:Evidence …>
...
  <AssuranceLevelsDetails>
   <GlobalAssuranceLevel>
    <AssuranceLevel>http://eidas.europa.eu/LoA/substantial</AssuranceLevel>
    <PolicyID>https://eidas.agid.gov.it/REM/rem-policy-it#assurance-level-policy</PolicyID>
   </GlobalAssuranceLevel>
   <tns:AuthenticationDetails>
    <AuthenticationTime>2021-05-25T09:03:38Z</AuthenticationTime>
```

```
    <AuthenticationMethod>https://eidas.agid.gov.it/REM/rem-policy-it#authentication-
method</AuthenticationMethod>
   </tns:AuthenticationDetails>
  </AssuranceLevelsDetails>
...
</tns:Evidence>
```

Figure 37 – LoA - Assurance level in ERDS evidence excertp

2.4.2.15 Policy di handshake durante l'operazione di relay | Handshake policy during relay operation

Al fine di garantire l'efficacia necessaria e sufficiente nella sicurezza del dialogo tra **REMSP** differenti è fondamentale assicurarsi che l'**handshake TLS** sia attivabile, attivato ed operativo. Per **attivabile** si intende che sia il REMSP mittente che il REMSP destinatario DEVONO SUPPORTARE un full **TLS**, e che i vari parametri e le procedure di sicurezza quali, ad es., la versione di **TLS**, la suite crittografica, la gestione delle chiavi crittografiche, etc. siano presenti ed aderenti alle current *security policy and best practice* previste per il servizio REM (si veda al fondo della presente sezione ed il § 2.6.1). Analogamente, per **attivato** ed **operativo** si intende che funzionalità gestibili in modo opportunistico quali le opzioni e "negoziazioni" al ribasso (come, ad es., il

To ensure the necessary and sufficient secure communication effectiveness between different **REMSP**s, it is crucial to make sure that the **TLS handshake** is activable, activated and operational. **Activable** means that both sender and recipient's **REMSP**s MUST SUPPORT a full **TLS**, and that various security parameters and procedures such as, for example, the **TLS** version, the cryptographical suite, the management of the cryptographic keys, etc. are present and compliant with the current *security policy and best practices* foreseen for the REM service (see at the end of the present section and § 2.6.1). Likewise, **activated** and **operational** mean that capabilities manageable in an opportunistic way as for instance the options and down-negotiations (such as "NON-

"NON-ANNUNCIO" dello STARTTLS, il "PROCEDERE IN CHIARO" sul non-annuncio STARTTLS, o il "NON-DARE-SEGUITO" all'annuncio dello STARTTLS) DEVONO ESSERE IMPEDITI. In altre parole, il TLS handshake DEVE avvenire con assoluta certezza e NON DEVONO essere possibili scorciatoie che ne riducano la sicurezza. In assenza di ciò la connessione DEVE essere **ABORTITA**[37] (ad es. con alert fatal handshake failure).

A supporto ed in aggiunta alle suddette considerazioni si vedano anche le misure relative al **DNS**, quanto inerente il **TLS** handshake già accennato nel § 2.4.2.8, la gestione delle chiavi crittografiche relative al **TLS** da attuare in accordo con i requisiti delle *security policy and best practice* di riferimento (es. EN 319 521 **[8]** ed ETSI EN 319 401 **[11]** ad

ANNUNCEMENT" of STARTTLS, proceed in a clear way when STARTTLS is not announced, or NOT-FOLLOW the STARTTLS announcement) MUST BE PREVENTED. In other words, the TLS handshake MUST TAKE PLACE with the absolute certainty and shortcut that reduce the security MUST NOT be possible. In absence of this, the connection MUST be **ABORTED**[37] (e.g., through a fatal handshake failure alert).

To support and complete the aforementioned considerations see also the security measures relevant to the **DNS**, everything regard the **TLS** handshake already mentioned in § 2.4.2.8, the management of the cryptographic keys relevant to **TLS** handled in accordance with requirements of reference *security policy and best practices* (e.g., EN 319 521 **[8]** and ETSI EN 319 401 **[11]** to which is normatively bound) and

[37] L'abort dovuta al TLS handshake failure galleggia verso l'alto, trasformandosi in un evento applicativo di segnalazione all'utente, attraverso una **RelayFailure** con codice **RB08/R_ERDS_NotIdentified**. Si noti che questo caso non si traduce in un downgrade segnalato all'utente con un UntrustedPathToRecipient (previsto invece verso la posta ordinaria). Infatti, questo caso riguarda un dominio "trusted" (correttamente ancorato alla TL mediante il DNS e la CSI) ma con handshake TLS verso l'R-REMS che fallisce.

[37] The abort due to the TLS handshake failure floats upwards, turning into an application event noticing the user, through a **RelayFailure** with code **RB08 / R_ERDS_NotIdentified**. It is noted that this case doesn't translate in a downgrade noticed to the user with an UntrustedPathToRecipient (provided in case of ordinary email). In fact, the present case regards a "trusted" domain (correctly anchored to the TL by DNS and CSI) but with a failure on the TLS handshake towards R-REMS.

esso normativamente legato) e ad eventuali specifiche previste nell'ambito della **REM-Policy-IT** (si veda il § 2.6.1), ed i seguenti punti dello standard EN 319 532-4 [**4**].

possible specifications provided in the context of **REM-Policy-IT** (see § 2.6.1), and the following points of the EN 319 532-4 [**4**] standard.

"Clause 5.3.4

*a) The Relay Interface **shall** be implemented using SMTP protocol **securing** the communication from the sender REMSP server to the recipient REMSP server **using TLS"***

⇨ **TLS is mandatory.**

Clause C.2.3.4.4

*c.3.5.1) The TLSCertificate element of CapabilityBasedSecurity **shall** contain the **X509Certificate** used for the Transport Layer Security (**TLS**) mechanism of REMS SMTP ServiceEndpoint, for the **basic handshake**.*

*NOTE 2: It is important to have the **TLS certificate ensured by an anchor in the Trusted List**. The sender's REMS needs to be sure that **the contacted REMS**, resolved by DNS lookup, **is the intended server** (thus guaranteeing that any REM message hands over only to Trusted REMS). The TLS handshake between Trusted REMS, that has to take place in its completeness, and **the subsequent secure matching between the server's certificate and the TLS certificate anchored by the Trusted List** concur for the accomplishment of this assurance task. The domain resolved by DNS is not always (indeed almost never) the same domain contained in the service's certificate. For example, in the case of a REMS managing thousands of email domains, these are resolved by the DNS to the MX records. Therefore, **only the MX record hostnames are configured inside the certificate SAN,** and not all the thousands of managed domains; and the TLS certificate **certifies** only the **MX records hostnames**. The **coverage against security threats** provided by this "basic handshake" mechanism is implemented by: **DNS**, **TLS** plus **TLS certificate anchored in Trusted List** through the CapabilityAndSecurityInformation XML structure. Possible **MITM attacks** are detected right through the **TLS certificate ensured in TL and not solely by TLS standalone certificate checks**; and the relevant session is intended in the "forced TLS" form (and not as an "opportunistic TLS").*

⇨ **The TLS certificate is anchored ALSO to the Trusted List.**
⇨ **It is necessary an additional secure matching between the server certificate and the certificate in the Trusted List.**
⇨ **Man-in-the-middle attacks are detected by checking the REAL OPERATION of a full TLS and through a check that the TLS certificate is ensured in the Trusted List and NOT ONLY by the generic TLS standalone certificate check.**

Considerare che l'utilizzo di un approccio che adotti quanto **necessario/sufficiente al**

Consider that, the use of an approach that adopts as **necessary/sufficient to**

raggiungimento del livello di sicurezza atteso - tenendo sempre conto del contesto di utilizzo di tali mezzi (che è confinato al dialogo server-to-server tra **REMSP**) - **tende a non introdurre** né meccanismi, né strumenti e né risorse che non siano strettamente necessarie, e che vadano ad aumentare le complessità statiche (es. di configurazione) o le performance dinamiche (es. di utilizzo) dell'intero sistema.

Si consideri inoltre che tutta l'architettura dell'**ERDS** - e così anche lo strato che gestisce il dialogo tra **REMSP** - è estremamente modulare, organizzata a livelli, standardizzata e basata su protocolli e meccanismi standard. Ognuno dei livelli o dei moduli si presta quindi molto bene ad essere rivisto nel tempo, integrato e/o sostituito, in un'**ottica a PLUG-IN**, in accordo a nuove necessità di qualsivoglia natura, ma in particolare in funzione della **salvaguardia della sicurezza** dell'intero sistema (si veda il § 2.6.1 che indica come è previsto che le varie entità possano evolvere, esse aggiornate o riadeguate, riguardo le security practice da adottare sulla base delle linee guida e best practice a livello nazionale ed internazionale).

achieve the expected security level - always taking into account of the usage context of such means (that is confined to the **REMSP** server-to-server communication) - **tends to not introduce** mechanisms, instruments nor resources that are not strictly necessary, and that can increase the static complexity (e.g., of configuration) or the dynamic performance (e.g., of usage) of the entire system.

Consider also that the entire **ERDS** architecture – and then also the layer that manages the interaction between **REMSP**s - is extremely modular, organized by layers, standardized, and based on protocols and standard mechanisms. Each layer or module lends itself very well to be revised, integrated or substituted over the time, in a **PLUG-IN optical**, according to new needs of whatever nature, but in particular in relation to the **protection of** the entire system **security** (see § 2.6.1 indicating how any entity can evolve, to be updated or readjusted, regarding the security practices to adopt, based on national and international guidelines and best practices).

2.5 Gestione degli errori | Error management

2.5.1 Eventi e codici di errore | Events and error codes

La **Table 15** contiene una versione compatta e correlata di eventi e codici di errore presenti ed usati in più punti del presente documento. In particolare:

G03 ERDSEventId:	Table 3, Table 5
ERDSEventId:	Table 10
G04 EventReason:	Table 3, Table 5
Reason code:	Table 10
G04 Details:	Table 3, Table 5
EventReasons:	Row PP24 of Table 2

The **Table 15** contains a compact and correlated version of events and error codes present and used in many points of the present document. In particular:

G03 ERDSEventId:	Table 3, Table 5
ERDSEventId:	Table 10
G04 EventReason:	Table 3, Table 5
Reason code:	Table 10
G04 Details:	Table 3, Table 5
EventReasons:	Row PP24 of Table 2

Table 15 – Events and Reason codes in REM-Policy-IT

Event and (code) Table 1 EN 319 522-1 [5]	Reason Code Clause 8.3.3 EN 319 522-2 [6]	Table 3 – EN 319 522-3 - URIs for EventReason of ERDS evidence	REM baseline
SubmissionAcceptance (A.1)	RA01	http://uri.etsi.org/19522/EventReason/MessageAccepted	Y
SubmissionRejection (A.2)	RA02	http://uri.etsi.org/19522/EventReason/InvalidMessageFormat	Y
	RA03	http://uri.etsi.org/19522/EventReason/MalwareFound	Y
	RA05	http://uri.etsi.org/19522/EventReason/S_ERDS_PolicyViolation	Y
	RA06	http://uri.etsi.org/19522/EventReason/S_ERDS_Malfunction	Y
RelayAcceptance (B.1)	RB01	http://uri.etsi.org/19522/EventReason/S_ERDS_MessageSuccessfullyRelayed	Y
RelayRejection (B.2)	RB02	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejected	Y
	RB03	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForMalware	Y
	RB04	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForInvalidSignature	Y
	RB05	http://uri.etsi.org/19522/EventReason/R_ERDS_MessageRejectedForInvalidCertificate	Y
	RB06	http://uri.etsi.org/19522/EventReason/R_ERDS_PolicyViolation	Y
RelayFailure (B.3)	RB07	http://uri.etsi.org/19522/EventReason/R_ERDS_Malfunction	Y
	RB08	http://uri.etsi.org/19522/EventReason/R_ERDS_NotIdentified	Y
	RB09	http://uri.etsi.org/19522/EventReason/R_ERDS_Unreachable	Y
	RB10	http://uri.etsi.org/19522/EventReason/UnknownRecipient	Y
	RB21	http://uri.etsi.org/19522/EventReason/MessageNotAcceptedForUnregisteredRecipient	Y
	RB22	http://uri.etsi.org/19522/EventReason/S_ERDSP_ReceivedNoRelayAcceptanceInfoFromR_ERDSP	Y
ContentConsignment (D.1)	RD01	http://uri.etsi.org/19522/EventReason/MessageConsignedToRecipient	Y
ContentConsignmentFailure (D.2)	RD03	http://uri.etsi.org/19522/EventReason/S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP	Y
	RD04	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForQuota	Y
	RD05	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForMalfunction	Y
	RD06	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnallowedType	Y
	RD21	http://uri.etsi.org/19522/EventReason/MessageNotConsignedForUnregisteredRecipient	Y
RelayToNonERDS (F.1)	RF01	http://uri.etsi.org/19522/EventReason/MessageRelayedToNonERDS	N
RelayToNonERDSFailure (F.2)	RF02	http://uri.etsi.org/19522/EventReason/ExternalSystemUnreachable	N
	RF03	http://uri.etsi.org/19522/EventReason/MessageRejectedByExternalSystem	N
	RF51	*http://uri.etsi.org/19522/EventReason/RelayToNonERDSNotAllowed*	*N*
ReceivedFromNonERDS (F.3)	RF04	http://uri.etsi.org/19522/EventReason/MessageReceivedFromNonERDS	N

Gli eventi F.1, F.2 e F.3 non fanno parte della REM baseline (e quindi dell'interoperabilità cross-border) ma sono utilizzati a livello di **REM-Policy-IT** per l'interoperabilità con la posta elettronica ordinaria (si veda § 2.4.2.2).

The events F.1, F.2 e F.3 are not part of the REM baseline (and then of the cross-border interoperability) but are used at **REM-Policy-IT** level for the interoperability with the ordinary email (see § 2.4.2.2).

Si noti che il seguente error code non è parte della REM baseline ma essendovi la possibilità nello standard di definire dei CustomCode (come si evince dal documento EN 319 522-2 **[6]**, Clause 8.3.3), a livello di **REM-Policy-IT** è definito il seguente nuovo Reason Code, ed è posto per uniformità sempre sotto la stessa URI base di ETSI:

RF51 http://uri.etsi.org/19522/EventReason/RelayToNonERDSNotAllowed

La descrizione di dettaglio da utilizzare in questo caso come terzo sub-element dell'EventReason nella ERDS evidence (come spiegato in riga **PP24**, **Table 2**) è:

"*Relay to non-ERDS not allowed*" per RF51 (si veda **Figure 10** per un esempio).

Si noti che l'evento RA04 non è inserito nella suddetta tabella in quanto si riferisce alla firma digitale incorporata nell'*original message* che è out-of-scope rispetto al trasporto del messaggio (e pertanto non è previsto che un **REMSP** usi tale codice nelle ERDS evidence emesse all'interno della REM baseline).

The following error code is not part of the REM baseline but since the standard allows to define new CustomCodes (as clearly follows from the tables of the document EN 319 522-2 **[6]**, Clause 8.3.3), the following new Reason Code is defined at **REM-Policy-IT** level, and it is put for uniformity under the same ETSI base URI:

RF51 http://uri.etsi.org/19522/EventReason/RelayToNonERDSNotAllowed

The detailed description to use in this case, as third ERDS evidence EventReason sub-element (as illustrated in row **PP24**, **Table 2**) is:

"*Relay to non-ERDS not allowed*" for RF51 (see **Figure 10** for an example).

Note that the event RA04 is not present in the table above since it refers to a possible user's digital signature incorporated in the *original message* that it is out of scope in respect to the transport (and so it is not foreseen that a **REMSP** uses such code in ERDS evidence issued inside the REM baseline).

2.6 Buona prassi | Best practice

2.6.1 Prassi generali e di sicurezza della REMID Authority | Security and general REMID authority practice

Riguardo le pratiche generali e di sicurezza (a titolo esemplificativo ma non esaustivo, parametri di competenza della sicurezza complessiva del sistema quali, password/credenziali/token/chiavi crittografiche/certificati digitali e le relative policy di gestione/lunghezza/durata, così come per Common Service Interface (**CSI**), Trusted List (**TL**), **time-stamp**, **DNS**, misure anti-malware, procedure di migrazione **utenze** e domini, ma pure parametri nuovi o aggiornati, anche se già specificati come valore iniziale nel presente documento) sarà necessario nel tempo fare riferimento ad apposite note emesse da AGID (**REMID authority** per l'Italia) per quanto concerne la **REM-Policy-IT**.

Regarding the general and security practices (by way of example but not limited to, parameters of the competences of the overall security of the system such as, password/credentials/tokens/ cryptographic keys/digital certificates and the relevant policies of management/length/duration, as well as for Common Service Interface (**CSI**), Trusted List (**TL**), **time-stamp**, **DNS**, anti-malware measures, migration procedures for users **account** and domains, but also new or updated parameters even whether already specified as initial value in the present document) refer, over the time, to the appropriate notes issued by AGID (the **REMID authority** for Italy) with regards to **REM-Policy-IT**.

2.6.2 Prassi generali migrazione dominio della REMID Authority | General REMID authority practice for domain migration

2.6.2.1 Descrizione generale | General description

La migrazione di un dominio tra due differenti REMS Provider, vista la criticità delle operazioni previste, comporta sempre il rischio di creare un disservizio per il **cliente**.

In questa sezione vengono descritte le pratiche adottate dalla **REM-Policy-IT** al fine di garantire massima trasparenza ed efficacia

The migration of a domain between two different REMS Providers, given the criticality of the envisaged operations, always entails the risk of creating a disservice for the **customer**.

This section describes the practices adopted by the **REM-Policy-IT** in order to

nella salvaguardia del sistema, in tutte le circostanze dove si verificasse la necessità di migrare un dominio **DNS** con delle **utenze** associate, da un REM service provider cedente (es. REMSP-A) verso un altro cessionario (es. REMSP-B). Si faccia pertanto riferimento alle linee guida esemplificate nel seguito che, se adottate correttamente, minimizzano impatto e durata del potenziale disservizio.

guarantee maximum transparency and effectiveness in safeguarding the system, in all circumstances where the need arises to migrate a **DNS** domain with associated users **accounts**, from a transferring provider (e.g., REMSP-A) to another transferee (e.g., REMSP-B). Please therefore refer to the guidelines exemplified below which, if adopted correctly, minimize the impact and duration of the potential disruption.

2.6.2.2 Soggetti coinvolti | Involved parties

I principali attori coinvolti in un esempio tipico di migrazione di dominio **DNS** sono descritti nel seguito.

- **Cliente**: è il soggetto, **titolare** di un dominio **DNS** su cui sono attestate delle **caselle** REM, che vuole effettuare la migrazione di tale dominio da un REMSP (REMSP-A) ad un altro (REMSP-A) dove:
- **REMSP-A**: REM Service Provider cedente
- **REMSP-B**: REM Service Provider destinazione
- **Maintainer** del dominio **DNS**: per le finalità del presente documento, è il soggetto coinvolto nella gestione tecnica ed operativa

The main players involved in a typical example of domain migration are described below.

- **Customer**: is the legal person, **owner** of a **DNS** domain on which users **account** are registered, who wants to migrate such domain from a REMSP (REMSP-A) to another (REMSP-A) where:
- **REMSP-A**: transferring REM Service Provider
- **REMSP-B**: transferee REM Service Provider
- **Maintainer** of the **DNS** domain: for the purposes of the present document, it is the person involved in the technical and operational management of the domain

del dominio dopo la sua registrazione (può essere anche lo stesso **cliente**).

after its registration (it can be also the **customer** itself).

2.6.2.3 Condivisione migliori pratiche | Best practice sharing

I passi principali da tenere in considerazione in un esempio tipico di migrazione di dominio **DNS** sono descritti nel seguito.

1. Pianificare la migrazione con sufficiente anticipo, in modo da definire i dettagli di tutte le attività necessarie.

2. Predisporre in anticipo le **caselle** da migrare sul REMSP-B.

3. [Opzionale] Avviare eventuali procedure di trasferimento dei messaggi dal REMSP-A al REMSP-B - in osservanza degli accordi in essere con il **cliente** - per mezzo di protocolli e/o integrazioni applicative adeguate messe a disposizione dai due REMSP coinvolti, e sempre nel rispetto delle policy di autenticazione previste dagli standard, e delle prassi di sicurezza nazionali che ne possono limitare o estendere ulteriormente l'uso (si veda il § 2.6.1).

The main steps to take into consideration in a typical example of **DNS** domain migration are described below.

1. Plan the migration far enough in advance, in order to define the details of all the necessary tasks.

2. Prepare the users **account** to be migrated to the REMSP-B in advance.

3. [Optional] Initiate any procedures for transferring messages from REMSP-A to REMSP-B - in compliance with the agreements in place with the customer – by means of protocols and/or adequate software integrations made available by the two impacted REMSPs, and always in compliance with the security policies authentication required by the standards, and within national security practices that can limit or further extend their use (see § 2.6.1).

4. Il giorno precedente alla migrazione, il **Maintainer** del dominio deve configurare un valore basso del TTL (Time to Live), ad esempio a 5 minuti.

5. Il giorno della migrazione:

5.1 [Opzionale] In funzione a se / come è gestito il punto **3.** sopra, viene effettuata un'ultima sincronizzazione dei contenuti delle **caselle**.

5.2 Il REMSP-A disattiva (a livello logico) il dominio e le relative **caselle**. Di conseguenza, nel caso in cui un qualsiasi altro REMSP dovesse tentare di trasmettere messaggi (tecnicamente di effettuare un relay) a **caselle** del dominio oggetto della migrazione, il REMSP-A deve rifiutare tali messaggi (errore standard relativo a **casella** NON gestita).

5.3 Il **Maintainer** del dominio configura l'**MX record** all'indirizzo del REMSP-B (coincide con il Service Supply Point con schema *smpt* es. presente all'interno della Trusted List; es. *ServiceSupplyPoint: smtp://{REMSP-MX-RECORD-NAME}*), e riporta il valore del TTL a quello precedente.

5.4 Il REMSP-B attiva (a livello logico) il dominio e le relative **caselle**. Da questo momento in poi accetta i messaggi relativi a caselle del dominio oggetto di migrazione

5.5 Il REMSP-A completa le operazioni di "cancellazione" delle **caselle** migrate.

4. The day before the migration, the domain **Maintainer** configures a low value for the TTL (Time to Live), for instance 5 minutes.

5. Migration day:

5.1 Depending on whether / how point **3.** Above is managed, a final users' **mailboxes** content synchronization is carried out.

5.2 REMSP-A deactivates (from logical viewpoint) the domain and its **mailboxes**. Consequently, if any other REMSP attempts to transmit messages (i.e. to do a relay, from technical view point) to **mailboxes** of the migrated domain, REMSP-A has to reject such messages (by a standard non-existent email address error for the **mailbox**).

5.3 Maintainer of domain configures the record to the address of REMSP-B (i.e. with the Service Supply Point of the Trusted List characterized by the *smtp* schema; e.g. *ServiceSupplyPoint: smtp://{REMSP-MX-RECORD-NAME}*), and returns back the value of TTL to the previous one.

5.4 REMSP-B activates (from logical viewpoint) the domain and its **mailboxes**. From this moment onward it will accept messages relating to **mailboxes** of the domain being migrated.

5.5 REMSP-A completes the deletion of the migrated **mailboxes**.

2.6.2.4 Considerazioni finali | Final considerations

Partendo dall'assunto che la migrazione non deve essere "sincronizzata" con le tempistiche di aggiornamento di un sistema "esterno" (come ad es. l'IGPEC), eventuali impatti di disservizio sono principalmente legati alle tempistiche di aggiornamento del **DNS** e all'eventuale corretta gestione del TTL da parte dei client **DNS**.

Pertanto, in queste buone prassi di procedura sono volutamente omesse considerazioni circa la re-identificazione del **titolare** delle **caselle** da parte del REM Service Provider destinazione, REMSP-B, che sono out of scope rispetto ai presenti contenuti.

Starting from the assumption that the migration has not to be "synchronized" with the update times of an "external" system (like for instance the IGPEC), any impacts of disruption are mainly relevant to the **DNS** update timing and the possible correct management of the TTL by **DNS** clients.

Therefore, these best procedural practices have deliberately omitted considerations regarding the re-identification of the **owner** of the **mailboxes** by the target REM Service provider, REMSP-B, which are out of scope with respect to the present contents.

2.7 Esempi di formati REM | Examples of REM formats

2.7.1 Generalità e struttura | General properties and structure

Viene fornito, assieme al presente allegato tecnico, lo zip file `STESSO-NOME-DEL-DOCUMENTO.examples.zip` contenente vari esempi che racchiudono degli interi cicli di interscambio di tipo REM (in accordo alla REM baseline e la REM-Policy-IT) partendo dal messaggio iniziale da inviare (il cosiddetto "*original message*") fino alle due ricevute di avvenuta consegna nella mailbox dei rispettivi destinatari (le cosiddette REM ContentConsignment receipt), incluso anche il set di messaggi che simulano tutti i possibili errori. Per comodità sono fornite a parte, oltre che allegate ovviamente in ognuno dei REM message, le ERDS evidence come XML stand-alone.

Gli esempi sono suddivisi in quattro macro-classi:

Intra-REM-flow: relativi a scambi tra REMSP tutti appartenenti al sistema REM, aderenti alla REM baseline e alla presente REM-Policy-IT.

Outflow: relativi ad uno scambio da un REMSP appartenente al sistema REM e un service provider esterno alla REM.

The zip file `SAME-NAME-OF-DOCUMENT.examples.zip` is provided as an attachment of the present document. It contains a set of examples of full cycles of REM interchanges (according to the REM baseline and the REM-Policy-IT), starting from the initial user content to send (the so called "*original message*") up to the two REM ContentConsignment receipts (i.e. the proof of consignment of the user content to each of the relevant recipient's mailbox), including also the set of messages that mimic all the possible errors. The ERDS evidence XMLs are provided apart, as stand-alone files, for the convenience of the users of these examples.

The examples are divided into four macro-classes:

Intra-REM-flow: relevant to exchanges between REMSPs belonging to the REM system, compliant with the REM baseline and the present REM-Policy-IT.

Outflow: relevant to an exchange between a REMSP belonging to the REM system and a service provider external in respect to the REM.

Inflow: relativi ad uno scambio da un service provider esterno alla REM e un REMSP appartenente al sistema REM.

Mixed flows with: relativi scambio misti o con particolarità da sottolineare.

Infine, per facilitare le verifiche c'è una cartella contenente tutti i certificati digitali utilizzati per le firme digitali e per il **time-stamp** dei vari oggetti che si sono resi necessari per comporre i suddetti esempi.

Tutti i file forniti con gli esempi, oltre che utilizzabili dalle applicazioni cui risultano associate le rispettive filename extension, sono tutti in formato testo; quindi, apribili ed ispezionabili da qualsiasi editor. Il codice nel nome del file (es. `RA01`) rappresenta il *Reason Code* del REM message, e tutte le sue possibili casistiche sono illustrate nella seconda colonna in **Table 15**.

Inflow: relevant to an exchange between a service provider external in respect to the REM and a REMSP belonging to the REM system.

Mixed flows with: relevant to mixed exchanges or with some peculiarity to outline.

Lastly, a folder with all digital certificates used for the digital signature and the **time-stamp** of the REM objects constituting the aforementioned examples is provided, in order to facilitate the verifications.

All the files provided with the examples, besides being bound to the respective applications associated to any filename extension, are all in pure text format. So, they can be opened and inspected by any common text editor. The code in the name of the file (e.g., `RA01`) represents the *Reason Code* of the REM message, and all its possible variants are illustrated in the second column of **Table 15**.

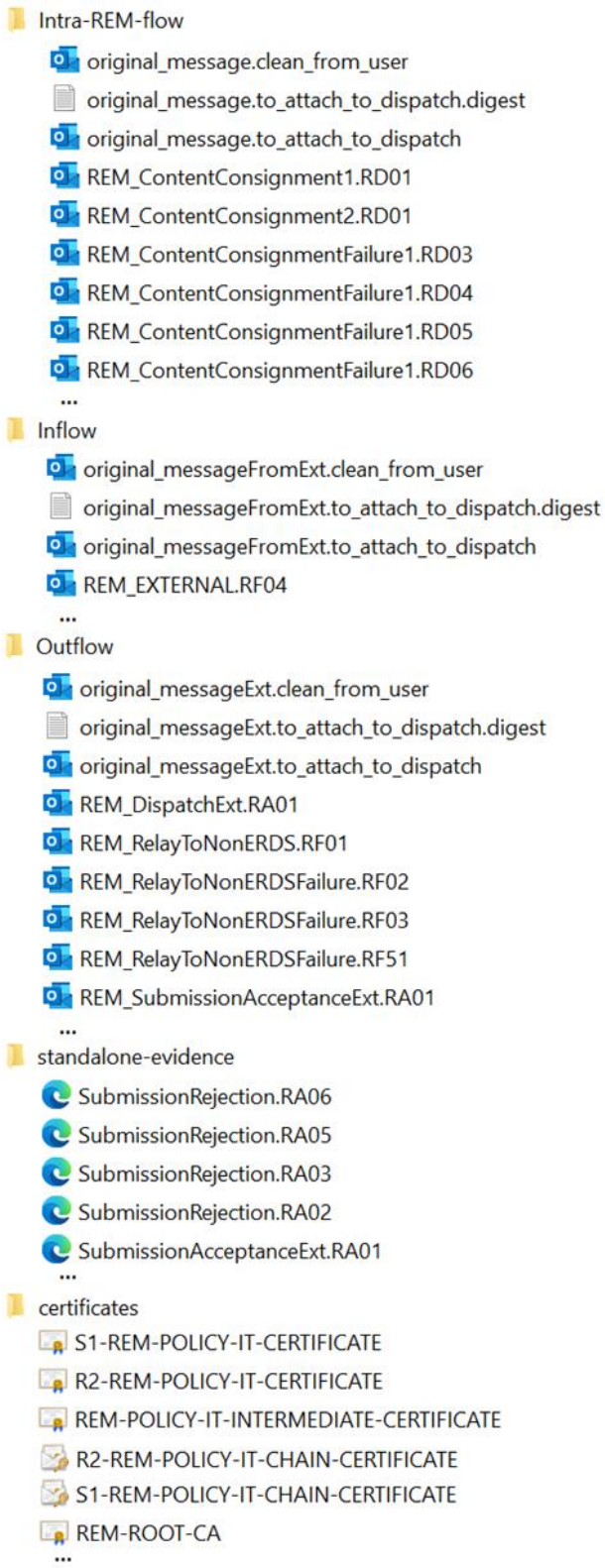


Figure 38 – Examples: structure of the folders

2.7.2 original messages – Intra-REM-flow examples inside REM baseline circuit (TUC1)

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

Used Intra-REM-flow (inside REM baseline circuit – REM messages in § 2.7.3 and 2.7.4):

```
original_message.clean_from_user(.eml)
original_message.to_attach_to_dispatch(.eml)
original_message.to_attach_to_dispatch.digest(.txt)
```

2.7.3 REM dispatch – Intra-REM-flow examples inside REM baseline circuit (TUC1)

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
REM_Dispatch.RA01(.eml)
```

2.7.4 REMS receipts – Intra-REM-flow examples inside REM baseline circuit (TUC1)

2.7.4.1 REM_SubmissionAcceptance

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
REM_SubmissionAcceptance.RA01(.eml)
```

2.7.4.2 REM_SubmissionRejection

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
REM_SubmissionRejection.RA02(.eml)
REM_SubmissionRejection.RA03(.eml)
REM_SubmissionRejection.RA05(.eml)
REM_SubmissionRejection.RA06(.eml)
```

2.7.4.3 REM_ RelayAcceptance

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
REM_RelayAcceptance.RB01(.eml)
```

2.7.4.4 REM_ RelayRejection

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
REM_RelayRejection.RB02(.eml)
REM_RelayRejection.RB03(.eml)
REM_RelayRejection.RB04(.eml)
REM_RelayRejection.RB05(.eml)
REM_RelayRejection.RB06(.eml)
REM_RelayRejection.RB21(.eml)
```

2.7.4.5 REM_ RelayFailure

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
REM_RelayFailure.RB02(.eml)
REM_RelayFailure.RB03(.eml)
REM_RelayFailure.RB04(.eml)
REM_RelayFailure.RB05(.eml)
REM_RelayFailure.RB06(.eml)
REM_RelayFailure.RB21(.eml)

# The following are exclusive failure occurring at S-REMS side:
REM_RelayFailure.RB07(.eml)
REM_RelayFailure.RB08(.eml)
REM_RelayFailure.RB09(.eml)
```

```
REM_RelayFailure.RB10(.eml)
REM_RelayFailure.RB22(.eml)
```

2.7.4.6 REM_ContentConsignment

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
REM_ContentConsignment1.RD01(.eml)    [for the first user]
REM_ContentConsignment2.RD01(.eml)    [for the second user]
```

2.7.4.7 REM_ContentConsignmentFailure

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
REM_ContentConsignmentFailure1.RD03(.eml)    [for the first user]
REM_ContentConsignmentFailure1.RD04(.eml)    [for the first user]
REM_ContentConsignmentFailure1.RD05(.eml)    [for the first user]
REM_ContentConsignmentFailure1.RD06(.eml)    [for the first user]
REM_ContentConsignmentFailure1.RD21(.eml)    [for the first user]
REM_ContentConsignmentFailure2.RD03(.eml)    [for the second user]
REM_ContentConsignmentFailure2.RD04(.eml)    [for the second user]
REM_ContentConsignmentFailure2.RD05(.eml)    [for the second user]
REM_ContentConsignmentFailure2.RD06(.eml)    [for the second user]
REM_ContentConsignmentFailure2.RD21(.eml)    [for the second user]
```

2.7.5 ERDS evidence – Intra-REM-flow examples inside REM baseline circuit (TUC1)

2.7.5.1 SubmissionAcceptance – SubmissionRejection

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
SubmissionAcceptance.RA01(.xml)
SubmissionRejection.RA02.xml
```

```
SubmissionRejection.RA03.xml
SubmissionRejection.RA05.xml
SubmissionRejection.RA06.xml
```

2.7.5.2 RelayAcceptance – RelayRejection – RelayFailure

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
RelayAcceptance.RB01.xml
RelayRejection.RB02(.xml)
RelayRejection.RB03(.xml)
RelayRejection.RB04(.xml)
RelayRejection.RB05(.xml)
RelayRejection.RB06(.xml)
RelayRejection.RB21(.xml)
RelayFailure.RB02(.xml)
RelayFailure.RB03(.xml)
RelayFailure.RB04(.xml)
RelayFailure.RB05(.xml)
RelayFailure.RB06(.xml)
RelayFailure.RB21(.xml)

# The following are exclusive failure occurring at S-REMS side:
RelayFailure.RB07(.xml)
RelayFailure.RB08(.xml)
RelayFailure.RB09(.xml)
RelayFailure.RB10(.xml)
RelayFailure.RB22(.xml)
```

2.7.5.3 ContentConsignment – ContentConsignmentFailure

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
ContentConsignment1.RD01(.xml)    [for the first user]
ContentConsignment2.RD01(.xml)    [for the second user]
ContentConsignmentFailure1.RD03(.xml)    [for the first user]
ContentConsignmentFailure1.RD04(.xml)    [for the first user]
ContentConsignmentFailure1.RD05(.xml)    [for the first user]
ContentConsignmentFailure1.RD06(.xml)    [for the first user]
ContentConsignmentFailure1.RD21(.xml)    [for the first user]
ContentConsignmentFailure2.RD03(.xml)    [for the second user]
ContentConsignmentFailure2.RD04(.xml)    [for the second user]
ContentConsignmentFailure2.RD05(.xml)    [for the second user]
ContentConsignmentFailure2.RD06(.xml)    [for the second user]
ContentConsignmentFailure2.RD21(.xml)    [for the second user]
```

2.7.6 original messages – Outflow examples to non-ERDS systems (TUC2)

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

Used for Outflow (towards non-ERDS systems – REM messages in § 2.7.7):

```
original_messageExt.clean_from_user(.eml)
original_messageExt.eml.to_attach
original_messageExt.eml.to_attach.digest
```

2.7.7 REM dispatch / REMS receipts – Outflow examples to non-ERDS systems (TUC2)

2.7.7.1 REM_Dispatch (RelayedToNonERDS) – REM SubmissionAcceptance

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
REM_DispatchExt.RA01(.eml)
REM_SubmissionAcceptanceExt.RA01(.eml)
```

2.7.7.2 REM_RelayToNonERDS

Si veda l'esempio contenuto nel file:

See the example contained in the file:

REM_RelayToNonERDS.RF01(.eml)

2.7.7.3 REM_RelayToNonERDSFailure

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

REM_RelayToNonERDSFailure.RF02(.eml)
REM_RelayToNonERDSFailure.RF03(.eml)
REM_RelayToNonERDSFailure.RF51(.eml)

2.7.8 ERDS evidence – Outflow examples to non-ERDS systems (TUC2)

2.7.8.1 SubmissionAcceptance – SubmissionRejection

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

SubmissionAcceptanceExt.RA01(.eml)
SubmissionRejection.*: see files at § 2.7.5.1 for RA02, RA03, RA05 and RA06 Reason Codes that are similar also for these Outflow examples.

2.7.8.2 RelayToNonERDS – RelayToNonERDSFailure

Si veda l'esempio contenuto nel file:

See the example contained in the file:

RelayToNonERDS.RF01(.xml)
RelayToNonERDSFailure.RF02(.xml)
RelayToNonERDSFailure.RF03(.xml)
RelayToNonERDSFailure.RF51(.xml)

2.7.9 original messages – Inflow examples from non-ERDS systems (TUC3)

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

Used for Inflow (from non-ERDS systems – REM messages in § 2.7.10):

```
original_messageFromExt.clean_from_user(.eml)
original_messageFromExt.eml.to_attach
original_messageFromExt.eml.to_attach.digest
```

2.7.10 REM dispatch – Inflow examples from non-ERDS systems (TUC3)

2.7.10.1 REM_EXTERNAL (ReceivedFromNonERDS)

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
REM_EXTERNAL.RF04(.eml)
```

2.7.11 ERDS evidence – Inflow examples from non-ERDS systems (TUC3)

2.7.11.1 ReceivedFromNonERDS

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
ReceivedFromNonERDS.RF04(.xml)
```

2.7.12 Full flows with mixed cases

2.7.12.1 Inside-REM service provider delivery and use of Cc:

Si veda l'esempio completo contenuto nel seguente folder:

See the full example contained in the following folder:

```
Inside-a-REM-Service-provider
```

2.7.12.2 Between-REM service providers delivery with split of REM dispatch:

Si veda l'esempio completo contenuto nel seguente folder:

See the full example contained in the following folder:

```
Between-REM-Service-providers
```

2.8 Panoramica termini e significati | Summary terms and meanings

2.8.1 Glossario dei termini principali | Glossary of key terms

La seguente tabella riassume alcuni termini chiave ed il loro significato inteso nel presente documento. Dove possibile viene fornito il riferimento alla definizione originale, dalla quale si è tratta ispirazione, per fornire una descrizione non formale ma contestualizzata allo scopo esclusivo del presente documento, che è da intendere puramente esemplificativo e non esaustivo.

Eventuali effetti legali, responsabilità e/o gli usi finali che possono effettivamente scaturire da tali definizioni sono out of scope rispetto alla presente policy.

The following table summarizes some key terms and their meanings as intended in the present document. Where possible, reference is given to the original definition, from which inspiration was drawn, to provide a non-formal but contextualised description just for the purpose of the present document, which is bound to be purely illustrative and non- exhaustive.

Possible legal effects, accountability and/or the end-uses that can effectively arise from such definitions are out of scope in respect to the present policy.

Table 16 – Glossary of key terms

Business term (IT/EN)	Technical term	Description (*)	Reference
utente/user	**User**	The technical term ***user*** is used, in the referenced standards, in multiple shades depending on the business context and the level of detail the text assumes, or the particular concept that it would like to highlight. In fact, in its most general meaning, it stands for the ***natural person*** or ***ERD-UA*** or ***natural person/ERD-UA*** representing the ***legal person*** (subscribed by the **owner** to the ***qualified electronic registered delivery service***, as outlined below) to whom the service is provided, as an ***end-user***. And also, it takes a further level of details when mentioned in the text, for instance, in its **Sender** and/or **Recipient** role including the meanings illustrated in the following rows.	EN 319 532-1 **[1]** EN 319 521 **[8]**
	Sender	*Natural person* or ***ERD user agent/application (ERD-UA)*** who accesses a **mailbox** provided with the ***qualified electronic registered delivery service*** through their **credentials** to submit the ***user content*** addressed to the ***recipient****(s)*,	EN 319 532-1 **[1]**
	Recipient	*Natural person* or ***ERD-UA*** who accesses a **mailbox** provided with the ***qualified electronic registered delivery service*** through their **credentials** to access the ***user content*** sent from the ***sender*** through/and made available by the service.	EN 319 532-1 **[1]**
utenza/account	**User**	The terms *utenza* (representing, in its broadest sense, a plurality of generic users of the service) and *account* are semantically assimilated to the same entity – the ***user***(s) or ***end-user***(s) (as illustrated above) – unless otherwise specified in the context, according to their most general and abstract meaning.	eIDAS Regulation n. 910/2014 EN 319 521 **[8]**
titolare/owner (**)	**User**	The terms *titolare* (representing the **Customer** or **Cliente** of the service) and *owner* stands for the ***natural*** or ***legal person*** that *subscribes* (registers) to the ***qualified electronic registered delivery service*** as **registered holder** – at a ***QERDSP*** from which is ***established the identity*** (by his/her ***initially identity verification*** as ***natural person*** or ***natural person representing the legal person***) – and that can assume the right to *suspend*, *cease, revoke* or migrate the service as a whole (or even just partially, as a specific domain or a selection of users and/or mailboxes bound with the subscribed service).	eIDAS Regulation n. 910/2014 EN 319 521 **[8]**
casella/mailbox	**registered email**	The *storage area* linked and identified by an ***email address***. In the context of ***Registered Electronic Mail (REM)***, that is a ***particular instance of Electronic Registered Delivery Service***, the mailbox represents the place or area where a **REM message** (envelope containing the ***user content***) is sent, received and/or stored.	EN 319 532-1 **[1]** EN 319 532-4 **[4]**
credenziali/credentials	**authentication means**	This term represents the typical *security information* and/or *technology* allowing to verify ***user***'s identity and the relevant authorization enabling to use the service (for instance by ***an authentication means*** bound to the ***user***, by the ***QERDSP***, during the ***initial identity verification***). The most used authentication mechanism is currently the ***multifactor authentication*** (***MFA***) that foresees two or more different categories of credentials. If required for instance in particular usage contexts, this term can be also intended according to a more general and abstract meaning. All this so that the ***authentication mechanism*** is afterwards adapted, accordingly with the current best practices (see § 2.6.1) and the prescribed security level, for the specific circumstance.	EN 319 521 **[8]** EN 319 401 **[11]**

(*) The text in the present column does not intend to establish a redefinition of the terms but, rather, to provide a high-level description and exemplification of any term in the contexts of application of the present document and with particular regards to **REM-Policy-IT**, taking inspiration (for instance concerning all the terms in ***Bold-Italic*** inside the description) from the various sources' definitions provided in the Reference's column.

(**) EXAMPLE: The company Bianchi & Verdi S.p.A requires a number of **mailboxes** for itself and its employees, of which some **mailboxes** for a "functional" use or of an "institutional" nature.
For instance, "Bianchi & Verdi S.p.A" is the **customer** (the legal person) and **owner**; and a natural person representing the **owner**, (e.g. a person of the secretariats of the chief executive officer) will physically proceed with the ***initial identity verification*** and with the further administrative processes in managing the contract.
A possible scenario illustrating the present example is the following:

(1) *bianchi-e-verdi@bianchi-verdi-rem.it* for a **mailbox** of which "*Bianchi & Verdi S.p.A*" is the **owner**;

(2) *mario.rossi@bianchi-verdi-rem.it*, and similar, are **mailboxes** for the employees of "*Bianchi & Verdi S.p.A*" and for which "*Bianchi & Verdi S.p.A*" is the **owner**.
There could be also specific circumstances where *mario.rossi@bianchi-verdi-rem.it* (bound also to some other domain like *mario.rossi@other-domain.it*) are **mailboxes** for employees of "*Bianchi & Verdi S.p.A*" but used for some specific purpose; and in this case a specific ***initial identity verification*** of the ***end-user*** employees could be required during the activation and release phase of the **mailboxes'** credentials;

(3) *ufficio-legale@bianchi-verdi-rem.it* is a "functional" or "institutional" nature **mailbox** of which "*Bianchi & Verdi S.p.A*" is the **owner**, and it represents "*Bianchi & Verdi S.p.A*" for the specific purpose.

2.9 Raccomandazioni per sviluppatori ed integratori | Recommendation for developers and system integrators

2.9.1 Raccomandazioni generali | General recommendation

La presente sezione contiene delle raccomandazioni per il software utilizzato per implementare il servizio REM e/o per le varie integrazioni applicative che dovessero utilizzare la REM come mezzo per offrire nuovi servizi.

I punti chiave sono: privilegiare l'aspetto della robustezza, in modo da massimizzare la resilienza del sistema complessivo soprattutto in ordine all'integrabilità con l'universo applicativo che ne fa uso e all'interoperabilità cross-border tra REMSP.

The present section contains recommendations for the software used to implement the REM service and/or the various applicative integrations that should use the REM as a means to offer new services.

The key points are: privileging robustness aspect, in a way to maximize the resilience of the overall system especially in order to the integration with the applicative universe that use it, and to the cross-border interoperability.

2.9.2 Resilienza rispetto ai formati | Resilience with regard to the formats

Nel caso in cui i messaggi provengano da oltre confine o da altre policy (e quindi, pur

In case of a message that comes from outside the border or from other policy

aderendo alla REM baseline, non è assicurato che rispettino i limiti che sono dichiarati localmente nella **REMID policy**=**REM-Policy-IT**) è necessario che l'intero sistema, attraverso delle caratteristiche di robustezza, offra il massimo delle garanzie affinché "il trasporto" dello user content (rappresentato dall'*original message*) e delle relative ERDS evidence sia assicurato da punto a punto.

Tale comportamento assicura di per sé una considerevole forma di interoperabilità coerentemente a quanto riportato nello standard (si veda EN 319 532-4 **[4]**, Clause B.2) e alle prescrizioni del **Regolamento eIDAS n.910/2014**. Eventuali effetti legali e/o gli usi applicativi che possono effettivamente scaturire da tale forma di trasporto sono out of scope rispetto alla presente policy.

I seguenti punti forniscono delle raccomandazioni su come impostare questa resilienza legata alla garanzia del "trasporto".

1. Evitare le scorciatoie che possano sembrare in un primo momento molto comode ma poi, alla lunga, portano ad un irrigidimento del sistema.

2. Non è raccomandato basarsi sugli header delle buste MIME soprattutto quando questi si trovano al di fuori del perimetro protetto dalla firma digitale (cioè esterni alla sezione protetta

(therefore, even if they adhere to the REM baseline, it is not ensured that they respect the limits that are declared locally in the **REMID policy**=**REM-Policy-IT**) it is necessary that the whole system, through the robustness, offer the best guarantee in order that the "transport" of the user content (represented by the *original message*) and the relevant ERDS evidence is assured from point to point.

Such behaviour is per sé a considerable form of interoperability coherently in line with the standard (see EN 319 532-4 **[4]**, Clause B.2) and to the **eIDAS Regulation n. 910/2014**. Possible legal effects and/or the applicative uses that can effectively arise from such form of transport are out of scope in respect to the present policy.

The following points give some recommendations how to get this resilience related to the "transport" assurance.

1. avoid short-cuts that seems at first sight comfortable but after, can lead to an inflexibility of the system.

2. It is not recommended rely too much on the headers of MIME envelops mostly when these are outside of the protected perimeter of the digital signature (i.e., external to the pkcs7-signature protected section). The reference to these headers

dalla pkcs7-signature). Il riferimento a questi header può servire per una scrematura iniziale del processing del REM message ma non per asserire delle assunzioni che abbiano a che vedere rispetto alla "**assicurazione**" e alle garanzie della comunicazione, nel senso della specifica REM. Infatti, tutti questi aspetti di rilievo che danno una determinata "valenza" al messaggio (ed al suo transito nelle componenti che costituiscono il servizio di trasporto) si devono trovare (e si trovano) all'interno dell'ERDS evidence o dell'*original message*. Tra questi header si menzionano alcuni quali il Subject, il From, etc. di cui, per le suddette ragioni se ne sconsiglia un uso applicativo.

Un sistema resiliente NON basa le proprie scelte sul formato del Subject e/o del From (che possono subire o meno delle trasformazioni incontrollate). Ad es. la presenza del formato tipo "On behalf of user@rem_md_x.com <service_rem_md_x@rem_md_x.com>" è sicuramente garantito all'interno della **REMID policy=REM-Policy-IT**; ma NON è detto che messaggi provenienti da altre policy, anche se aderenti alla REM baseline, rispettino questa comoda "convenzione". Analogo discorso può essere trasposto al *MIME header component* rappresentato dal Subject.

Quindi, un approccio prudenziale rispetto a questioni importanti sui flussi dei messaggi, e a

could be useful for an initial skimming of the REM message processing, but not to assert assumptions that have to do with the "**assurance**" of communication, in the sense of the REM specification. Indeed, all these relevant aspects that give a determined "status" to the message (and to its transit through the components constituting the transport service) must be identified (and they are found) inside the ERDS evidence or the *original message*.

Among these headers, some like Subject, From, etc. are cited here, for which, for the above said reasons, it is not recommended an applicative usage.

A resilient system does not base any choice on the Subject and/or the From format (which may or may not undergo uncontrolled transformations). E.g. the presence of the type "On behalf of: sender@s-rems-only-for-test.it <rem-service@s-rems-only-for-test.it>" is definitely ensured inside the **REMID policy=REM-Policy-IT**; but there absolutely no reason to believe that messages coming from other policies, even if adhering to REM baseline, respect this "conventions". The same rational is applicable to the Subject *MIME header component*.

In conclusion, a cautious approach for important questions in respect to the flow of

decisioni da prendere su di essi è sempre la miglior strategia. Spesso, per avere un dato certo, risulterà quindi necessario recuperarlo all'interno della ERDS evidence (che è autoritativa) o dell'*original message*. Oppure utilizzare header previsti dallo standard, ma solo quando questi si trovino all'interno della zona del **S/MIME** protetta da firma digitale.

the messages, and to decisions to take on it is always the best strategy. Often, to get a certain element, will result necessary to retrieve it into the ERDS evidence (that is authoritative) or from the *original message*. Or to use headers required by the standard, but only when these are inside the of the **S/MIME** zone protected by the digital signature.

2.9.3 Resilienza rispetto alle S/MIME extension | Resilience with regard to S/MIME extensions

Anche nel caso delle **S/MIME** extension (previste dallo standard REM) valgono considerazioni simili a quelle fatte nel § 2.9.2 sugli header. Qui viene considerata la presenza o meno di MIME part addizionali che rientrino nelle suddette estensioni.

Così come per le raccomandazioni del § 2.9.2, i sistemi REM e le varie applicazioni che vi afferiscono all'interno della **REMID policy=REM-Policy-IT** devono manifestare delle forme di resilienza rispetto alla presenza body part addizionali (nella struttura MIME dei REM message in arrivo) rientranti nello schema di estensioni **S/MIME** dello standard REM.

Il REM service deve offrire tutte le garanzie affinché "il trasporto" dello user content

Similar considerations apply even in case of the **S/MIME** extensions (foreseen by the REM standard), as per the § 2.9.2 on the headers. The presence of additional MIME parts that fall in the aforementioned extensions is considered here.

As per the recommendations of § 2.9.2, the REM systems and the various applications that use them inside the **REMID policy=REM-Policy-IT**, have to manifest forms of resilience in respect to additional body parts (in the MIME structure of incoming REM messages) that fall in the **S/MIME** extension scheme of the REM standard.

The REM service has to offer the best guarantee in order that the "transport" of

(rappresentato dall'*original message*) e delle relative ERDS evidence sia assicurato da punto a punto.

Ciò costituisce una seconda considerevole forma di flessibilità nell'interoperabilità. Poi, gli effetti legali e/o gli usi applicativi che possono effettivamente scaturire da tale trasporto sono out of scope rispetto alla presente policy.

the user content (represented by the *original message*) and the relevant ERDS evidence is assured from point to point.

This constitutes a second considerable form of flexibility during the interoperability. Then, the legal effects and/or the applicatory uses that can effectively arise from such transport are out of scope in respect to the present policy.