AGID
Agenzia per l'Italia Digitale

Gestione servizi Infrastrutturali

REM SERVICES – Criteri di adozione degli standard ETSI – Policy IT

Versione 1.1

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 le nuove Regole tecniche conformi ai requisiti funzionali previsti per un servizio elettronico di recapito certificato qualificato dal Regolamento eIDAS, 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.

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 principali degli standard ETSI

CSI: Common Service Infrastructure

ERDS: Electronic Registered Delivery Services

REM: Registered Electronic Mail

REMID: REM Interoperability Domain

REMSP: Registered Electronic Mail Service Provider

REMS: Registered Electronic Mail Service

R-REMS: Recipient's REMS

S-REMS: Sender's REMS

Per maggiori dettagli sul significato di questi termini e sulla specifica terminologia utilizzata nell'intero documento si faccia riferimento ai documenti indicati al paragrafo § 4.1 e, in particolare, a EN 319 532-1 **[1]** ed EN 319 522-1 **[5]**.

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

2 L'approccio seguito da AGID

Gli articoli 43 e 44 del Regolamento eIDAS definiscono gli effetti giuridici di un servizio elettronico di recapito certificato e i requisiti funzionali per i servizi elettronici di recapito certificato qualificati.

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 lo sviluppo 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.

La REM è una particolare "istanza" di un ERDS che si basa sui protocolli della posta elettronica e i relativi standard.

Le attività del TC ESI, realizzate in accordo con un significativo numero di stakeholders, si sono concluse nel febbraio del 2019 e gli standard ETSI sono stati pubblicati nel mese di giugno 2019.

AGID 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.

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, responsabile per Agid del servizio *Gestione servizi Infrastrutturali*.

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, ITnet, 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 e risulta la soluzione più prossima alla PEC.

La scelta tiene conto dei livelli di diffusione che ha raggiunto la PEC in Italia: alla data di stesura del presente documento (febbraio 2021) i Gestori che erogano il servizio sono 18, il numero di caselle di PEC attive supera i 12 milioni, con una stima per l'anno 2021 di superare i 2,5 miliardi di messaggi di PEC scambiati. 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 dell'accreditamento, 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 al nuovo sistema 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, con performance difficilmente eguagliabili 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.

I protocolli utilizzati dagli ERDS non avrebbero garantito un'adeguata rispondenza ai punti elencati, pur non essendo preclusi da evoluzioni future.

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, Trusted List 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 Comitato ESI per una condivisione, presentando un documento analitico con le relative evidenze e alcune proposte di soluzione, avviando così un'importante collaborazione orientata a fare chiarezza indirizzando le osservazioni ricevute nella modalità ritenuta più opportuna.

Da tale collaborazione, che ha dato il via ad una analisi dettagliata del materiale preparato dal GDL, il Comitato ESI ha prodotto, come primo risultato, una nuova versione dell'EN 319 532-4 **[4]**, uno dei documenti costituenti il set dello standard della REM e pubblicato in forma di draft il 28 gennaio 2021, che introduce la **REM baseline,** pienamente allineata con i risultati del GDL in ambito Common Service Interface, Trusted List e time-stamp.

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 come **riferimento principale** dal presente documento, connessa e rapportata alle varie scelte addizionali necessarie per la transizione del servizio PEC emerse seguendo quanto indicato sopra come **razionale**.

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***.

Per ultimo, il GDL 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. 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 dalla **REM-Policy-IT**;

L'allegato, per quanto sopra, si prevede fin da ora che non possa essere un documento "stabile": andrà aggiornato nel tempo per recepire, quando possibile, la dinamica intrinseca dei servizi digitali coinvolti.

4 Analisi documentazione ETSI

4.1 I documenti di riferimento

In questo documento si usano i termini "standard" e "standardizzazione" al posto dei termini formalmente corretti di "norma" e "normazione" come da Regolamento (UE) 1025/2012 sulla normazione europea per una maggiore fruibilità.

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 che 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 [REM - Part 1 Framework and architecture]
- **[2]** ETSI EN 319 532-2 V1.1.1 [REM - Part 2 Semantic contents]
- **[3]** ETSI EN 319 532-3 V1.2.1 [REM - Part 3 Formats]
- **[4]** Draft ETSI EN 319 532-4 V1.1.3 (2021-01) [REM - Part 4 Interoperability profiles (including the new REM baseline)]
- **[5]** ETSI EN 319 522-1 V1.1.1[2] [ERDS - Part 1 Framework and architecture]
- **[6]** ETSI EN 319 522-2 V1.1.1 [ERDS - Part 2 Semantic contents]
- **[7]** ETSI EN 319 522-3 V1.1.1 [ERDS - Part 3 Formats]
- **[8]** ETSI EN 319 521 V1.1.1 [Policy and security requirements for ERDSP]
- **[9]** ETSI EN 319 531 V1.1.1 [Policy and security requirements for REMSP]

Come si evince dal prefisso "ETSI EN", questi sono tutti classificati come European Standard[3]. Nella valutazione dei precedenti documenti è stato necessario integrare i contenuti prendendo a riferimento anche gli omologhi documenti - quando "normativamente connessi" - che fanno riferimento al modello funzionale ERDS e che sono individuati 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 del documento EN 319 532-1 **[1]**. Invece la mappa del set completo di standard "normativamente" connesso e costituente i concetti cardine per

[2] Alla data di stesura del presente documento l'EN 319 532-4 [4] è disponibile in forma di draft e potrà subire variazioni. È possibile monitorare lo stato corrente del documento sul sito ETSI al seguente indirizzo:
https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=59579

[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.

l'interoperabilità della **REM baseline** è riportato nella Table 24 (CSI) e Table 35 (digital signature & time-stamp) del documento EN 319 532-4 **[4]**.

4.2 Modalità di notazione dell'analisi

L'approccio è stato analitico, individuando puntualmente e valutando i margini di libertà, associati ai verbi modali ***may*** e ***should***, presenti nel perimetro dei documenti identificati: in altre parole nel set di standard completo riportato al § 4.1 e in quelli legati a questo set nel rispetto ed in coerenza con la **REM baseline**. Tali verbi modali sono utilizzati nel presente documento con lo stesso significato prescrittivo presente nello standard[4]. Per ogni documento è stata prodotta una scheda, i cui contenuti sono di seguito commentati con le decisioni prese collegialmente dal GDL.

Le schede sono definite 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
		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 (a cascata) che conducono e guidano fino al testo che si sta esaminando. ATTENZIONE:

[4] Si rimanda al paragrafo "Modal Verbs Terminology" presente in ogni standard ETSI per la corretta interpretazione di ognuno di questi verbi modali.

per comprendere correttamente l'interpretazione data poi nelle colonne tre e quattro è fondamentale leggere attentamente l'intero paragrafo (di cui un breve stralcio è mostrato in colonna due) 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, oggetto di valutazione e di eventuale scelta da parte del GDL; la seconda sezione riporta lo stesso testo con il verbo modale profilato in base alla decisione del GDL.

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

La quinta colonna riporta le note e le scelte effettuate dal GDL che possono prevedere anche 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 [5] [6] a pag. 16 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 risoluzione del GDL è interamente conclusa nella nota in quinta colonna, senza la necessità di riformulazione del testo sorgente 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" effettuate dal gruppo di lavoro, oltre ad eventuali commenti.

Laddove l'argomento lo ha consentito, sono state inoltre formulate soluzioni tecniche per il recepimento degli standard, nonché proposte di soluzioni raccomandabili ai service provider. Tali contributi sono descritti nell'allegato tecnico.

Circa l'interoperabilità, il GDL ha considerato utile garantire due distinti livelli: un **primo livello**[5] specifico per i sistemi di recapito certificato qualificato italiani (e cioè all'interno del REMID policy=REM-Policy-IT), ed un **secondo livello**[6] per l'interazione con sistemi di recapito certificato qualificato appartenenti ad altre REMID policy (anche se comunque aderenti alla **REM baseline**).

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

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 V.1.1.3 **[4]** che consente di individuare il punto dove l'argomento in questione è trattato.

[5] 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".

[6] 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. **shall=REM-Policy-IT**, **should=interoperabilità**.

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 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, il GDL constata che:

1. le ERDS evidence[7] 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 considerazioni sopra, seguendo il principio della distanza minima dalla PEC (in accordo al **razionale** in premessa e l'adesione alla **REM baseline**), il GDL ritiene di non dover prevedere 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

[7] 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 verrà implementato con le stesse modalità previste per i log "legali" della PEC (si veda il § 2.4.2.4 dell'allegato tecnico).

Lo standard prevede il servizio opzionale "user directory": nell'uso reale, all'interno della **REM-Policy-IT**, il concetto astratto di "user directory" dello standard è costituito dall'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.

Esisterà inoltre un altro "directory" (visto sempre come termine astratto), con scopi e contenuti differenti dal primo che si ferma a livello di dominio delle caselle, con tutti i domini del circuito (assimilabile all'IGPEC), che dovrà essere gestito da un soggetto terzo (che nel modello PEC è AGID).

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[12] a pag. 28).

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*** **REM baseline [4] Clause C.1** ***Vedi spiegazione sottostante e relativa nota***

B. Store and forward/Store and Notify

Si rileva che nelle parti dello standard che descrivono il servizio REM più ad alto livello lo "style of operation" Store and Forward (abbreviato in S&F da qui in poi) è riportato già da subito come obbligatorio, mentre Store and

Notify (abbreviato in S&N da qui in poi) è considerato opzionale. Nella parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4]** **SMTP Interoperability profile** + **REM baseline**) lo S&N **non è previsto**, mentre, il modello S&F, **ne rappresenta un caposaldo**.

Pertanto, in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, il modello S&N, in questa prima fase, non risulterà applicabile: potrà essere considerato successivamente dopo una più approfondita valutazione delle potenzialità che può offrire (ad es. gestione di file di grandi dimensioni e invii verso utenze non appartenenti al circuito qualificato/certificato)[8].

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.3.6.1, Table 55 item g) Item h)/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.**

[8] Caratteristiche 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 S&F. Inoltre, considerando che i service provider devono fornire servizi qualificati, lo S&N pone delle criticità in ambiente distribuito quali ad es. 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 "ortogonale" al **razionale** in premessa e all'adesione alla **REM baseline**.

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**; il GDL recepisce la non applicabilità, coerentemente con il **razionale** in premessa e l'adesione alla **REM baseline**.

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 37, 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 viene utilizzato il protocollo DNS, opportunamente protetto tramite misure atte a mitigare i rischi di attacchi informatici.

I dettagli del message routing, e più in generale del flusso di comunicazione tra due service provider, viene dettagliato all'interno di 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 4.4) 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.* *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.* 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 19]*** ***[pag 19-20]*** ***[pag 20]***	***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.3.6.1, C.3.6.2, C.3.6.3**

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 non prescrittive che verranno affrontate in dettaglio nel seguito del documento.

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.3.6**

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. 18 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)

Poiché questa fase non include lo S&N, coerentemente con gli obiettivi del **razionale** in premessa e l'adesione alla **REM baseline**, il GDL decide di non adottare le prescrizioni legate ai suddetti eventi.

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 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*** **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 presente per alcuni service provider (notifica debole al destinatario[9]). Il GDL decide di lasciare libera scelta al service provider. Il terzo ***may*** permette al R-REMS di generare ed inviare al mittente una ERDS evidence[10] 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 premessa e l'adesione alla **REM baseline**, questa non viene inclusa nella REMID policy=REM-Policy-IT.

[9] Es. SMS o PEO.

[10] Questa ERDS evidence - non prevista - 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).

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-REMSP e richiesto esplicitamente dall'utente (come previsto nel § 2.4.2.2 dell'allegato tecnico) è possibile venga prodotta questa evidenza verso il mittente che è opzionale e addizionale rispetto alla **REM baseline**.

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** la posizione del GDL è di implementarlo. 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 dispacth** **REM payload non applicabile** **REM baseline [4] Clause C.1, C.3.6.1, Table 55 Item a)** **Il REM payload è un'opzione della REM che è usata nella forma "detached" dell'evidenza dal 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.3.6.1, Table 55 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 REM receipt.

Come argomento collegato alle ricevute, 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)[11].

[11] Si noti che la ricevuta di consegna riveste un significato molto importante in quanto chiude il ciclo di comunicazione "assicurata" da un mittente "registrato" presso un REMSP fino ad un destinatario "registrato" presso un secondo REMSP, e si può definire pienamente consegnata nella mailbox del destinatario solo al completamento della transazione con il ricevimento della **ContentConsignment** REM receipt (si veda § 2.2 e **Table 1** 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 38 Item b.2.1.2)** **Nella parte di standard in esame si parla di TRUST e per esso si usa la Trusted List!**
		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 38 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

Il GDL conferma l'adozione di un modello che faccia riferimento alla EU Trusted List (TL)[12], in accordo alle prescrizioni della **REM baseline**.

[12] 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 V1.1.1 [ERDS (for REM) - Part 2 Semantic contents]

Per via della compliance con eIDAS nella REM sono richiamati i concetti di "identificazione" e "autenticazione" come indicato negli standard EN 319 521 **[8]** ed EN 319 531 **[9]** 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 standard).

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.3.5, Table 54 ed in particolare gli Item g,h,i,l**
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.3.5, Table 54 ed in particolare gli Item g,h,i,l**
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.3.5, Table 54 ed in particolare gli Item g,h,i,l**

A1-A2-A3. Identity verification assurance levels information

Il GDL recepisce il punto a) (***shall***) e per i punti b) c) d) (***may***), poiché questi ultimi non introducono elementi concreti di garanzia o valore aggiunto, i service provider avranno, comunque, la facoltà di implementare i ***may*** ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** (nel rispetto delle condizioni riportate nella nota[19] a pag. 43; si veda anche il § 2.8.2 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.3.2 Table 51 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.3.3 Table 52 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.3.2 Table 51 Item b) per il CAdES** **Clause C.3.3 Table 52 Item d) per lo XAdES**
		4) A signature time-stamp shall be added to the digital signature of evidence; with CAdES signature, the B-T signature level shall be used.		**SI - shall** **REM baseline [4]** **Clause C.3.4 Table 53 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.

Il GDL recepisce le varie prescrizioni come indicato nella suddetta tabella relativamente alla REMID policy=REM-Policy-IT.

La firma digitale sull'oggetto S/MIME, costituente il REM message, essendo apposta da un soggetto giuridico, è definita come "sigillo elettronico qualificato".

I punti cardine delle scelte sono la presenza del time-stamp e, al fine di favorire l'interoperabilità, la scelta di applicarlo direttamente all'XML della ERDS evidence, così come prescritto nella **REM baseline**.

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 Table 2** dell'allegato tecnico. Si rimanda, invece, all'apposita Clause C.3 della **REM baseline** contenuta nel documento EN 319 532-4 V1.1.3 **[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		**shall=REM-Policy-IT** ***may*=interoperabilità**

C. <u>Evidence components values</u>

Il GDL conviene di aggiungere obbligatoriamente anche il testo in lingua italiana con uno ***shall***, per la REMID policy=REM-Policy-IT, e di lasciare ***may*** per quanto riguarda i messaggi provenienti da altre REMID policy, per agevolare l'interoperabilità[13].

[13] Si consideri che ci si sta riferendo ai valori che possono essere assunti da ogni "ERDS evidence component" che permetta l'uso di testo libero. Questi sono: G01, M04. Si vedano le Clause 8.2.1, 8.2.26 e 8.3.1 dello standard EN 319 522-2 **[6]**.

4.3.4 ETSI EN 319 532-3 V1.2.1 [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 8]***	**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 9]***	**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

Scelta rilevante solo quando si supporta lo S&N. La scelta del GDL è di non accettare *may*, per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** che non prevede di supportare 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 9]***	**Non applicabile** **REM baseline [4]** **Clause C.1** **Si veda spiegazione sottostante**

C. Internet Message Format in the REM services

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 basato esclusivamente sull'**SMTP**.
La scelta del GDL è di non accettare ***may***, in quanto l'adesione alla **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 10]***	**Si conferma il testo originario**

D. Internet Message Format in the REM services

L'apertura, rappresentata dall'uso di ***should*** nello standard, permette di poter effettuare alcune modifiche all'"original message"[14] (ad es. la re-impostazione del Message-ID, come avviene nella PEC)[15]. Considerato però questo requisito del regolamento europeo riportato nella nota[15], bisogna limitare i cambiamenti degli header a cosa è effettivamente necessario.
Inoltre, la specifica implementazione (cioè il set di profili usati/definiti a livello di **REM-Policy-IT**) deve pienamente definire 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 ed i requisiti al § 2.4.2.2 ed esempi al § 2.7 dell'allegato tecnico per i dettagli realizzativi.

[14] 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".

[15] 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.

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 10]***	**Non applicabile** **REM baseline [4] Clause C.1**

E. REM message - Structure Definition

Il suddetto ***may*** (nella prima parte della frase) non può essere accolto in toto a livello di policy REMID policy=REM-Policy-IT. Infatti, lo standard EN 319 532-1 **[2]** è molto aperto 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**) è basato esclusivamente sull'**SMTP**. Il GDL decide di non accogliere ***may*** 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 10]***	**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 11]***	**Si conferma il testo originario**

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. Le regole tecniche possono fornire un minimo di struttura da dare a questo testo, un po' come avviene oggi nel testo che

compare nella busta della PEC (si vedano il § 2.4.2.6 e gli esempi al § 2.7 dell'allegato tecnico).

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 11]***	Si conferma il testo originario

H. 4.3 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. Le regole tecniche possono fornire un minimo di struttura da dare a questo testo (si vedano gli esempi al § 2.7 dell'allegato tecnico), come per il punto precedente. Il contenuto informativo per l'utente di queste due parti *plain text/HTML* deve essere identico. Infatti, questa parte HTML del MIME e la precedente TXT non sono altro che due facce della stessa medaglia (due parti "alternative" del MIME) che un client può usare ed interpretare[16] 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**.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
I	**4.3 REM message - Structure Definition** ***Fig. 2 - REM 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 12]***	Si conferma il testo originario

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

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

[16] 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
J	**4.3 REM message - Structure Definition** ***Fig. 2 - REM 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 12]***	**Si conferma il testo originario**

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

Anche il testo di accompagnamento alla **REM receipt** può contenere del testo HTML libero di spiegazione. Valgono anche per la REM 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 13]***	**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, il GDL decide di non recepire i suddetti ***may*** 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 13]***	**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 GDL decide di non recepire ***may*** 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 14]***	**Non applicabile** **REM baseline [4]** **Clause C.1** **Il REM payload è un'opzione della REM che è usata nella forma "detached" dell'evidenza dal 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 GDL decide di non recepire ***may*** 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 14]***	**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 GDL decide di non recepire ***may*** 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 15]***	**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 (Table 5 of EN 319 522-2 **[6]**) e in REM (6.2.1 of EN 319 532-2 **[2]**). La Table 2 EN 319 532-3 **[3]** li riassume, e i campi non presenti in tale tabella possono essere non presenti nella struttura

MIME della REM ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**.

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 16]*	
		*- 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.3.6.1, C.3.6.2, C.3.6.3 item c). point IV. I suddetti valori si riflettono anche dai contenuti della ERDS evidence. Clause C.3.5 Table 54 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 l'elemento in discussione nello standard è l'MD14 che, a parte il formato stabilito dalle regole di binding, ha una semantica identica all'elemento M02 (si faccia riferimento agli standard EN 319 522-3 **[7]**, EN 319 532-3 **[3]** e alla **REM baseline [4]** Clause C.3.6.1 elemento c) punto IV. Che spiega come debba essere interpretato, nel contesto e nel binding REM, l'elemento in esame).

Il GDL recepisce le varie prescrizioni dello standard, come indicato nella suddetta tabella. All'interno della REMID policy=REM-Policy-IT deve essere riportato un algoritmo da usare in emissione (che sarà http://www.w3.org/2001/04/xmldsig-more#sha256) e una lista di algoritmi ammessi e tollerati (ad esempio per comunicazioni provenienti da altre policy). Questi algoritmi sono rappresentati sottoforma di URI e ripresi dall'RFC 6931, in accordo allo standard EN 319 532-3 **[3]** e alla seguente disposizione della **REM baseline [4]** (c.f. Clause C.3.6.1 punto c) punto 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 **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 16]***	**SI – shall** **REM baseline [4]** **Clause C.3.6.1, C.3.6.2, C.3.6.3 item c) point 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.3.5 Table 54 item l).** **L'elemento in discussion coinvolge gli elementi MD14 e M02. La REM baseline conferma shall.**

Q. General requirements Table 2

Il GDL recepisce la codifica **base64** in accordo alle prescrizioni della **REM baseline**.

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. 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 16]***	**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.3.5 Table 54 item l).** **I suddetti valori si riflettono anche dai contenuti della ERDS evidence (*AppLayerIdentifier*).**

R. General requirements Table 2

Il GDL decide di fissare il requisito che l'eventuale Message-ID specificato dal client utente nell'original message venga "salvato" nell'header REM-

UAMessageIdentifier[17] di ogni REM message, per la REMID policy=REM-Policy-IT, e di lasciare ***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 § 2.4.2.2 ed esempi al § 2.7 dell'allegato tecnico per i dettagli realizzativi.

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 16]***	**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.3.5 Table 54 elements 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[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 riguardo gli aspetti relativi alla resilienza e si veda anche il punto successivo che vale in generale e non solo riguardo gli eventuali allegati).

[17] 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 entrare nel merito 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 – in fallback - all'interno della ERDS evidence (si veda 2.8.2 dell'allegato tecnico).

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 16]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

T. General requirements Table 2 – Extensions

Questa scelta 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[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 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 17]***	**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, per il quale si lascia la libertà (nel rispetto delle condizioni riportate nelle note[18] [19]). Si rimanda alle apposite prescrizioni al § 2.3.2.2 dell'allegato , che

[18] Il REM message prodotto dai vari service provider deve avere una firma digitale (o **"sigillo") CAdES compliant** in accordo alla sezione C.3 della REM baseline (si veda anche punto "B. Common requirement for digital signatures." del § 4.3.3, pag. 32 del presente documento).

[19] 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 della scelta 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 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.

specificano, più nel dettaglio, le varie scelte relative al sigillo da applicare ai REM message. In particolare, il parametro *micalg* può essere ulteriormente selezionato ed appartenere ad un set ristretto di valori previsto nelle best practice di sicurezza correnti.

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
V	**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 17]***	
		The value for this header field ***shall*** be an UID…		**shall=REMPolicy-IT** **REM baseline [4] Clause C.3.5 Table 54 punto k).** **I suddetti valori si riflettono anche dai contenuti della ERDS evidence.**

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

In merito alla suddetta tabella si conferma ***shall*** come definito, al punto su indicato, nella **REM baseline**. 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 nei servizi governati dalla REMID policy=REM-Policy-IT è opportuno implementare un meccanismo assolutamente analogo. 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
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 17]***	
		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

Così come nella PEC vi è una trasformazione del "FROM", per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, anche nei servizi governati dalla REMID policy=REM-Policy-IT è opportuno implementare un meccanismo assolutamente analogo accogliendo la scelta e il suggerimento fornito dallo standard. Il GDL conviene quindi di impostare il suddetto requisito con ***shall***, per la REMID policy=REM-Policy-IT, e di lasciare ***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 17]***	
		… 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.3.6.1** **Table 55 punti g) & h).** **Clause C.3.6.2** **Table 57 punti g) & h).** **Nei casi di SubmissionAcceptance, SubmissionRejection e RelayFailure è implicitamente riportato nei suddetti punti che la REM receipt è 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 ogni ricevuta ha il campo: *To: [mittente originale]*
per coerenza con il **razionale** in premessa e l'adesione alla **REM baseline**, anche nei servizi governati dalla REMID policy=REM-Policy-IT viene recepita la scelta di ***shall*** al posto di ***may*** 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 17]***	
		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**, il GDL decide di fissare come obbligatoria la suddetta scelta nei servizi governati dalla REMID policy=REM-Policy-IT con uno ***shall***, e di lasciare ***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 17]***	**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 § 2.8.2 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> * REM receipt relativa all'accettazione/non-accettazione: **REM SubmissionAcceptance**: <oggetto originale> **REM SubmissionRejection**: <oggetto originale> * REM receipt relativa alla consegna/non-consegna: **REM ContentConsignment**: <oggetto originale> **REM ContentConsignmentFailure**: <oggetto originale> * REM 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**, il GDL decide di fissare come obbligatoria la suddetta scelta nei servizi governati dalla REMID policy=REM-Policy-IT con uno ***shall***, e di lasciare ***should*** per quanto riguarda eventuali ricevute e messaggi provenienti da altri REMID policy. Al fine di facilitare l'interoperabilità si deve essere in grado di ricevere qualsiasi altra forma di subject (si veda l'allegato tecnico al § 2.8.2 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 17]***	
		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 policy italiana 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

Il GDL decide di fissare questo requisito con uno ***shall*** per la REMID policy=REM-Policy-IT, e di lasciare ***should*** (cui lo ***shall*** si riferisce, e 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***.

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 17]***	
		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 policy italiana 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** il GDL decide di rendere obbligatoria, con uno ***shall***, la corrispondenza del suddetto header del REM dispatch e dell'*original message*, per la REMID policy=REM-Policy-IT. Si lascia ***should*** per quanto riguarda i REM dispatch provenienti da altre REMID policy, per agevolare l'interoperabilità.

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 17]***	
		Return-Path: REMS ***conditionally shall*** assign…		***conditionally shall*=REM-Policy-IT** ***may*=interoperabilità** **Il REMS, quando (e solo quando) il client specifica tale header, nella policy italiana ripropone lo stesso header a livello di busta del REM dispatch (questa obbligatorietà complete 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 per la REMID policy=REM-policy-IT è opportuno implementare un meccanismo analogo accogliendo la scelta fornita dallo standard e restringendola 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.

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 17]***	
		Received: REMS ***conditionally shall*** assign…		***conditionally shall*=REM-Policy-IT** ***may*=interoperabilità** **Il REMS, quando (e solo quando) il client specifica tale header, nella policy italiana 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 per la REMID policy=REM-policy-IT è opportuno implementare un meccanismo analogo accogliendo la scelta fornita dallo standard e restringendola 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.

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 17]***	**Si conferma il testo originario**

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

Si propone di lasciare 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".

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 17]***	**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).

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 18]***	**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. Il GDL lascia aperta 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[17] a pag. 42 e nota[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 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 18]*	**Viene prescritta la codifica base64, ove richiesto, per eventuali header addizionali nei REM messages emessi all'interno della policy italiana.**
		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 spiega 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[20] di pag. 53) viene ristretto ad obbligatorio con uno ***shall*** all'interno della REMID policy=REM-Policy-IT. Si lascia ***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[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 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 19]*	**Si conferma il testo originario 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. Ciò, ovviamente, quando non è possibile usare gli header[20] 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[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 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 19]***	**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, per il quale si lascia libertà (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 19]***	
		REM-Section-Type: The value of this field ***shall*** be: "rem_message/introduction".		**shall**

[20] 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.

KK. REM-Section-Type

Il GDL restringe con uno ***shall*** questa scelta, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 8 Clause 5.4.3.1) questo header è prescritto come obbligatorio[21].

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 19]***	**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, per il quale si lascia libertà (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 19]***	
		• '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 e il GDL stabilisce di fissarlo con uno ***shall*** all'interno della REMID policy=REM-Policy-IT (nel rispetto delle condizioni riportate nella nota[19] a pag. 43 e quanto

[21] Generalmente si usa il razionale di far prevalere le scelte più stringenti presenti nel profilo di interoperabilità definito 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.

deciso, sempre per questo parametro, nei requisiti presenti nel EN 319 532-4 **[4]** Clause 5.4.3.2 al punto 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 19]***	
		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). Il GDL rende il campo *mandatory* per la REM-Policy-IT, e *optional* per l'interoperabilità per messaggi provenienti da altre policy (nel rispetto delle condizioni riportate nella nota[19] a pag. 43 e che 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 19]***	**Si conferma il testo originario**

OO. Content-Transfer-Encoding

Il GDL decide di lasciare libera la scelta (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 20]***	
		• '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 e il GDL stabilisce di fissarlo come indicato (nel rispetto delle condizioni riportate nella nota[19] a pag. 43 e quanto deciso, sempre per questo parametro, nei requisiti presenti nel EN 319 532-4 **[4]** Clause 5.4.3.3 al punto 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 20]***	Si conferma il testo originario

QQ. Content-Transfer-Encoding

Il GDL decide di lasciare libera la scelta (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 20]***	Si conferma il testo originario

RR. Content-Description

Il GDL decide di lasciare libera la scelta (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 20]***	
		REM-Section-Type: The value of this field ***shall*** be "rem_message/original".		shall

SS. REM-Section-Type

Il GDL recepisce e mette in evidenza con uno ***shall*** questa scelta, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 11 Clause 5.4.4), relativo all'interoperabilità, questo header è prescritto come obbligatorio.

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 21]***	
		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 § 2.4.2.2 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 nei servizi governati dalla REMID policy=REM-Policy-IT è opportuno implementare un meccanismo assolutamente analogo, e si denota quindi ciò 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 21]***	**L'intera sezione è opzionale.** **Si conferma il testo originario.**
		• '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 opzionale del MIME

"REM extensions" fosse presente[22]. Lo ***should*** si riferisce ai vari parametri. Il GDL stabilisce come indicato e cioè lasciare libertà rispetto ai primi due parametri e di restringere l'ultimo parametro con uno ***shall*** all'interno della REMID policy=REM-Policy-IT (il tutto sempre alle condizioni riportate nella nota[19] a pag. 43) 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.

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 21]***	Si conferma il testo originario

VV. Content-Description

L'intera sezione è opzionale. Se/quando si rendesse necessario utilizzarla, il GDL decide di lasciare libera scelta riguardo l'header in questione (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 21]***	
		REM-Section-Type: The value of this field ***shall*** be "rem_message/extension".		shall

WW. REM-Section-Type

[22] Si veda a modello esemplificativo 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:

```
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

…
```

L'intera sezione è opzionale. Se/quando si rendesse necessario utilizzarla, il GDL restringe con uno ***shall*** la scelta riguardo l'header in questione, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 12 Clause 5.4.5) questo header è prescritto come obbligatorio.

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 21]***	
		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, il GDL decide di restringere questo requisito con uno ***shall*** all'interno della REMID policy=REM-Policy-IT (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).
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 21]***	**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, il GDL decide di lasciare libera scelta riguardo l'header in questione (ma sempre in coerenza con il **razionale** in premessa e l'adesione alla **REM baseline** e nel rispetto delle condizioni riportate nella nota[19] a pag. 43 e della semantica dell'header).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
ZZ	**6.2.5 REMS extensions MIME Header Fields**	In particular, one of these extensions ***may*** be used to associate an electronic time stamp (see note) to the REM message certifying the date and time of sending, receiving and/or any change/transformation of the message transmitted from the sender to the recipient.	***[pag 21]***	***Non applicabile*** **REM baseline [4]** **Clause C.3.2, C.3.4** ***Il time-stamp è applicato esclusivamente alla ERDS evidence. Si veda in particolare la Nota della Clause C.3.2 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 X-ADES-B-T. Coerentemente con gli obiettivi del **razionale** in premessa e l'adesione alla **REM baseline** il GDL decide pertanto di **non** considerare il ***may***. Si rimanda alle apposite sezioni dello standard EN 319 532-4 **[4]** Clause C.3.2 e C.3.4 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 TTT al § 4.3.4, pag. 68

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 22]***	**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).
In tal caso i dati possono essere strutturati come indicato. Il GDL decide di lasciare libera scelta ai 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[19] a pag. 43 ed in coerenza 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 § 2.8.2 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 22]***	**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 22]***	
		The ERDS evidence ***shall*** be in XML format.		**shall**

CCC. ERDS evidence

Poiché devono essere sempre presenti delle ERDS evidence almeno nel formato XML, il GDL restringe lo ***should*** presente nello standard EN 319 532-3 **[3]** con uno ***shall***, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 14 Clause 5.4.6) 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 22]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1.**

DDD. ERDS evidence

Il GDL decide che le evidenze (come ulteriore allegato rispetto a quanto stabilito al punto CCC) possono essere opzionalmente anche in formato PDF[23] oltre che in XML (obbligatorio) e lascia libera scelta ai 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[19] a pag. 43 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 § 2.8.2 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 22]***	
		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

Si propone di accogliere la raccomandazione dello standard e quindi l'uso dei seguenti filename, per le ERDS evidence, nel caso di **emissione** REM message dall'**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 nota[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 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]
- **REM receipt**: SubmissionAcceptance.xml o SubmissionRejection.xml
  [caso ricevuta di accettazione (per usare termine noto nella PEC): si veda SEF1 & SEF2 in **Table 14** dell'allegato tecnico]

[23] Questo 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 al processing applicativo.

- **REM receipt**: ContentConsignment.xml o ContentConsignmentFailure.xml [caso ricevuta di consegna (per usare termine noto nella PEC): si veda SEF4 & SEF5 in **Table 14** dell'allegato tecnico]
- **REM receipt**: RelayAcceptance.xml o RelayRejection.xml [caso ricevuta di presa in carico (per usare termine noto nella PEC): si veda SEF6 & SEF7 in **Table 14** dell'allegato tecnico]
- **REM 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 ***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 22]***	**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. 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[19] a pag. 43; si veda anche l'allegato tecnico al § 2.8.2 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 23]*	Si conferma il testo originario

GGG.Content-Description

Il GDL decide di lasciare libera la scelta (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 23]*	
		REM-Section-Type: The value of this field shall be "rem_message/xml_evidence".		shall

HHH.REM-Section-Type

Il GDL recepisce e mette in evidenza con uno ***shall*** questa scelta, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 13 Clause 5.4.6), relativo all'interoperabilità, 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 23]*	Si conferma il testo originario

III. Content-Description

Usato opzionalmente nel caso di presenza evidenze (come allegato addizionale) in PDF oltre che in XML. Il GDL decide di lasciare libera la scelta (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 23]*	
		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, il GDL decide di restringere questo requisito con uno ***shall*** all'interno della REMID policy=REM-Policy-IT (nel rispetto delle condizioni riportate nella nota[19] a pag. 43).

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 24]*	
		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]**. Il GDL restringe con uno ***shall*** questa scelta, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 15 Clause 5.4.7 punto a)) il parametro "name" è prescritto come obbligatoriamente 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 24]*	
		Content-Disposition: The value for this header field shall be: "attachment" • 'filename' parameter value **shall** be "smime.p7s".		**shall**

LLL. Content-Disposition

Il GDL restringe con uno ***shall*** questa scelta, in coerenza al fatto che nel documento EN 319 532-4 **[4]** (Table 15 Clause 5.4.7 punto b)) il parametro "filename" è prescritto come 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 24]***	**Si conferma il testo originario**

MMM. Content-Description

Il ***may*** si riferisce al parametro specificato, per il quale si lascia libertà (nel rispetto delle condizioni riportate nelle note[18] [19] a pag. 43).

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 24]***	**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. Si vedano per lo scopo la premessa e le condizioni del punto FFF al § 4.3.4, pag. 63 che sono da considerare prescrittive anche per il presente punto.

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 24]***	**Si conferma il testo originario**

OOO. REMS – signatures formats

Si lascia libertà di implementazione ai service provider (nel rispetto delle condizioni riportate nelle note[18] [19] a pag. 43 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 24]***	**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. Viene pertanto lasciata libera scelta di implementazione.

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 25]***	
		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 scelta del GDL è di proteggere, come indicato, eventuali evidenze addizionali in formato PDF nei REM message. Questo su tutti i messaggi emessi entro la REMID policy=REM-Policy-IT, e di lasciare ***should*** per quanto riguarda i messaggi provenienti da altre REMID policy, per agevolare l'interoperabilità (si veda il § 2.8.3 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 25]*	
		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.3.2, Table 51 item a)**

RRR. Signatures on REM messages

In merito alla suddetta tabella si conferma ***shall*** come definito, al punto su indicato, nella **REM baseline** (nel rispetto delle condizioni riportate nelle note[18] [19] a pag. 43 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 25]*	
		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.3.2, Table 51 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).

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
TTT	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 25]*	***Non applicabile*** **REM baseline [4] Clause C.3.2, C.3.4** ***Il time-stamp è applicato esclusivamente alla ERDS evidence. Si veda in particolare la Nota della Clause C.3.2 del EN 319 532-4 [4]***

TTT. 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 X-ADES-B-T. Coerentemente con gli obiettivi del **razionale** in premessa e l'adesione alla **REM baseline** il GDL decide pertanto di **non** considerare lo ***should***. Si rimanda alle apposite sezioni dello standard EN 319 532-4 **[4]** Clause C.3.2 e C.3.4 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. 72

4.3.4	Ambito	Statement	Riferimento	REM-Policy-IT
UUU	**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 25]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

UUU. 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 **Table 2** dell'allegato tecnico.

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. 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.	***[pag 25]***	
		The REM RI (Relay Interface) **shall** 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.		**SI – shall** **REM baseline [4] Clause C.2.3.3.2, Table 41, 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**) è basato esclusivamente sull'**SMTP.** Il GDL recepisce quanto riportato nella suddetta tabella e quanto previsto per la Common Service Interface in accordo alle prescrizioni della **REM baseline**[24] (si veda anche la nota[12] a pag. 28).

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.

[24] 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 di intenti del profilo di interoperabilità EN 319 532-4 [4]: << *…[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 25]***	
				SI – shall **REM baseline [4] Clause C.2.3.3.2, Table 41, item b.2.4.2)**

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 elemento. Pertanto, sfruttando l'apertura rappresentata dal ***may*** (si veda testo in grassetto che fa riferimento a "*Other techniques*") è consentito l'unico valore, come MX record, prescritto nella **REM baseline**. Lo ***shall*** in tabella denota l'adesione alla **REM baseline**.

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 26]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.**

XXX. Trust information

Il GDL conferma l'adozione di un modello che si appoggia all'EU Trusted List (TL) System, in accordo alle prescrizioni della **REM baseline**, nel rispetto delle condizioni ed in coerenza con tutti i punti che nel presente documento definiscono delle scelte in tema di Trusted List (si veda la nota[12] a pag. 28).

Tutte le altre scelte che seguono rientrano tendenzialmente a cascata, 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 26]*	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 26]*	Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.2 Table 40.

ZZZ. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX. Si noti che la **REM baseline**, al punto indicato nella suddetta tabella, mantiene opzionale l'elemento in esame, in accordo alla semantica dello stesso.

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 26]*	Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] C.2.3.3.2 Table 41, item b.2.4.1).

AAAA. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX. Si noti che la **REM baseline**, al punto indicato nella suddetta

tabella, fissa l'utilizzo dell'elemento in esame per gli usi necessari in ambito REM, in accordo alla semantica dello stesso.

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 26]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.2.3.3.2 Table 41, item b.2.4.2).**

BBBB. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX. Si noti che la **REM baseline**, al punto indicato nella suddetta tabella, prescrive le modalità di utilizzo dell'elemento in esame per gli usi necessari in ambito REM, in accordo alla semantica dello stesso. Inoltre, la parte dello standard che assicura l'interoperabilità (EN 319 532-4 **[4] SMTP Interoperability profile** & **REM baseline**) è basato esclusivamente sull'**SMTP** (si veda il punto C al § 4.3.4, pag. 34).

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 26]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] C.2.3.3.2 Table 41, item b.2.4.2).**

CCCC. Trust information Table 13

Al presente punto si applicano le stesse considerazioni e condizioni del punto XXX. Si noti che la **REM baseline**, al punto indicato nella suddetta tabella, prescrive la sintassi con cui specificare l'elemento in esame, in accordo alla semantica dello stesso.

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 26]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] (Figure B.13).**

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 26]***	
		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 42 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. Trust information Table 13

Il GDL conferma l'adozione di un modello che si appoggia alle **Capability and Security Information**, in accordo alle prescrizioni della **REM baseline**, nel rispetto delle condizioni ed in coerenza con tutti i punti che nel presente documento definiscono delle scelte in tema di capability (si veda anche la nota[12] a pag. 28). Tutte le altre scelte che seguono rientrano tendenzialmente a cascata, 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 26]***	***Non applicabile*** **REM baseline [4] Clause C.1, C.2.3.4.1, Table 42 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" che sfrutta, appunto, l'apertura dello standard rappresentata dal suddetto ***may*** come indicato nella Clause C.2.3.4.1, Table 42, (ed in particolare all'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 26]***	***Non applicabile*** **REM baseline [4] Clause C.1, C.2.3.4.1, Table 42 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] Clause C.1, C.2.3.4.1, Table 42 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 V1.1.3 [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. As an example, SMTP on TLS according to IETF RFC 7817 [] or SSL plus check of credential over SMTP-AUTH ***may*** be used.	***[pag 12]***	
		Implementation guidance: a) .... As an example, SMTP on TLS according to IETF RFC 7817 [] or SSL plus 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.

Per la 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 viene fissato 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, 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. As an example, IMAP or POP or HTTP on TLS according to IETF RFC 7817 [] or SSL ***may*** be used.	***[pag 12]***	
		Implementation guidance: *a) .... As an 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 Interface, part of CSI, ***may*** be implemented using both or either TL or SMP protocols. [O]	***[pag 13]***	***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]**. Si ritengono pertanto non applicabili i suddetti ***may*** e ***should*** 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 in REM message with a list of REM-ReasonIdentifier header fields, 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

Il razionale è che si lascia a [R] (Raccomandato) per permetterne la valorizzazione durante la costruzione del REM message, quando se ne vedesse la necessità.

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 fields constraints, present in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.2 shall apply. An encoding according to the parameter: charset="UTF-8" ***should*** be used.	***[pag 14]***	
		… a) The header fields constraints, present in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.2 shall apply. An encoding according to the parameter: charset="UTF-8" **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. 54.

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 fields constraints, present in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.3 shall apply. An encoding according to the parameter: charset="UTF-8" ***should*** be used.	***[pag 15]***	
		… a) The header fields constraints, present in table 6 of ETSI EN 319 532-3 [], clause 6.2.3.3 shall apply. An encoding according to the parameter: charset="UTF-8" **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. 56.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
G	**5.4.6 ERDS evidence MIME Header Fields constraints**	The present profile requires XML format (defined in clause 7.4 of ETSI EN 319 532-3[]) for the REM evidence attachment. Optionally the PDF format, as defined in clause 6.2.6.3 of ETSI EN 319 532-3 [], ***may*** be additionally present.	***[pag 15]***	**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. 63.

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: Mandatory ERDS evidence set N. 5 e 6 NotificationForAcceptance NotificationForAcceptanceFailure NOTE 3: Rationale: The sender is made aware on whether the recipient was/was not made available (within the boundaries of recipient's REMS) of the notification the sender's REMS generated in relation to 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: 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** (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: I) The sender's REMS will assume that a REM dispatch or payload has been rejected by the recipient's REMS if any other contrary indication (e.g. REMS evidence and or SMTP DSN) is received within a predefined time period. II) The sender's REMS will assume that a REM dispatch or payload has been accepted by the recipient's REMS if any other contrary indication (e.g. REMS evidence 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 REM receipt including the RelayAcceptance or the RelayRejection evidence.* *c) In the cases addressed in the previous item I), the sender's REMS shall build a REM receipt including the RelayRejection evidence (and/or any other contrary indication to the relay, like SMTP DSN) and shall send it back to the sender.*	***[pag 18]***	**a)** **[C] RelayAcceptance - Sì Shall be generated** **[C] RelayRejection - Sì Shall be generated** **REM baseline [4]** **Table 56, Clause C.3.6.2** **"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**

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.

4.3.5	Ambito	Statement	Riferimento	REM-Policy-IT
K	**5.5.1.3 Conditional evidence – all styles of operation** (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:* *I) The sender's REMS will assume that a REM dispatch or payload has been rejected by the recipient's REMS if any other contrary indication (e.g. REMS evidence and or SMTP DSN) is received within a predefined time period.* *II) The sender's REMS will assume that a REM dispatch or payload has been accepted by the recipient's REMS if any other contrary indication (e.g. REMS evidence 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 REM receipt including the RelayAcceptance or the RelayRejection evidence. c) In the cases addressed in the previous item I), the sender's REMS shall build a REM receipt including the RelayRejection evidence (and/or 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** **b) If the evidence… "send back" - Sì Shall REM baseline [4] Table 56, Clause C.3.6.2 item h)** **c) "in the cases … item I" – 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.3.6.2**

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** (RelayFailure)	d) RelayFailure [C] shall be generated if there is not an 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 REM, if any other contrary indication (e.g. REMS evidence and or SMTP DSN) is received within a predefined time period. *Alternative conditions to III) may be specified in the aforementioned requirement provided that these conditions deal with the relay transaction closure with an exhaustive method.* e) The sender's REMS shall build a REM receipt, including the RelayFailure evidence (and/or 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 57, Clause C.3.6.2** **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** **(**Alternative conditions**)**	*d) RelayFailure **[C]** shall be generated if there is not an 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 REM, if any other contrary indication (e.g. REMS evidence and or SMTP DSN) is received within a predefined time period.* Alternative conditions to III) ***may*** be specified in the aforementioned requirement provided that these conditions deal with the relay transaction closure with an exhaustive method. *e) The sender's REMS shall build a REM receipt, including the RelayFailure evidence (and/or 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]** **Table 57, Clause C.3.6.2 point 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.3.6.2**

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 componenti da prevedere nella ERDS evidence REM baseline [4] Clause C.3.5**

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 when submission is regularly accepted no Reason code is necessary. Multiple Reason codes ***may*** be present depending on the reasons that caused the evidence's triggering event.	***[pag 196]***	**Si conferma il testo originario per quanto non altrimenti riportato nella REM baseline [4] Clause C.1**

O. SubmissionAcceptance - SubmissionRejection - Reason code [M]

Nel REMID policy=REM-Policy-IT almeno un "reason code" deve essere presente (a meno che non venga previsto il contrario). Si lascia aperta la possibilità di inserirne più di uno 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** it means that 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] sull'elemento I10. Pertanto, questo livello deve essere inserito.** **Shall**

P. <u>Sender 's identity assurance details [O]</u>

La REMID policy=REM-Policy-IT intende implementare un servizio qualificato dove non è sufficiente una "**basic**" authentication. Pertanto, questo elemento della ERDS evidence DEVE essere presente, secondo i requisiti della Table 13 EN 319 522-2 **[6]** (dove sono specificate tutte le cardinalità di ogni evidenza relative ai servizi qualificati). Infatti, come riportato nella nota b) della suddetta Table 13 EN 319 522-2 **[6]**, la "identity assurance level" o la "delegate assurance level" ***shall*** be present. Questa proprietà deve essere applicata ad ogni evidenza come indicato nella Table 13 EN 319 522-2 **[6]**. Pertanto, il requisito in esame, come riportato nel § 2.2 dell'allegato tecnico, è assolutamente garantito dalla modalità di identificazione dell'utenza, registrata 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 when consignment regularly occurred no Reason code is necessary. 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]

Come indicato in a) almeno un reason code deve essere presente (a meno che non venga previsto il contrario). Si lascia aperta la possibilità di inserirne più di uno 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
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 when download regularly occurred no Reason code is necessary. 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**; il GDL recepisce la non applicabilità, coerentemente con il **razionale** in premessa e l'adesione alla **REM baseline**.

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** it means that 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**; il GDL recepisce la non applicabilità, coerentemente con il **razionale** in premessa e l'adesione alla **REM baseline**.

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 when the relay to the recipient's REMS regularly occurred no Reason code is necessary. 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]

Come indicato in a) almeno un "reason code" deve essere presente (a meno che non venga previsto il contrario). Si lascia aperta la possibilità di inserirne più di uno 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
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 when relay to the recipient's REMS failed no Reason code is necessary. 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]

Come indicato in a) almeno un "reason code" deve essere presente (a meno che non venga previsto il contrario). Si lascia aperta la possibilità di inserirne più di uno 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.

5 Considerazioni finali

Con il presente documento il percorso avviato dal GDL AGID nel mese di ottobre 2019 ha raggiunto l'obiettivo di dare a tutti i service provider italiani interessati gli elementi per sviluppare le loro piattaforme REM e realizzare i propri servizi di recapito certificato qualificato in conformità ai requisiti del regolamento eIDAS.

L'interazione costruttiva tra il GdL AGID e il Comitato ETSI/ESI è stata inoltre di impulso per la sperimentazione in ambito italiano delle soluzioni tecniche proposte (CSI, Trust list, Time stamping). Sei Gestori PEC (Aruba, Poste Italiane, Telecom Italia Trust Technologies, Namirial, InnovaPuglia, InfoCert) hanno scelto di cogliere l'opportunità e hanno effettuato una PoC, creando un ambiente PEC ridondato con le varie componenti da testare; sono stati predisposti gli use case e realizzata una suite di test concordata, conclusasi a gennaio 2021; dopo varie sessioni e interazioni tra i suddetti Gestori la PoC ha confermato il corretto funzionamento del modello proposto.

In modo indipendente, l'ETSI ha stabilito di condurre una fase di test (nell'ambito dei cosiddetti ETSI Plugtests™ events) che ha come presupposto quello di disporre di un sistema che sia in grado di effettuare dei test significativi sulle funzionalità previste dalla **REM baseline**, a partecipazione libera e gratuita, aperta a tutti i service provider europei, in particolare quindi ai Gestori PEC, interessati a testare i propri servizi con particolare riferimento all'interoperabilità. Il Plugtests event si è concluso il 16 Luglio 2021. In attesa che ETSI renda evidenti gli esiti, i partecipanti del GDL hanno ritenuto opportuno aggiornare il presente documento ed in particolare l'allegato tecnico, precisando meglio, chiarendo e rendendo consistenti alcuni aspetti della REM-Policy-IT che si sono resi evidenti durante l'esecuzione dei Plugtests.

Nel complesso processo di transizione della PEC a servizi di recapito certificato qualificato conformi al regolamento eIDAS, il GDL ha manifestato l'esigenza di

disporre di una piattaforma campione che implementi correttamente tutte le regole tecniche prescritte dalla **REM baseline**, con la quale verificare la conformità dei servizi implementati dai Gestori PEC prima della migrazione. A tale scopo, come fu fatto per la PEC, AGID ha deciso di farsi carico della realizzazione di una tale piattaforma da rendere disponibile sia durante il periodo transitorio (ante migrazione) che a regime, quando i servizi saranno qualificati eIDAS, per verificarne la conformità nel tempo.

Il GDL ha manifestato inoltre la necessità di definire un modello di migrazione coerente con il quadro normativo italiano esistente: tale quadro prevede che sia un DPCM a stabilire la data di migrazione, ovviamente quando la **REM baseline** sarà stata sperimentata con il Plugtests event e consolidata. È stata definita quindi una soluzione che consenta a tutti i Gestori PEC in esercizio interessati alla migrazione verso la **REM baseline** di condurre, ognuno con le proprie scelte tecnologiche, organizzative e strategiche la transizione, senza che ci siano impatti sull'interoperabilità del sistema; tale ipotesi consente inoltre che anche i Gestori PEC non interessati alla migrazione possano 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 di AGID al tavolo regolatorio del Ministero per l'innovazione e le tecnologie che dovrà emanare il suddetto DPCM.

AGID
Agenzia per l'Italia Digitale

Agency for Digital Italy – Infrastructure service management

REM SERVICES

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

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

ALLEGATO TECNICO | TECHNICAL ANNEX

Version 1.1

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.

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.

1 Introduzione | Introduction

Il presente allegato tecnico contiene un insieme di requisiti che definiscono la cosiddetta **REMID policy** che, nel caso italiano, è identificata come "**REM-Policy-IT**".

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 present technical annex contains a set of requirements defining the so called REMID policy that, for the Italian Member State, is identified as "**REM-Policy-IT**".

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 2.7.6.1) 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 2.7.6.1) 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 della eIDAS regulation | Technical interpretation of eIDAS regulation principles

La presente policy connessa al tutto il set di standard normativamente legato ad essa rappresenta, nel suo complesso, una concretizzazione dei principi e dei capisaldi enunciati nella eIDAS regulation.

In sintesi, la policy e gli standard forniscono uno strumento per l'implementazione di quelli che nella eIDAS regulation 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

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 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.*>>

[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.*>>

assumendo una fisionomia tale che, anche 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*.

A tal proposito, essendo la REM, per definizione, una "**registered**" e-mail, si vuole rimarcare bene questo concetto attraverso la seguente **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

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 strongly oriented to the *user's view point*.

To that end, being the REM, by definition, a "**registered**" e-mail, the following **Figure 1** and from **Figure 2** to **Figure 5** for the error conditions emphasize, from an high level view perspective, the *internal* use of the service from the *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).

interoperabili[26]) dall'uso da/per l'*esterno* del suddetto servizio (cioè interscambi con sistemi diversi quali ad es. la posta elettronica ordinaria).

Utenza registrata (registered): utenza che è necessario sia registrata presso un REMSP perché possa usufruire del servizio REM, nel pieno delle sue potenzialità.

Utenza identificata (identified): il processo di registrazione prevede che il titolare dell'utenza venga "identificato" secondo le norme vigenti prima di utilizzare il servizio (tipicamente questa procedura 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).

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.

Identified users: the registration process foresees that the owner of the user(s) account is "identified" according to the regulations in force before the use of the service (typically this is an initial one time procedure, as prescribed 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).

[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**. 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**. 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**.

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**. 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.

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 (umani o applicativi) che accederanno alle "registered email" sottoscritte dal titolare.

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].

Il secondo passo è quello di connettere *il punto di vista dell'utente* con *le modalità di trasmissione*. La seguente **Table 1** riassume,

Authenticated users: the registration process to the REM service, once identified the owner, foresees that a set of secure credential(s) will be released: one for each physical user (human and/or application one) will really access to the "registered e-mail(s)" subscribed by the owner.

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].

Thereby, a further step is to correlate *the user view point*[29] with the *modes of transmission*. The following **Table 1** sums up, from a technical view point, the

[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.

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.

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").

[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).

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

Id	Sender	Recipient	Transmission type
TUC1	**registered**	**registered**	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)
TUC2	**registered**	**unregistered**	Transmission "**ensured**" from the sender up to the S-REMS. The "**last stretch**" from the S-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.
TUC3	**unregistered**	**registered**	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) to the R-REMS is "**not ensured**" in the sense of the REM standards, by a end-to-end evidence.

Come conseguenza alle suddette considerazioni, già l'evidenza di presa in carico dell'R-REMS (REM **RelayAcceptance** receipt), possibile solo nelle trasmissioni tra REMSP, garantisce che il destinatario sia "pertinente" e cioè "registrato" presso l'R-REMS che la emette. Pertanto, tale ricevuta (una cumulativa per ogni R-REMS) fornisce tutte le assicurazioni che la trasmissione stia avvenendo tra utenze 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 il ciclo e fornisce tutte le assicurazioni riguardo la avvenuta trasmissione dello *user content* dal mittente fino alla mailbox del destinatario[31].

As consequence of the aforementioned considerations, since from the evidence of occurred relay by R-REMS (REM **RelayAcceptance** receipt), possible only in transmissions between REMSPs, ensures that the intended recipient is "pertinent" and so "registered" at the R-REMS. Therefore, such receipt (one, cumulative, for each R-REMS), provides enough assurance that the transmission is occurring between registered users (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, and it provides the overall assurances regarding the occurred transmission of the *user content* from the sender to the recipient mailbox[31].

[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 REM receipt. Ma invece è sicuramente accurato che, prima della "delivery" del contenuto: (1) l'R-REMS si assicuri che il ricevente sia "**registrato**", e (2) produca tale assicurazione al mittente attraverso l'invio della RelayAcceptance REM receipt al mittente.

[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 REM 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 through the RelayAcceptance REM receipt to the sender.

Si noti infine che i meccanismi di identificazione dell'utenza sono regolati da opportuni *assurance level* descritti più nel dettaglio nel § 2.4.2.13.

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

Finally, note that the user's identification mechanisms are regulated by appropriate *assurance levels* described in detail in § 2.4.2.13. 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.

2.3 Prescrizioni della REM-Policy-IT previste nella REM baseline | REM-Policy-IT prescriptions envisaged in REM baseline

2.3.1 Parametri | Parameters

Nella seguente **Table 2** è riportata la specifica, all'interno della **REM-Policy-IT**, di concetti a carattere parametrico 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 PartInfo DigestMethod algorithm Any REM dispatch Any REM receipt **REM-DigestAlgorithm**	EN 319 532-4 **[4]**, Clause C.3.5 Table 54, l) EN 319 522-2 **[6]**, **M02** EN 319 522-2 **[6]**, **MD14**	Algorithm used for the digest of entire "original message" during emission: http://www.w3.org/2001/04/xmlenc#sha256 Algorithms, from RFC 6931, accepted from other policies during verification: 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

		NIST.FIPS.180-4 https://www.w3.org/TR/xmldsig-core2/ 3.1.1, 10.1	The present digest algorithm is set in: **partInfo/DigestMethod** ERDS evidence element and in the following REM dispatch / REM receipts header: **REM-DigestAlgorithm** *Note that this algorithm is subject to the current security practices (see § 2.6.1).*
PP2	Any ERDS evidence PartInfo DigestValue Any REM dispatch Any REM receipt **REM-DigestValue**	EN 319 532-4 **[4]**, Clause C.3.5 Table 54, l), EN 319 522-2 **[6]**, **M02** EN 319 522-2 **[6]**, **MD14** NIST.FIPS.180-4 https://www.w3.org/TR/xmldsig-core2/ 3.1.1, 10.1	Value of the digest Digest of entire "original message" during emission computed according to algorithm specified above. The digest value, obtained with such algorithm is set in: **partInfo/DigestValue** ERDS evidence element and in the following REM dispatch / REM receipts header: **REM-DigestValue** The digest-value is computed as the **SHA256** digest of "original message MIME part" (in base64 format). Note that 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).
PP3	**Message-ID / REM-UAMessageIdentifier MessageIdentifier**	EN 319 522-2 **[6]**, **MD11** EN 319 532-3 **[3]**, Table 2, Table 3	See § 2.4.2.3
PP4	**Subject**	EN 319 532-3 **[3]**, Table 2, Table 3	See Table 14 § 2.4.2.10
PP5	signature-policy-identifier	EN 319 532-3 **[3]**, Clause 8.3 EN 319 532-4 **[4]**, Clause C.3.2, Table 51, b) Table 52, 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 messages digital signatures	EN 319 532-4 **[4]**, Clause C.3.2 Table 51, a), Table 51, 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 set to the email address of the *From* header (the signer)**. 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.3.3 Table 52, c) Table 52, d) EN 319 532-4 **[4]**, Clause C.3.4 Table 53, 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 level **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.3.5, Table 54, 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 elements **I01** and **I05**.
PP10	CSIIssueDateTime	EN 319 532-4 **[4]**, Clause C.2.3.4.1, Table 42, c.3.1.8, point 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 42, c.3.1.8, point 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	*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 *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 *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*

PP15	Cycle-number for persistent errors and final behaviours	EN 319 532-4 **[4]**, Clause D.4.4	*Note 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 42, c.3.1.8, point 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-qualificati *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 50 b), Clause C.3.5, Table 54 f), Clause C.2.3.4.1, Table 42, c.3.1.8, point 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)*
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 *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1)*
PP20	**EvidenceIssuerPolicyID**	EN 319 522-2 **[6]**, **R01** EN 319 532-4 **[4]**, Clause C.3.5 Table 54, f) Clause C.3.6.x, Table 55 d), Table 56 d), Table 57 d), Table 58 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> *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 42, c.3.1.8, point 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 42, c.3.1.11 Clause D.2.2	The same digital signature and time-stamp requirements defined for ERDS evidence at row **PP7**. *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	**Sender/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 element 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 **NonERDS** systems events. Anyway, in case of its presence, values different from the following URI can be ignored: http://eidas.europa.eu/LoA/substantial *See § 2.4.2.13 for more details on LoA and on the rationales defining the level to "substantial".*
PP24	**EventReasons**	EN 319 522-2 **[6]**, **G04** EN 319 532-4 **[4]**, Clause C.3.5 Table 54, d) Clause C.3.6.x, Table 55 a), h) Table 56 a), h) Table 57 a), h) Table 58 a), h)	URI and details composing the event reason during emission: First element: <Code> with a uri from the third column of **Table 15** Second element: <Details> with the code from the second column of **Table 15** Third element: <Details> with the reason message taken from the second column of tables from Table7 to Table 12 of EN 319 522-2 **[6]**, Clause 8.3.3. Example: <tns:EventReasons> <tns:EventReason> <Code>http://uri.etsi.org/19522/EventReason/**MessageAccepted**</Code> <Details>**RA01**</Details> <Details>Message accepted</Details> </tns:EventReason> </tns:EventReasons> Different values for <Details> optional elements are accepted during verification for ERDS evidence issued under other policies.

PP25	**EvidenceIssuerDetails** **ExternalERDSDetails**	**EN 319 522-2 [6], R02** **M05** **EN 319 532-4 [4], Clause C.3.5 Table 54, g)**	Legal name of the issuer or counterpart 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 digital certificate signing REM messages and ERDS evidence XMLs, to facilitate additional automatic matching checks.

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. 20 e F di pag. 22 del § 4.3.1 del documento base). I flussi ed eventi previsti sono pertanto quelli illustrati nei seguenti scenari e schematizzati in **Table 3**. Di fatto, la trasmissione canonica tra utenze registrate (rappresentata come "ensured"), ed

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. 20 and F at pag. 22 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 in **Table 3**. Actually, the canonical transmission between registered users (represented as "ensured"), and

indicata come **TUC1** in **Table 1**, è quella riportata nella seguente **Figure 1**.

In aggiunta al suddetto tipo di trasmissione, la **REM-Policy-IT** prevede dei flussi ibridi "facoltativi" **non propri della REM baseline** (ma legati alla realtà locale regolata dalla **REM-Policy-IT**) ed illustrati nelle **Figure 6** e **Figure 8** del § 2.4.2.1.

referred as **TUC1** in **Table 1**, is shown in the following **Figure 1**.

Along with the aforementioned transmission type, 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**) and illustrated in the **Figure 6** and **Figure 8** of § 2.4.2.1.

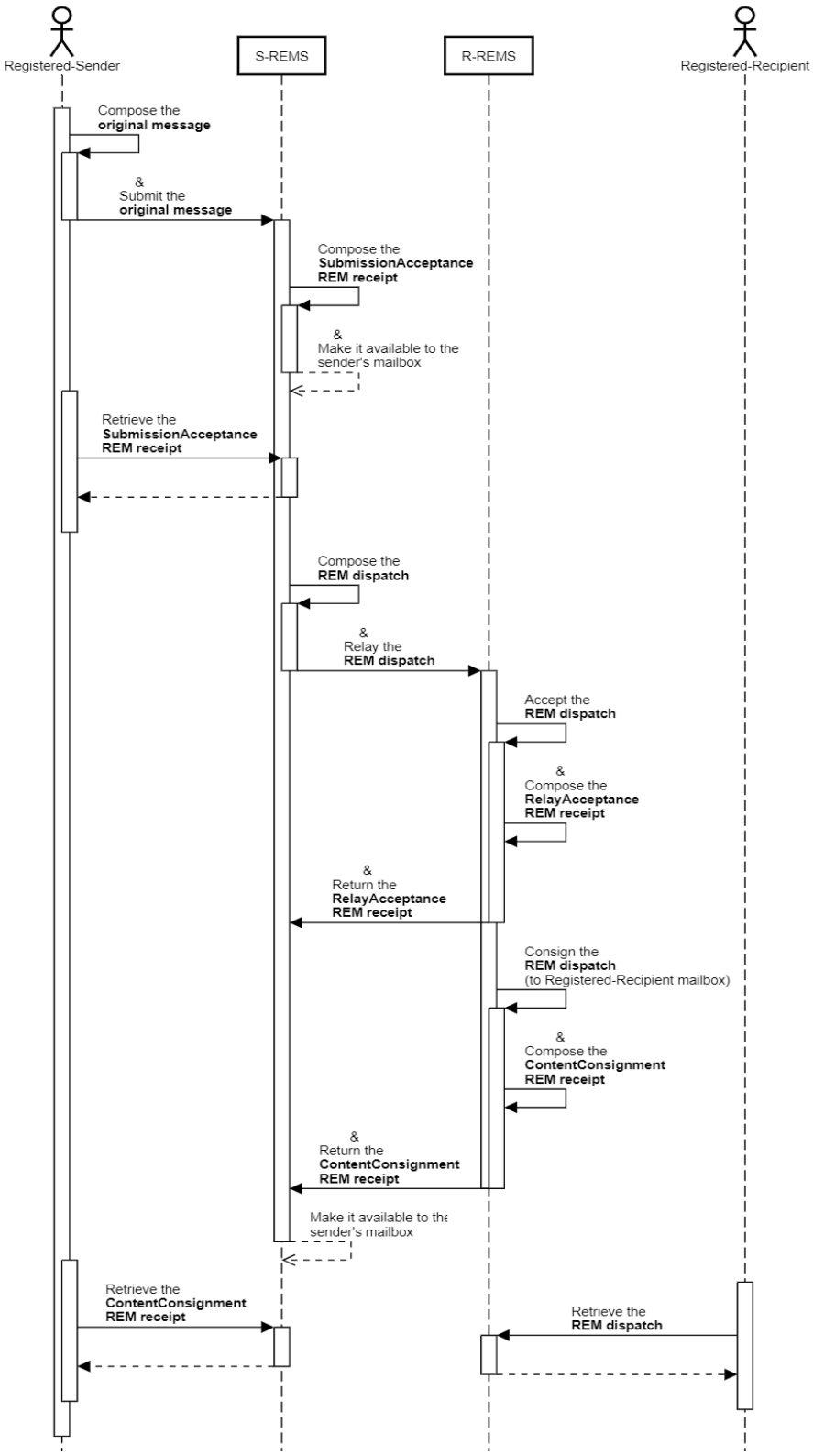

Figure 1 – 4-Corner model: "canonical/ensured" flow between registered users (TUC1)

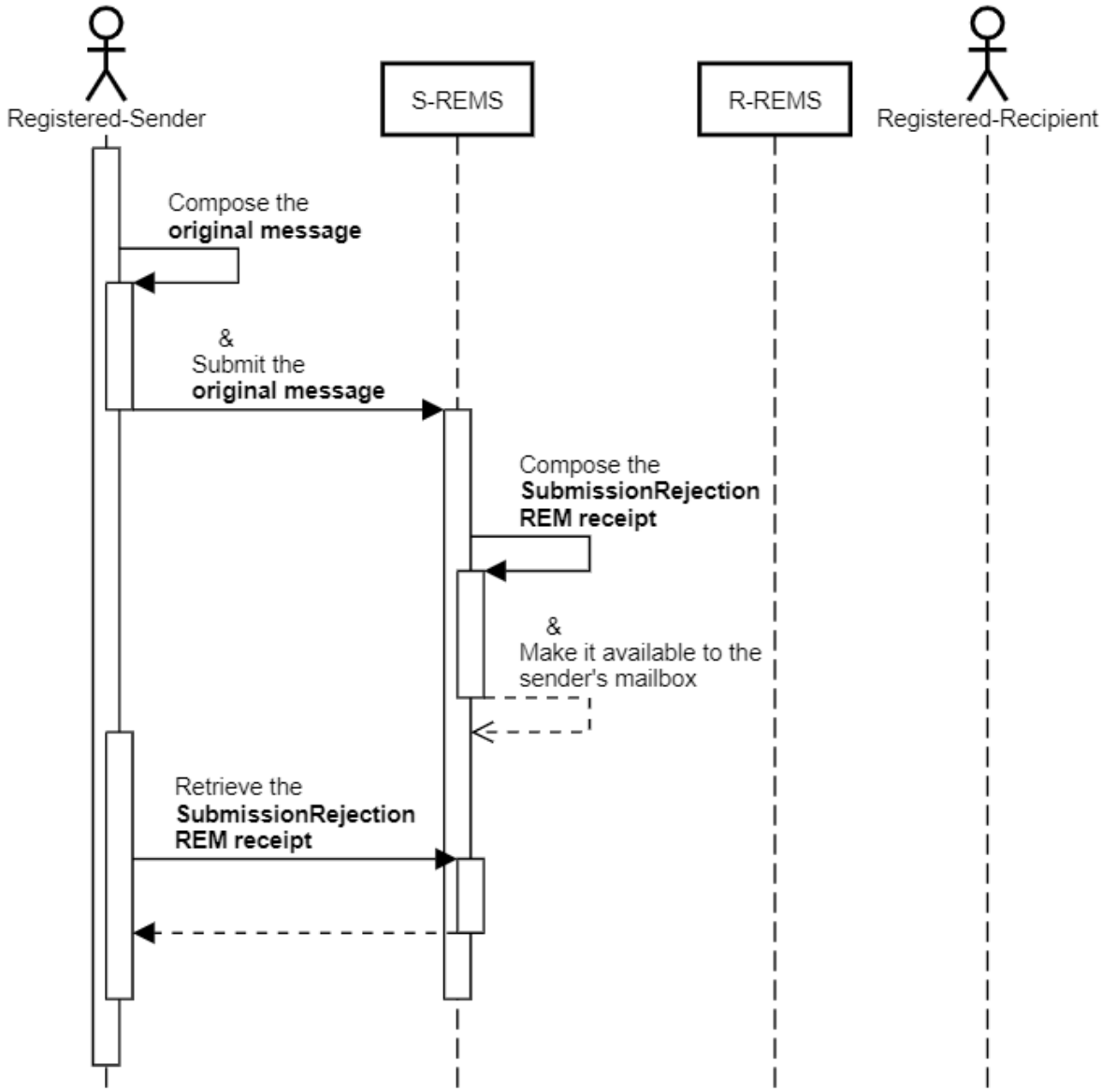

Figure 2 – 4-Corner model: "canonical " flow - SubmissionRejection (TUC1)

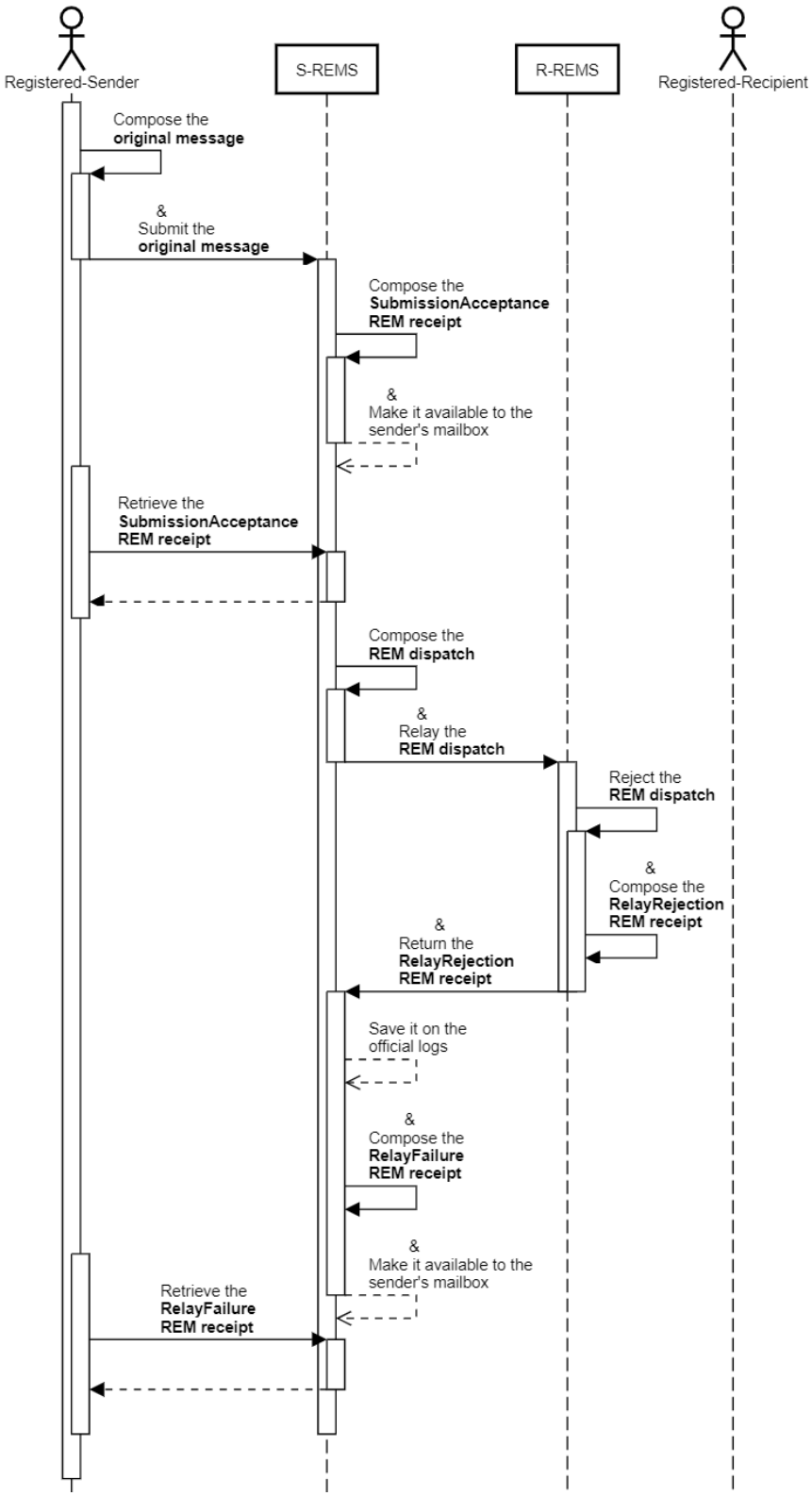

Figure 3 – 4-Corner model: "canonical " flow – RelayRejection & Failure (TUC1)

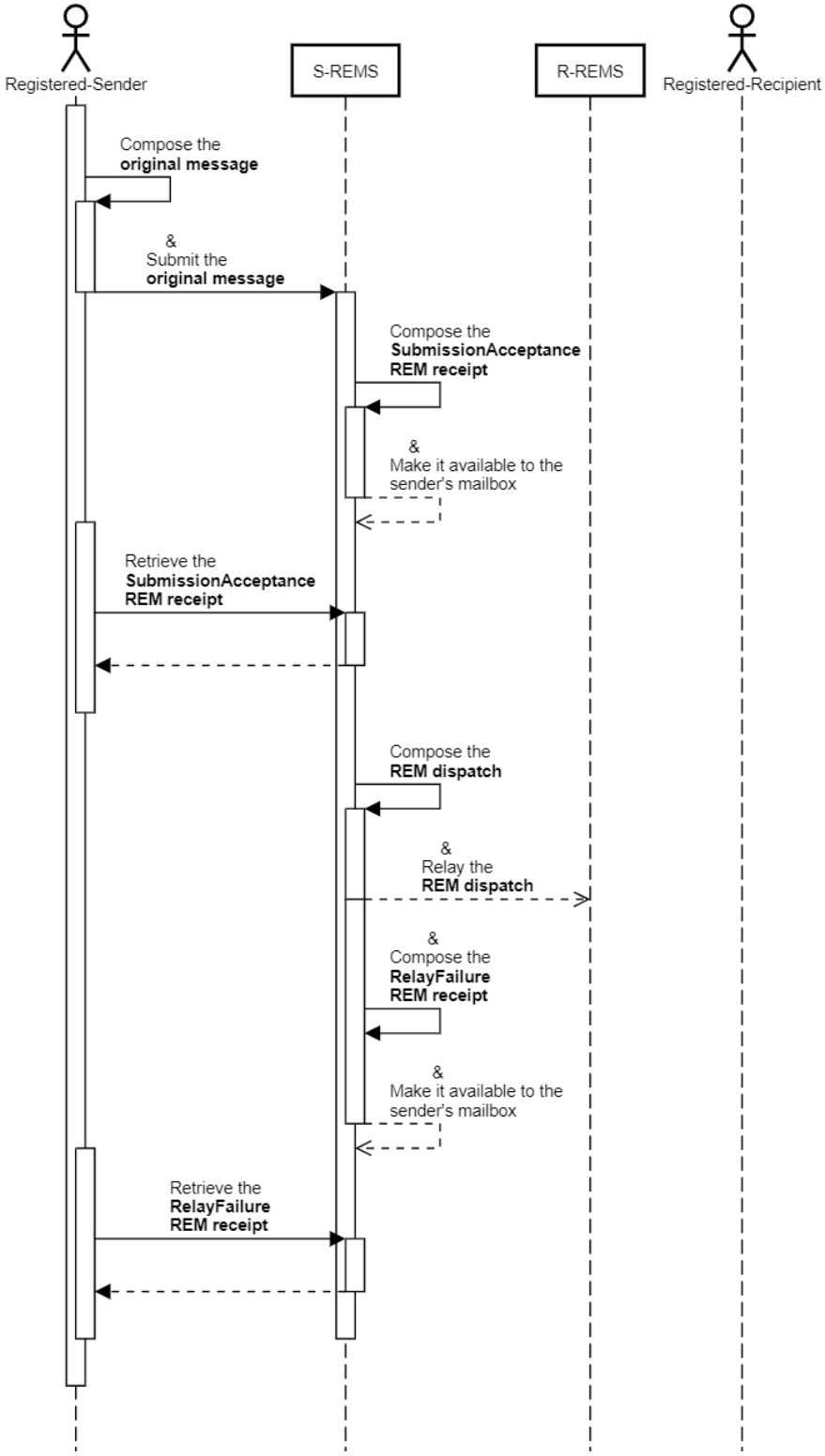

Figure 4 – 4-Corner model: "canonical " flow – RelayFailure (TUC1)

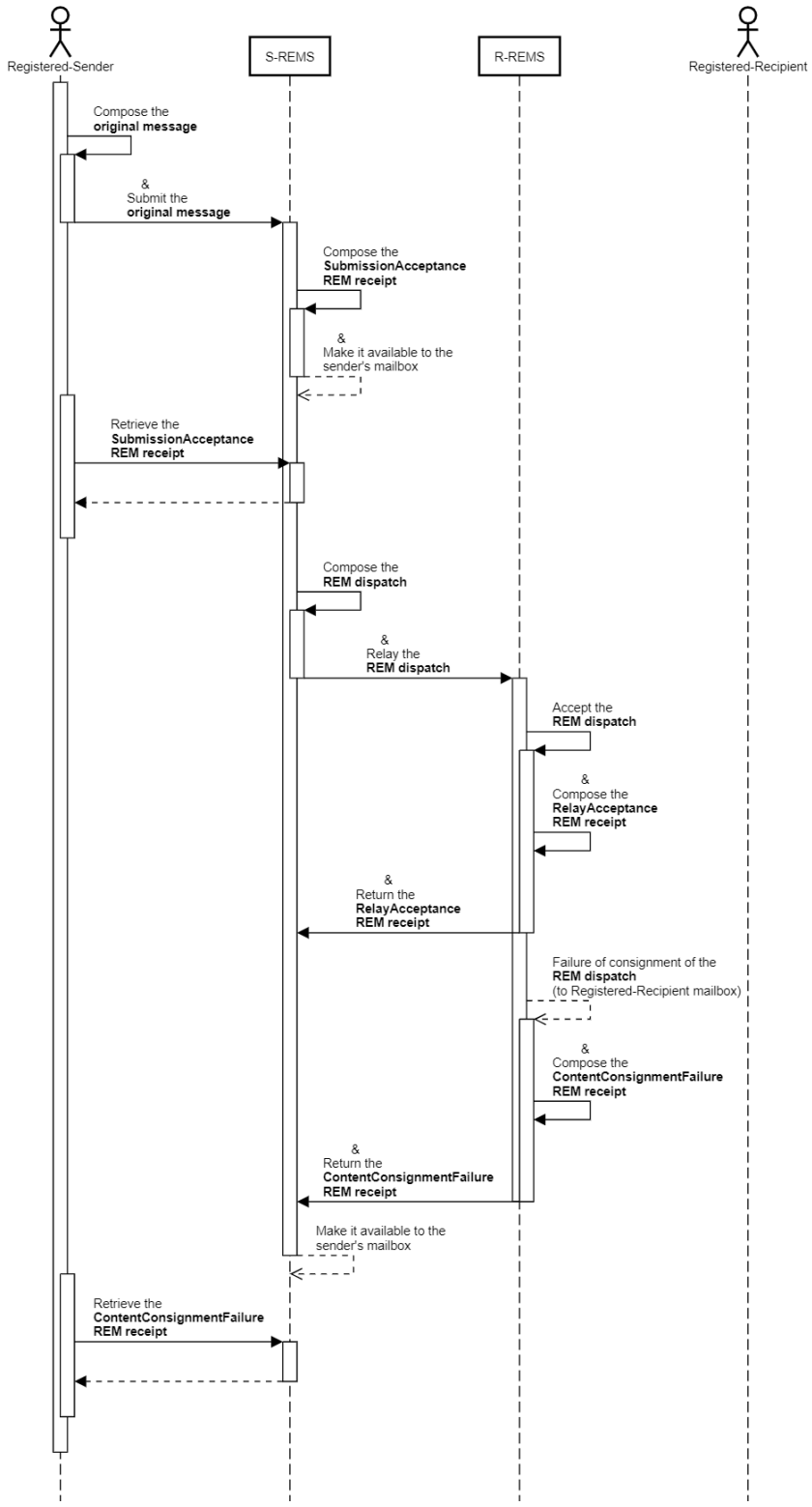

Figure 5 – 4-Corner model: "canonical " flow - ContentConsignmentFailure (TUC1)

In **Table 3** sono riportati gli eventi, le evidenze e i messaggi previsti come obbligatori all'interno della **REM baseline** (intestazione in grigio tabella), gli elementi 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 sottoforma 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 prevista nella **REM-Policy-IT** a destra dello stesso.

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 elements, 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 to use in **REM-Policy-IT** on the right of such symbol.

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

Summary table for elements, 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 / 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 element	Presence constraints								
G01	EvidenceIdentifier	1		1	1	1	1	1	1	
G02	Evidence (version)	1		1	1	1	1	1	1	
G03	ERDSEventId	1		1	1	1	1	1	1	I-G03
G04	EventReasons	1		1..N|1	1	1..N|1	1..N|1	1	1..N|1	I-G04
G05	EventTime	1		1	1	1	1	1	1	
R01	EvidenceIssuerPolicyID	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	
I05	RecipientDetails/Identity	0..N|0		0..N|0	0..N|1	0..N|1	0..N|1	0..N|1	0..N|1	I-I05
I06	RecipientDetails/Identifier	1..N		1..N	1..N	1..N	1..N	1..N	1..N	
I09	EvidenceRefersToRecipient	0		0	0	0	0	1	1	
I10	Sender/AssuranceLevelsDetails	1		1	1	1	1	1	1	I-I10
I12	Recipient/AssuranceLevelsDetails	0		0	0	0	0	0	0	
M01	MessageIdentifier	1		1	1	1	1	1	1	I-MD11
M02	UserContentInfo	1		1	1	1	1	1	1	I-M02
M03	SubmissionTime	1		1	1	1	1	1	1	I-M03
M05	ExternalERDSDetails	0		0	1	1	1	0	0	I-M05
Code	REM message header/metadata element	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	
MD02	REM-RelayDate	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	0..1|1	
MD03	REM-ExpirationDate	0	0	0	0	0	0	0	0	
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	
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	
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-MD11
N/A	From	1	1	1	1	1	1	1	1	AP4
N/A	Signature	1	1	1	1	1	1	1	1	PP6

(*) These events are extended in Table 5 and will be used in: OLR8 - Table 7, Table 8, Table 14, Table 15.

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.

I-G03: The official URI for these events coming, from G03 component of EN 319 522-2 [6], are in Table 2 of EN 319 522-3 [7].

I-G04: Row PP24 of Table 2.

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 element shall be present. In case of messages coming from outside the border or from other policies, this element 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-I05: Row PP9 of Table 2. For RelayAcceptance, RelayRejection, RelayFailure (due to a previous RelayRejection), ContentConsignment, ContentConsignmentFailure, ReceivedFromNonERDS ERDS evidence XMLs issued inside REM-Policy-IT this element shall be present. In the other cases this element 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>>.*

I-I10 / I-MD04: Row PP23 of Table 2 and § 2.4.2.13 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 44 point 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-MD08: This header is mandatory (as per Table 5 EN 319 522-2 [6]) and it is defined as per EN 319 532-3 [3] Clause 6.2.1), and its value is set to the email address of the From: header of the original message.

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.

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-MD11: Row PP3 of Table 2 and § 2.4.2.3 for more details.

I-M02 / I-MD14: Row PP1 and PP2 of Table 2.

I-M03: According to the REM baseline prescriptions defined in EN 319 532-4 [4], Table 54 row 13 and point j.

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

For any element that is not listed above, refer to the example illustrated at § 2.7 to get the relevant implementation 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 effettuata con certificato digitale della 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	Digital signature based on the digital certificate of the REMID authority (represented by **Agid**[32], for the **REM-Policy-IT**) and to ensure the Trust chain integrity at any time and over the time. Integrity that

[32] La firma digitale della presente struttura XML è un requisito "semanticamente" obbligatorio della **REM baseline** (si veda la Clause c.3.1.11 EN 319 532-4 **[4]**) 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** (si veda la Clause c.3.1.11 EN 319 532-4 **[4]**), not to be confused with the XSD notation that points it as "syntactically" optional (`<xsd:element ref="ds:Signature" minOccurs="0"/>`). This apparently asymmerty 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.

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 lenght

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, element c.3.1.8), points viii and ix riguardo la pubblicazione ed il mantenimento dello storico del presente XML.

goes from the TLS certificate, through the XML structure containing it, and it binds, from the cryptographic view point, 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 lenght

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, element c.3.1.8), points viii and ix regarding the publication and the historical preservation of the present XML.

2.4 Prescrizioni della REM-Policy-IT addizionali alla REM baseline | REM-Policy-IT prescriptions additional in respect to the REM baseline

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 concetti a carattere parametrico "addizionali" rispetto a quelli previsti all'interno della **REM baseline**.

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**.

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 value of *From* header of original message. See also examples at § 2.7
AP2	Received:	EN 319 532-3 **[3]**, Table 3	**Only for REM dispatch**: inheritance of *Received* header of original message. The usual SMTP standard behaviour for these multivalue headers for any additional necessary *Received* header in both REM dispatch and REM 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 X509v3 Subject Alternative Name 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.
AP6	Relay-rcv-cc-wait	**Table 15** – Events and Reason codes in REM-Policy-IT	24h S-REMS was unable to receive a ContentConsignment or ContentConsignmentFailure REM receipt 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 REM receipt: a REM **RelayFailure** with custom code *RB51 R_ERDS_MessageNotAcceptedInTime* *Note that this parameter is subject to the current Authority and security practices (see § 2.6.1).*

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**

In addition to the canonical flow of **REM baseline**, the **REM-Policy-IT** extends the 4-corner flows to **OPTIONAL** hybrid

da/verso sistemi esterni (non propri della **REM baseline**) considerati come sistemi di posta ordinaria (si vedano i punti J di pag. 25 del § 4.3.1 ed EEE di pag. 62 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 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 "NonERDS".

transmissions from/to external systems (**non** proper of the **REM baseline**) considered as ordinary email systems (see points J at pag. 25 of § 4.3.1 and EEE at pag. 62 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 table is formatted and refers to analogues contents of those in **Table 3**, but considering that it refers instead to the three "NonERDS" type events.

Table 5 – Extended elements for from/to NonERDS messages/events beyond REM baseline

Summary table for elements, headers, events, flows. Sources: Table 1, Table 5, Table 13 EN 319 522-1 [5], Table 1 & Figure 1..5 present doc.					Implementations
REM Message types / ERDS evidence events (*) Operation / 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**	
G02	**Evidence (version)**	**1**	**1**	**1**	
G03	**ERDSEventId**	**1**	**1**	**1**	**I-G03**
G04	**EventReasons**	**0..1|1**	**0..N|1**	**0..1|1**	**I-G04**
G05	**EventTime**	**1**	**1**	**1**	
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**	
I05	**RecipientDetails/Identity**	**0..N|0**	**0..N|0**	**0..N|1**	**I-I05**
I06	**RecipientDetails/Identifier**	**1..N**	**1..N**	**1..N**	
I09	**EvidenceRefersToRecipient**	**0**	**0**	**0**	
I10	**Sender/AssuranceLevelsDetails**	**1**	**1**	**0**	**I-I10**
I12	**Recipient/AssuranceLevelsDetails**	**0**	**0**	**0**	
M01	**MessageIdentifier**	**1**	**1**	**1**	**I-MD11**
M02	**UserContentInfo**	**1**	**1**	**1**	**I-M02**
M03	**SubmissionTime**	**0..1|1**	**0..1|1**	**0..1|0**	
M04	**ForwardedToExternalSystem**	**1**	**1**	**1**	**I-M04**
M05	**ExternalERDSDetails**	**0**	**0**	**0**	**I-M05**
Code	**REM message header/metadata element**	**Presence constraints. Sources: Table 5 EN 319 522-1 [5] (other than the sources on the head above)**			
MD01	**REM-MetadataVersion**	**1**	**1**	**1**	
MD02	**REM-RelayDate**	**0..1|1**	**0..1|1**	**0..1|1**	
MD03	**REM-ExpirationDate**	**0**	**0**	**0**	
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**	
MD08	**REM-MD08**	**1**	**1**	**1**	**I-MD08**
MD09	**Reply-To**	**1**	**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**	
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-MD11**
N/A	**From**	**1**	**1**	**1**	**AP4**
N/A	**Signature**	**1**	**1**	**1**	**PP6**

(*) These events extend the basic ones defined in Table 3 and will be used in: OLR8 - Table 7, Table 8, Table 14, Table 15.

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 element 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.

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 REM dispatches, issued inside the REM-Policy-IT, the ForwardedToExternalSystem element shall assume the following values:

***Received:* header, relevant to the external system triggering the ReceivedFromNonERDS event or, some other element that can identify the remote system (in case of absence of the Received header).**

***MX-record* relevant to the external system to which the REM dispatch has to be relayed, for RelayToNonERDS and RelayToNonERDSFailure events.**

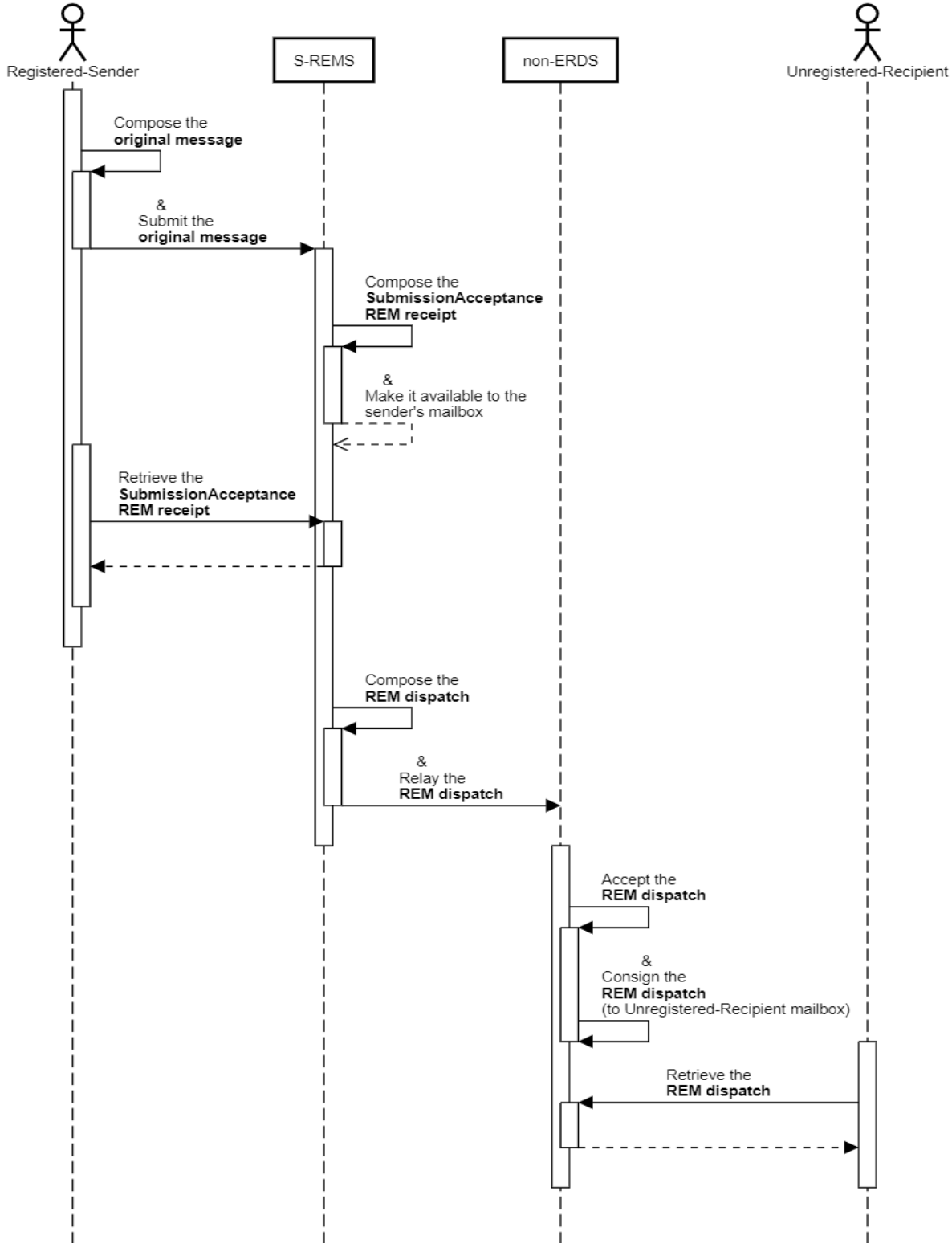

Figure 6 – 4-Corner model: flow from registered to un-registered users (TUC2/EME1)

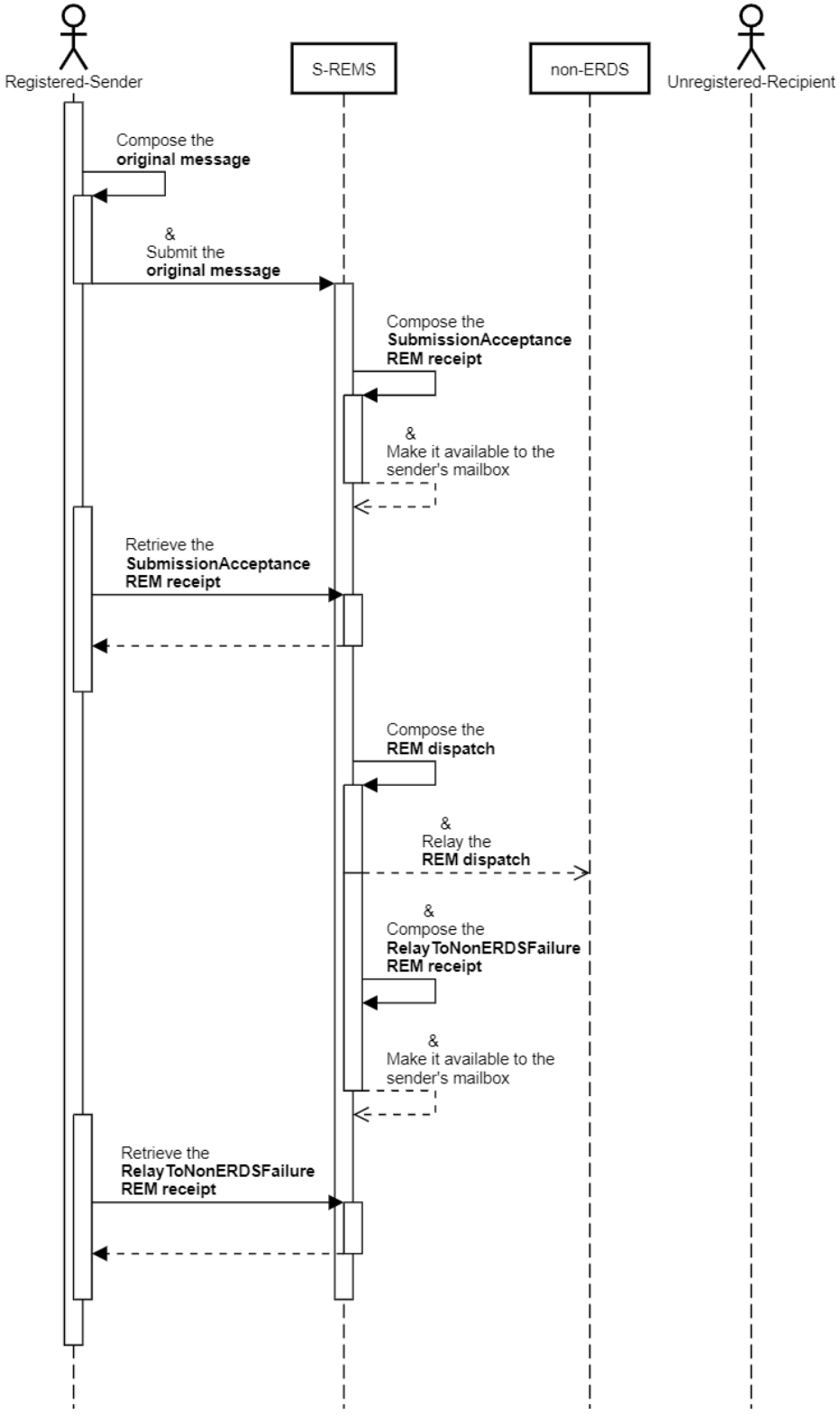

Figure 7 – 4-Corner model: flow from registered to un-registered users failure (TUC2/EME2)

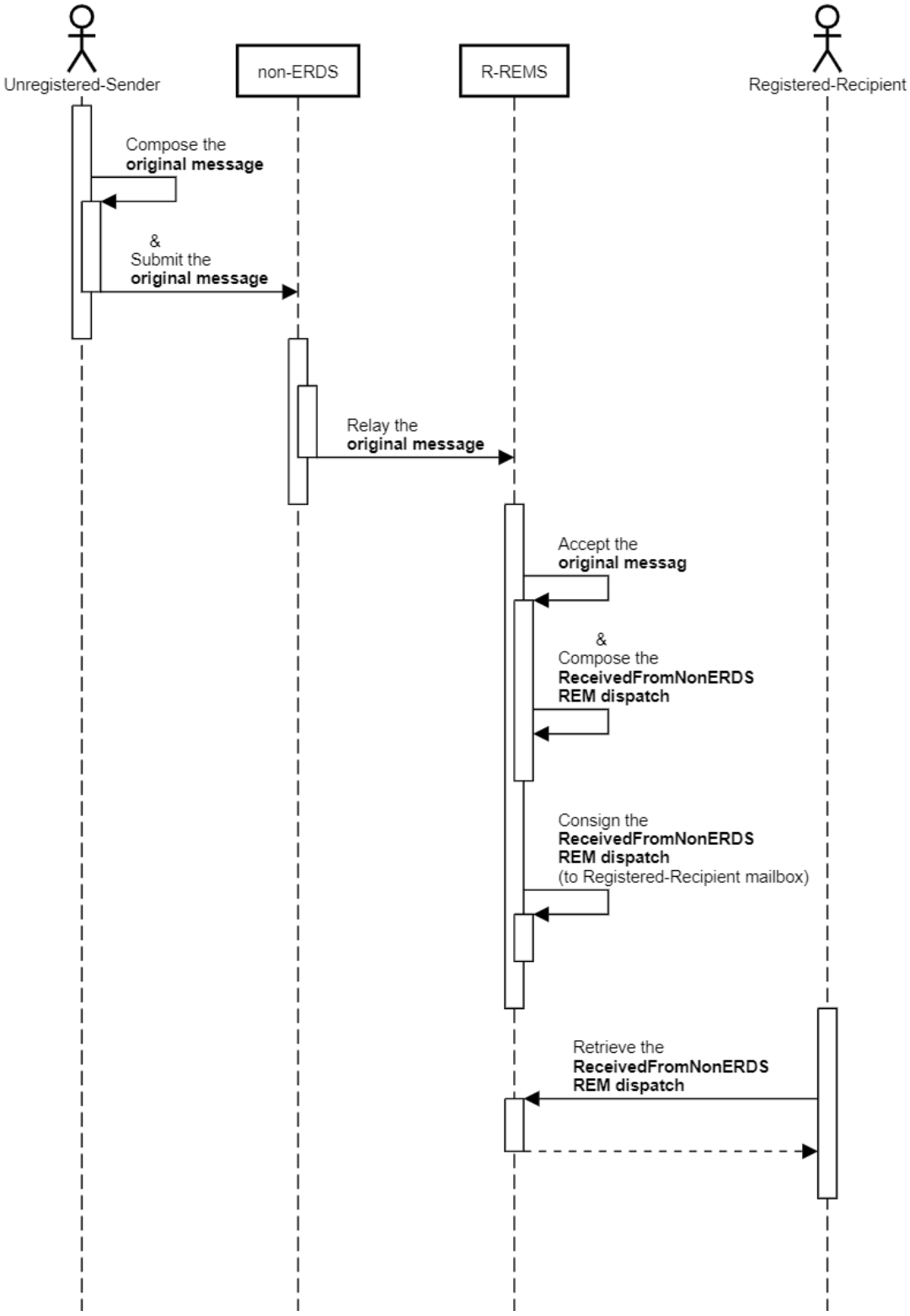

Figure 8 – 4-Corner model: flow from un-registered to registered users (TUC3/EME3)

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 REM receipt o di tipo D.1 o di tipo D.2. 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 viene tracciato, in piena trasparenza verso l'utenza, come indicato alla riga **AP6** della **Table 4** attraverso la definizione del timeout **Relay-rcv-cc-wait** e dell'emissione di una REM **RelayFailure** con evento specifico per questo caso:

RB51 R_ERDS_MessageNotAcceptedInTime.

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 REM receipt. 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 **AP6** of **Table 4** the **Relay-rcv-cc-wait** is defined and the issue of a REM **RelayFailure** with the following specific event is foreseen for this particular case:

RB51 R_ERDS_MessageNotAcceptedInTime.

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

This section analyses the case of hybrid transmissions between users of system adhering to the **REM baseline** (called also,

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. 13 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 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**.

simply **REM** hereinafter) from/to users of external systems (see case TUC2 and TUC3 in **Table 1** at pag. 13 relevant to communications from/to non-registerd 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 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**.

[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 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 not REM systems (aka ERDS in the general case) are mapped in the Table 1 of EN 319 522-1 **[5]**.

Table 6 – Extended messages/flows beyond REM baseline

Id	REMS → non-ERDS		non-ERDS → REMS		Table 5 Id	Event or SMTP	Example
	S-REMSP	Sender	R-REMSP	Recipient			
EMF1	Y	Y	*	*	EME1	RelayToNonERDS	Figure 9
					EME2	RelayToNonERDSFailure	Figure 7, Figure 11, 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

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. Le colonne 4 e 5 indicano la configurazione dell'opzione di ricezione da sistemi non-ERDS rispettivamente a livello di REMSP e a livello utente. La configurazione a livello di servizio 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 riportati degli esempi significativi.

Seguono una serie di figure che identificano ogni possibile caso d'uso. Si veda anche punto "J Event related to connections with non ERDS systems" del § 4.3.1, pag. 25 del documento base.

The columns nr. 2 and 3 of **Table 6** denote the configuration, at REMSP and at user level respectively, allowing to send REM messages towards non-ERDS systems. The columns nr. 4 and 5 denote the configuration, at REMSP and at user level respectively, allowing to receive messages from non-ERDS systems. The service level configuration 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 outlined significant examples.

Follows a variety of figures identifying the main possible use cases. See also the point "J Event related to connections with non ERDS systems" of § 4.3.1, pag. 25 of the basic document.

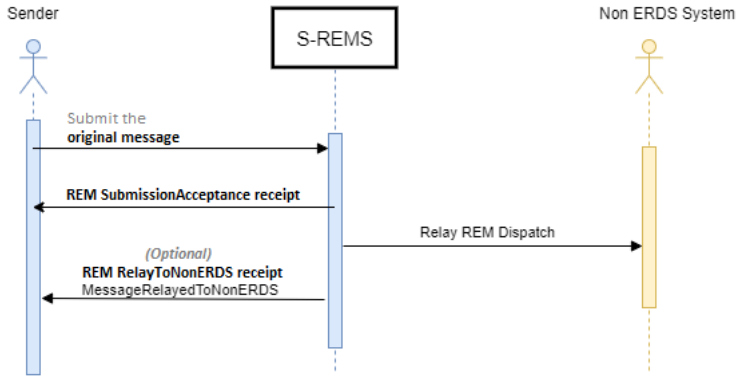

Figure 9 – Successful Outflow to non-ERDS systems (EMF1/EME1)

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**).

La REM 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, può tornare utile che il REMSP replichi tale header anche nel REM dispatch.

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

La REM 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. When a such header is present in the original message, may be useful that REMSP replicates such header also in the 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 Service Provider destinatario (**MX-record**) non appartenente al circuito **REM baseline** (cumulativa per tutti i destinatari che vi afferiscono). Nel caso di fallimento del relay, invece, l'S-REMS restituirà al mittente una REM **RelayToNonERDSFailure** receipt per ogni DSN (Delivery Status Notification bounced e-mail) - o non raggiungibilità - del sistema remoto: ma sempre una per ogni Service Provider destinatario non appartenente al circuito **REM baseline** che viene allegata alla suddetta REM receipt (si veda anche **I-M04**).

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 target Service Provider (**MX-record**) non belonging to the **REM baseline** circuit (anyone cumulative for all the recipients belonging to each Service Provider). 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) - or absence of reachability – of the remote system: one fo any target Service Provider non belonging to the **REM baseline** circuit (that will be attached to the aforementioned REM receipt) in any case (si veda anche **I-M04**).

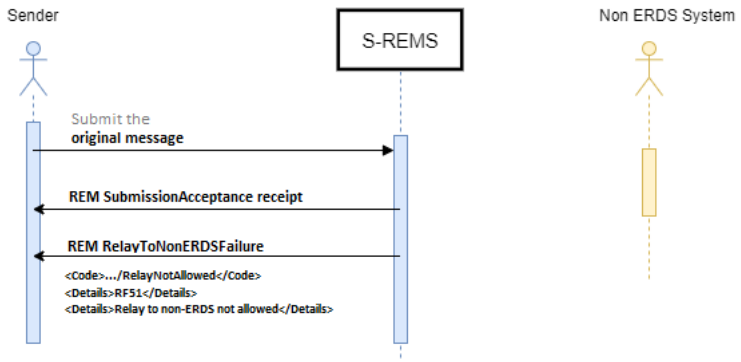

Figure 10 – Not allowed Outflow to non-ERDS systems (EMF3/EMF5/EME2)

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**).

The case of deny of relay towards a non-ERDSsystem 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**).

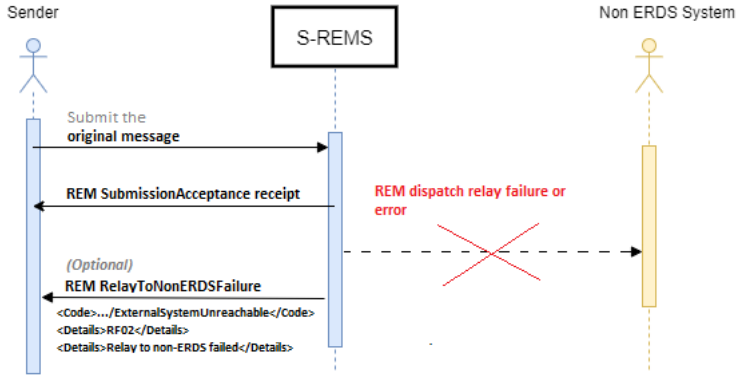

Figure 11 – Failure Outflow to non-ERDS systems (EMF1/EME2)

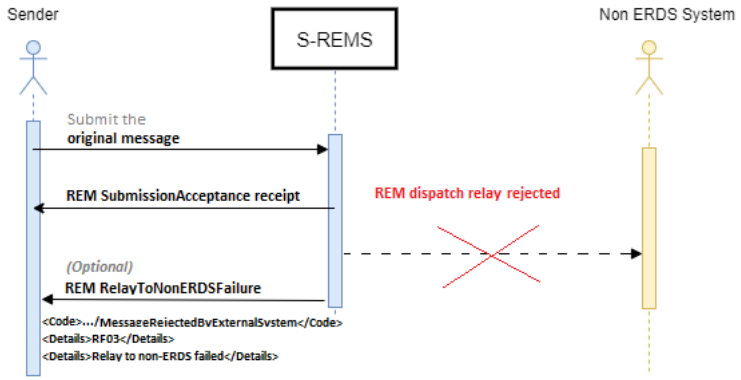

Figure 12 – Rejection Outflow to non-ERDS systems (EMF1/EME2)

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

Figure 11 e **Figure 12** outline two cases of uncompleted relay towards a non-ERDS system due to different causes. These two

scenari rientrano nelle configurazioni identificate in **Table 6** alle righe **EMF1/EME2**.

scenarios fall within the configurations identified in **Table 6** rows **EMF1/EME2**.

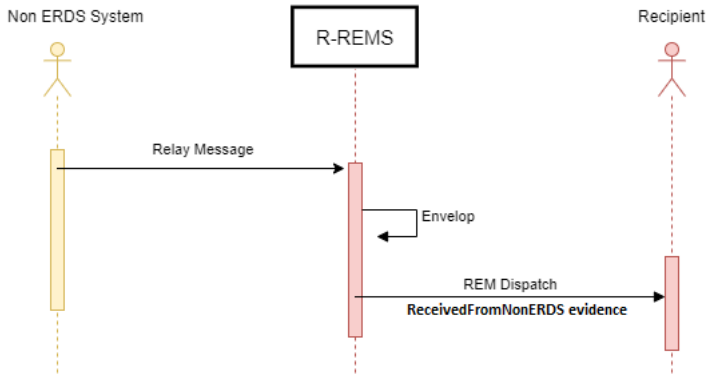

Figure 13 – Inflow received from non-ERDS systems (EMF2/EME3)

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 viene 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 della **Table 6** alla riga **EMF2/EME3**).

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 of **Table 6** at the row **EMF2/EME3**).

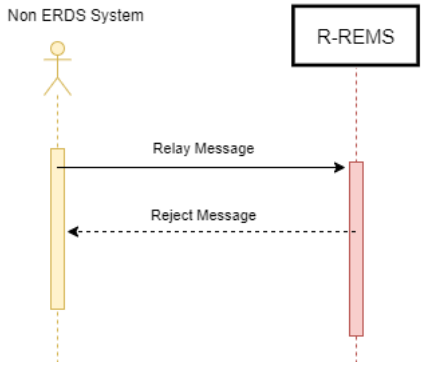

Figure 14 – Inflow rejected from non-ERDS systems (EMF4/EMF6)

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 viene pertanto rigettato (o scartato senza alcuna 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 della **Table 6** alle righe **EMF4** ed **EMF6**).

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 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 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. 35 e note [14] e [15], 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*

How is referred in § 4.3.4 on point D of pag. 35 and note[14] and [15], 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. 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 REM receipt) afferenti, ognuno di essi, ad un'unica transazione legata all'*original message*. Non potendo fare un affidamento 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

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 REM receipts) relevant, everyone, to same transaction related to the *original message*. 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

automaticamente dall'S-REM) sarà salvato nell'*original message* stesso, nel REM dispatch e nelle varie REM 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, anche nei due seguenti elementi della 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 (section 3.6.4).
- EN 319 532-3 **[3]**, Clause 6.1: REM-UAMessageIdentifier, nello standard REM, dovrebbe contenere il Message-ID

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 REM 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*

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 (section 3.6.4).
- EN 319 532-3 **[3]**, Clause 6.1: REM-UAMessageIdentifier, in the REM

dell'*original message* inviato dall' e-mail user agent.

- EN 319 532-3 **[3]**, Annex A: il messaggio di esempio riporta, nel Message-ID, l'identificativo sostituito dal S-REMS, and in REM-UAMessageIdentifier quello originale.

Si noti inoltre che, come stabilito nell'EN 319 532-4 **[4]**, Clause C.3.5 punto l), l'AppLayerIdentifier riporta il Message ID dell'*original message*, cioè quello generato dello User Agent.

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

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

Fare riferimento al § 2.8.2 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.

standard, has to contain the Message-ID of the *original message* submitted by e-mail user agent.

- 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.3.5 element l), the AppLayerIdentifier contains the Message-ID of the *original message*, i.e. that generated by the User Agent.

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 (section 3.6.4)
- The possible Message-ID present in the *original message* will be set in the REM dispatch, in any relevant REM receipt correlate and in in the *original message* through the REM-UAMessageIdentifier header.

Refer to § 2.8.2 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**.

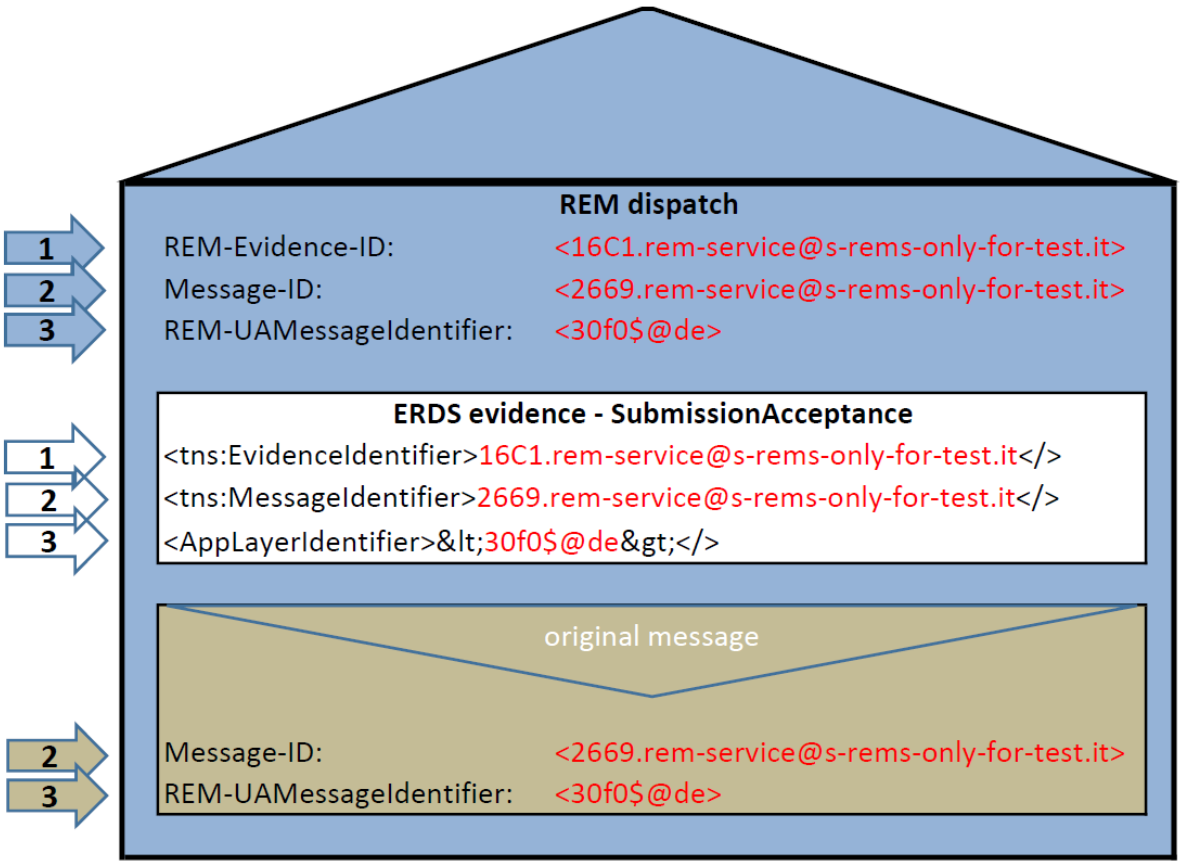

Figure 15 – REM dispatch – message and evidence identifiers

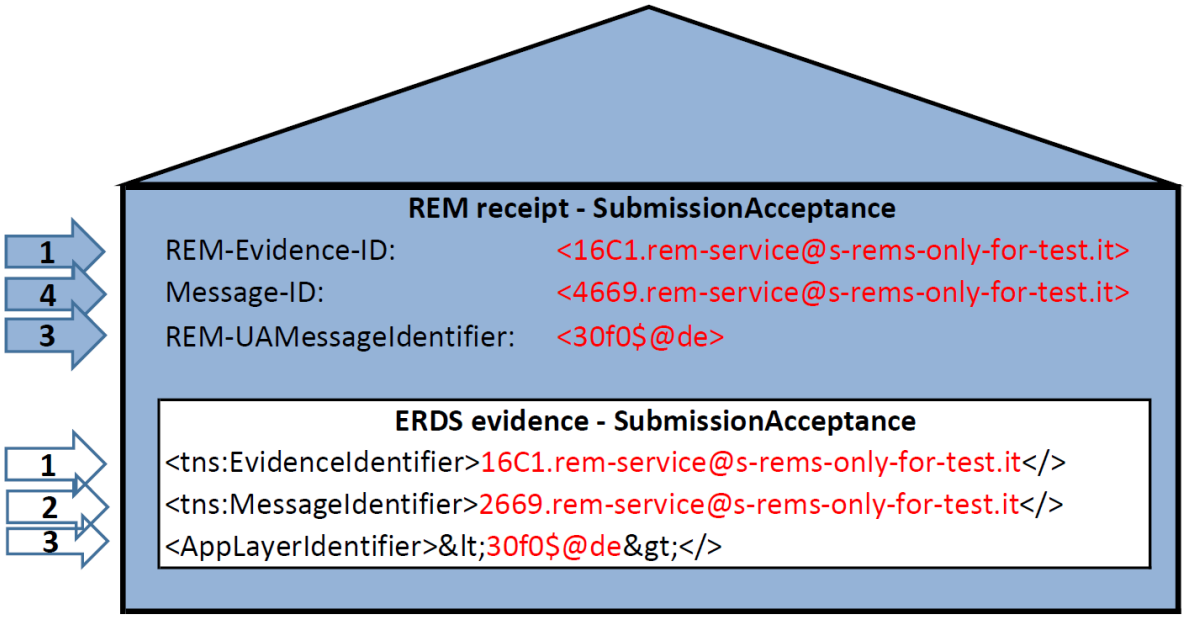

Figure 16 – REM receipt – SubmissionAcceptance – message and evidence identifiers

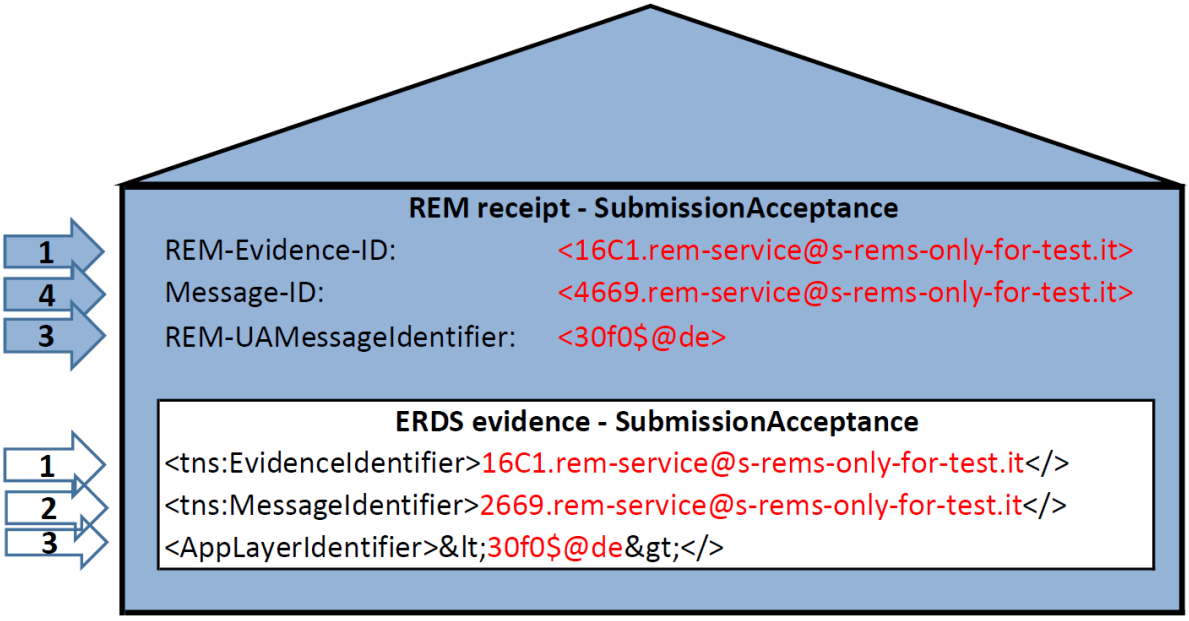

Figure 17 – REM receipt – RelayAcceptance – message and evidence identifiers

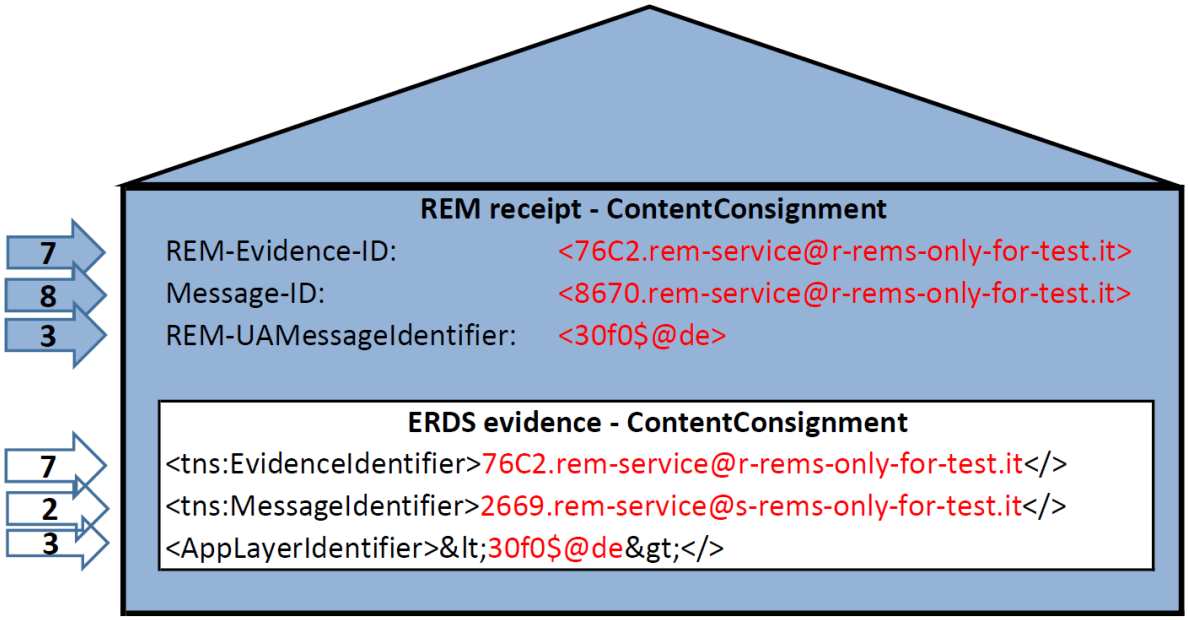

Figure 18 – REM receipt – ContentConsignment – message and evidence identifiers

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.

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) viene denominato **official log**.

Il processo di generazione degli **official log** inizia con la presa in carico dell'*original*

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.

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**.

The process of generation of the **official log** begins when the sender's REMSP takes in charge the *original message*. While, for

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 (REM 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 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 (REM 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 5322/3.6.4) identifying any REM message envelope (see the second header 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. It has the same value of **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 examples from **Figure 15** up to **Figure 18**).
OLR2	**UAMessageId**	UserContentInfo/ AppLayerIdentifier	M02/MD14	Message-ID specified, if any, by the client User Agent (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 white arrows Nr. 3 on 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 arrows Nr. 1, 5 and 7 on the examples from **Figure 15** up to **Figure 18**).
OLR4	**EventTime**	EventTime	G05	Date and time of the event in UTC time 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/Code)*	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 element).
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

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 tracciare le operazioni rilevanti al funzionamento del servizio.

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 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-

È compito del REMSP assolvere alla funzionalità di memorizzazione e conservazione a lungo termine dell'**official log** per il periodo e le modalità stabilite dalle norme correnti (al momento pari ad una durata di 30 mesi).

Di seguito nella terza colonna della **Table 8** l'elenco degli **Eventi** e dei relativi passaggi che possono generarsi all'interno del flusso di un messaggio REM e che devono essere tracciati nell'**official log**. Mentre, 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**.

term retention of **official log** for the period and modality stated by current regulations (for now it is equal to 30 months).

Following, the third column of **Table 8**, contains the **Event** list and the relevant steps that could be generated inside the flow of a generic REM message and that must be tracked in the **official log**. While, 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

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. 26 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*, un po' come avviene con la ricevuta di consegna "completa" dell'attuale Posta Elettronica Certificata (PEC da qui in avanti). Invece, la REM ContentConsignment receipt prevede solo il "digest" dell'*original message*. Il GDL conviene che, per rendere il massimo vantaggio all'utenza, nell'ambito della REMID policy=**REM-Policy-IT** (e, uniformemente, nel bacino di utenza servito dalla suddetta policy) si possa implementare un flusso più completo; e che tale opzione sia governabile direttamente dall'utenza.

Le questioni da indirizzare per tale scopo sono:

1) Permettere, quando richiesto, la possibilità di verifica 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. 26 of the basic document, the standard doesn't specify a REM receipt that ensures the delivery of the message to the recipient with the *original message* attached inside it, like happens in the delivery receipt "complete" of the actual Posta Elettronica Certificata (PEC hereinafter). While, only the "digest" of the *original message* is foreseen in the REM ContentConsignment receipt. The GDL agrees that, in order to give maximum benefit to the sender, in the REMID policy=**REM-Policy-IT** scope (and, uniformly, in the area served by the aforementioned policy) it is possible to implement a more comprehensive flow; and that such option is governable directly from the users.

The questions to address for such purpose are:

1) Allow, when requested, the option to verify the *original message* against its "**digest**" (present in any evidence and therefore even in the ERDS ContentConsignment evidence) according to one of the following modalities:

a) Permettere, quando selezionato, di salvare l'*original message* – mantenuto in forma protetta e incapsulata dentro il REM dispatch – nella casella del mittente (in un folder di default o specificato in un apposito header)
b) Permettere, quando selezionato, di richiedere che la **ContentConsignment receipt** ritorni indietro al mittente, come allegato, l'*original message* – integro e preso byte a byte - dal REM dispatch.

2) Permettere 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 REM receipt).
3) Individuare il comportamento di **default**[35] del servizio, quando nessuno dei suddetti comportamenti è selezionato dall'utente (o nelle sue preferenze).

a) Allow, when selected, to save the *original message*, protected in the incapsulated form inside the REM-dispatch - in the sender's mailbox (in a default folder or in one specified through a MIME header)
b) Allow, when selected, to request 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 REM receipt.
3) Individuate the **default**[35] behaviour for the service, when no one of the options above 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.

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): Per emulare il comportamento nativo della **PEC**, 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): To mimic the native behaviour of the **PEC**, 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

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. 57 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 appartenenti alla **REM-Policy-IT**, anche le seguenti opzioni:

the Header of the *original message*) with this 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. 57 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:

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**	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**
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:	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

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 REM 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	How per the dispositions of EN 319 532-3 **[3]**, Figure 1 e Figure 2, every REM dispatch and REM 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

formati (si vedano anche i punti G di pag. 36 e H di pag. 37 del § 4.3.4 del documento base). 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**.

(see also the points G at pag. 36 and H at pag. 37 of § 4.3.4 of the basic document). La **REM-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%

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%"

The SubmissionAcceptance.xml attachment contains service information on the transmission.
```

Figure 20 – REM dispatch – Introduction template – TXT format

```
      <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:</p>

      %VAR_RECIPIENTS_LIST%

      <BR>
      Il messaggio originale è incluso in allegato.

      <p>Identificativo messaggio: <a
href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a></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:</p>

      %VAR_RECIPIENTS_LIST%

      <BR>
      The original message is attached.

      <p>Message identifier: <a href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a></p>

      The SubmissionAcceptance.xml attachment contains service information on the transmission.
```

Figure 21 – REM dispatch – Introduction template – HTML format

```
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%

-------------------------------------------------------------------------------------

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%".
```

Figure 22 – REM 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:</p>

%VAR_RECIPIENTS_LIST%

<p>%VAR_RECEIPT_DESCRIPTION_IT%</p>

<p>Identificativo messaggio: <a
href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a></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:</p>
%VAR_RECIPIENTS_LIST%

<p>%VAR_RECEIPT_DESCRIPTION_EN%</p>

<p>Message identifier: <a href="mailto:%VAR_MESSAGE_IDENTIFIER%">%VAR_MESSAGE_IDENTIFIER%</a></p>.
```

Figure 23 – REM 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	REM 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)

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

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.

In some REM message are present further place holders like

%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.	**%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.	was accepted by the REM system.
TDE2	**SubmissionRejection**	RA02	è stato rifiutato dal sistema REM a causa di uno 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).
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 system 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 per cause indefinite (Codice RB02).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected due to undefined reasons (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 signature (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 invalid digital signature (Code RB06).
		RB07	ed inoltrato al REM service provider %REM_SERVICE_NAME% è stato rifiutato per un malfunzionamento generale (Codice RB07).	and relayed to the %REM_SERVICE_NAME% REM service provider was rejected 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 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 because it is unreachable (Code RB09).

		RB10	è stato rifiutato per un destinatario sconosciuto presso il REM service provider %REM_SERVICE_NAME% (Codice RB10).	was rejected due to unknown recipient to the %REM_SERVICE_NAME% REM service provider (Code RB10).
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 RD03).	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).
		RD04	non è stato consegnato nella mailbox del destinatario 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 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 presso il REM service provider REM_SERVICE_NAME% a causa di un malfunzionamento generale (Codice RD05).	was not consigned in the recipient's mailbox to %REM_SERVICE_NAME% REM service provider due to a general malfunction (Code RD05).
		RD06	non è stato consegnato nella mailbox del destinatario 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 to %REM_SERVICE_NAME% REM service provider due to message type not allowed (Code RD06).
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).

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 codice **RB10** (**UnknownRecipient**) può essere inserito

The events **TDE4** and **TDE5** in **Table 10** are considered together from the error code view point (and so they are in the same row of the table). In fact, as an example, the error due to the code **RB10** (**UnknownRecipient**) can be used in ERDS evidence issued on the occurrence

in ERDS evidence emesso su entrambi gli eventi. 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 **RB10** per l'S-REMS e a seguito di questa, l'S-REMS emette una REM relayFailure receipt 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**).

of both events. A first example of this case is that of a REM dispatch sent to a un-registered user to a R-REMS. It issues a REM relayRejection receipt for S-REMS with error code **RB10** and, in turn, the S-REMS issues a REM relayFailure receipt 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 standard | Authentication using standard 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 approfondire una modalità di utilizzo del servizio che consentisse elevati standard di sicurezza e contemporaneamente rendesse possibile l'accesso via protocolli classici della posta elettronica (SMTP/POP3/IMAP4).

Considerando che le modalità prescritte nello standard EN 319 521 **[8]**, Clause 5.2.2,

Introduction

A considerable part of the **PEC** service user experience is today is largely based on a fruition through the standard e-mail client.

In order to guarantee a ever-growing spread of the REM services it was necessary to deepen for the use mode of the service. This in order to allow, at the same time, highest security standards and to make it possible the access through the traditional e-mail protocols (SMTP/POP3/IMAP4).

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

punti a), b) e c) non risultano ancora sufficientemente diffuse nei vari prodotti di mercato, e quindi indisponibili attualmente all'utenza, 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). Il rimedio individuato si basa sulla produzione e fornitura di credenziali sufficientemente robuste in accordo al metodo descritto nel seguito.

Soluzione

Una volta che l'utente si è autenticato in modo "forte" accedendo ad una specifica applicazione messa a disposizione 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 - ha la possibilità di farsi rilasciare uno speciale *token* di sicurezza. Tale *token* può essere 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 SMTP/POP3/IMAP4.

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). The identified remedy is based on the ability of generating and provisioning of enough robust credentials, according to the following procedure.

Solution

Once the user is authenticated in a "strong" way using a specific application of 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 – she/he gains the possibility to obtain a special security *token*. Such *token* can 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 SMTP/POP3/MAP4.

The security practice to adopt (see § 2.6.1) will state the length and the validity period of the token (e.g. 2 months) that,

Le security practice da adottare (si veda il § 2.6.1) stabiliranno la lunghezza ed il periodo di validità del token (ad esempio 2 mesi), superato il quale il token dovrà essere rigenerato con il medesimo meccanismo.

Si noti che questa modalità di accesso è applicabile limitatamente a quelle situazioni che sono al di fuori dei ragionevoli margini di manovra del REMSP. In altre parole, la soluzione può essere utilizzata solo per i client utente o gli applicativi che per accedere al servizio REM possono utilizzare esclusivamente i protocolli standard (i.e. POP3, IMAP4, SMTP) per i quali non è possibile l'implementazione o l'adozione di meccanismi di autenticazione multi-fattore[36]. Non è invece giustificato che gli applicativi "web mail" o le "app mobile proprietarie" che sono sotto il controllo dell'REMSP utilizzino questa soluzione.

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

after witch, a new generation of the token, with the same mechanism, will be required.

Note that this access mode is applicable limitedly to those situations that are outside of a reasonable room of manoeuvre of the REMSP. In other words, the solution can be destined only for user's clients or applications that use exclusively standard protocols (i.e. SMTP, IMAP4, POP3) for which isn't possible the implementation or the adoption of authentication multi-factor mechanisms[36]

Whereas, is not justified that applications like web mail" or "custom mobile apps", that are under REMSP control, use this solution.

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.

[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.

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 2FA con username/password, seguita 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 classiche 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;

b) mutual TLS authentication, which includes advanced user's certificate;

c) advanced electronic signature

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 2FA with username/password, followed by a 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[TBD] clause 5.2.2 (and summarized below for information):

a) multi factor authentication mechanisms;

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 una 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 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 della 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).

La password così ottenuta può essere applicata, tramite copia/incolla, nel classico client di posta elettronica standard che si

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 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 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 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 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.

intende utilizzare per accedere al servizio REM (si veda **Figure 27**).

Segue l'esempio completo.

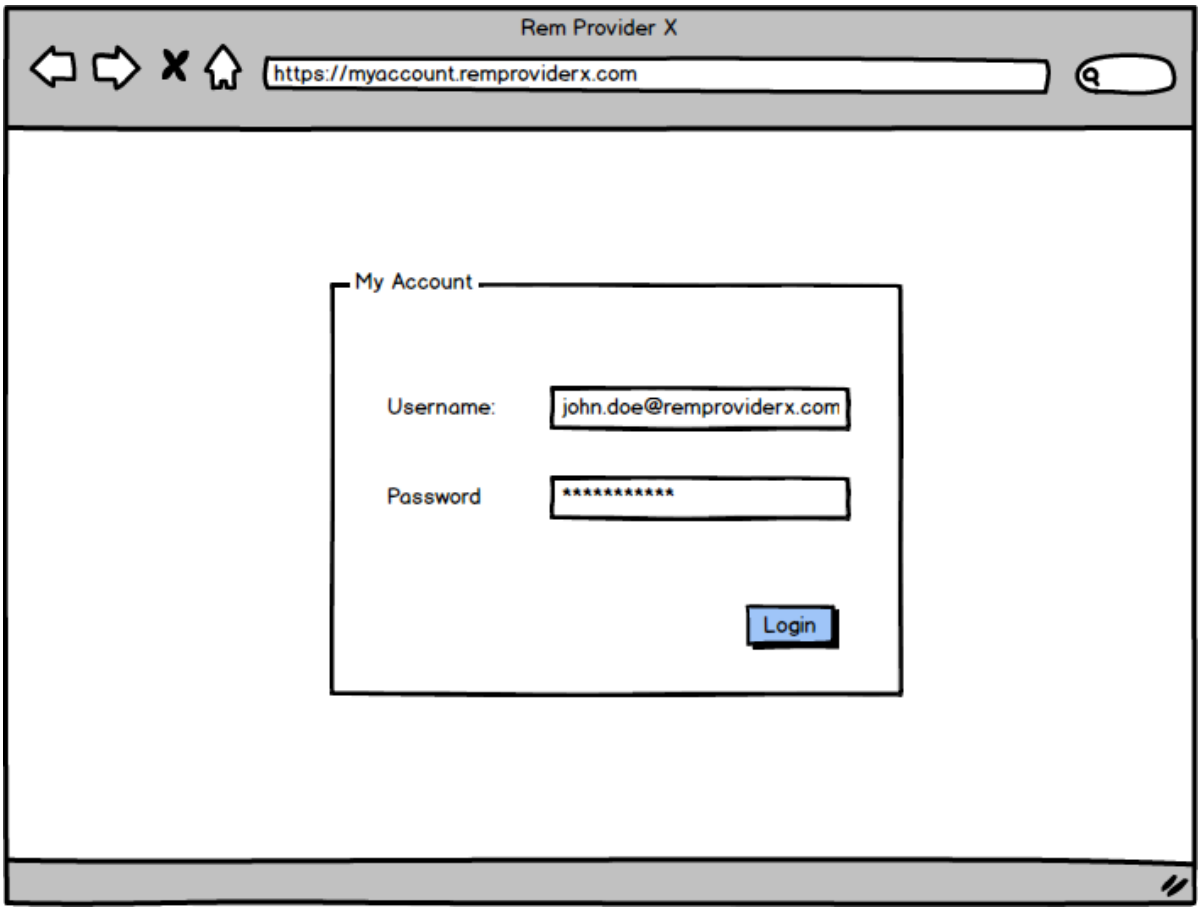

Figure 24 – User's login to the token generation service (panel)

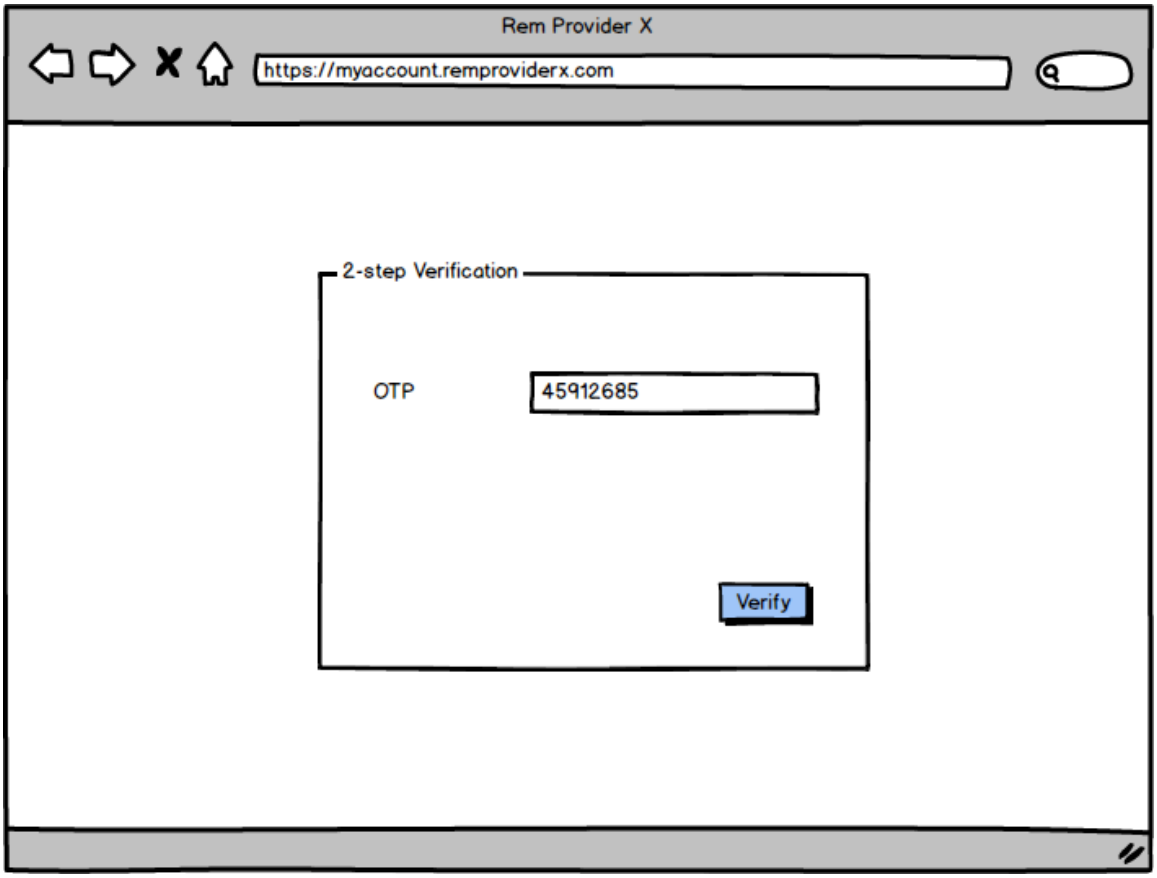

Figure 25 – Verification of the OTP for the multifactor authentication

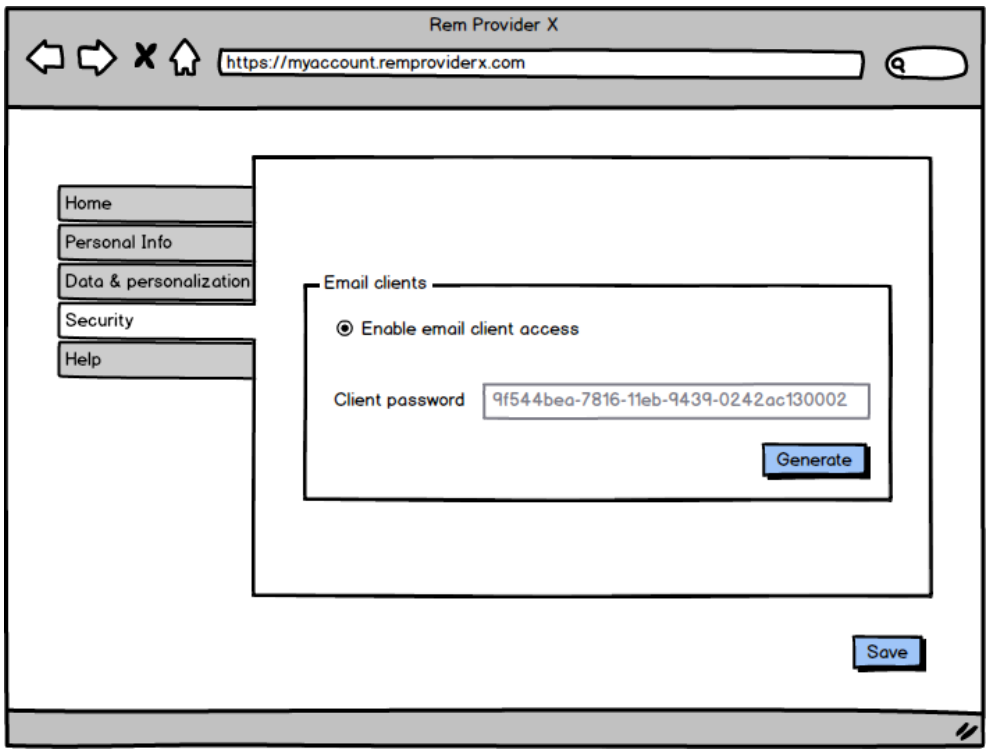

Figure 26 – Enabling client access and token generation to use as client password

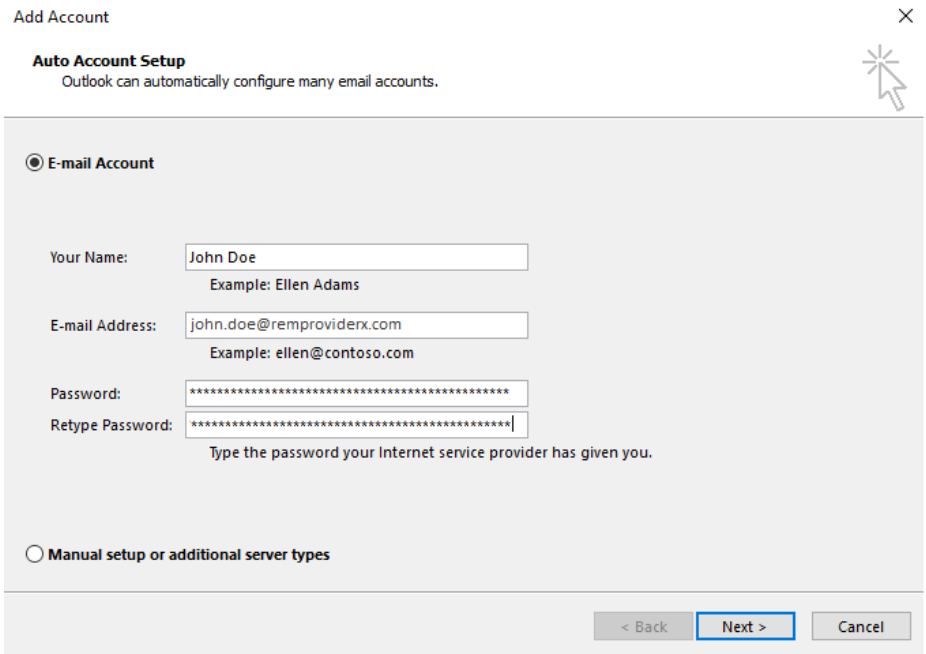

Figure 27 – Updating the password with the secure token generated on the panel

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.

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 (Secure Domain Name System Deployment Guide).

- Utilizzare un DNS Resolver privato opportunamente protetto da accessi esterni.

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.

One of the most common attack 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 (Secure Domain Name System Deployment Guide).

- Use of a private DNS Resolver properly protected from external access.

• 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 l'interfaccia di Relay 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. Inoltre, la **REM-Policy-IT** prevede che il file CapabilityAndSecurityInformation.xml di ciascun REMS sia firmato digitalmente in accordo a quanto prescritto nel § 2.3.2.4.

Ulteriori misure potranno essere man mano predisposte in accordo alle evoluzioni delle security practice nazionali che ne

• 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. Furthermore, the **REM-Policy-IT** requires that the file CapabilityAndSecurityInformation.xml of any REMS is digitally signed according to the prescriptions of § 2.3.2.4.

Further measures can be gradually arranged according to the national security practices evolutions that can even more fine-

potranno ampliare e perfezionare l'attuazione. A titolo esemplificativo, il recente standard ***IETF RFC 8460*** offre preziosi spunti che possono essere trasposti nel campo del monitoring del DNS nella REM così come usato nella **REM baseline** (si veda il § 2.6.1).

tune and improve the application. By way of example, the recent ***IETF RFC 8460*** 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 Politiche di 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. Queste 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.2.6.1, C.3.6.2 e C.3.6.3, nei casi h) 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 (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.

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.2.6.1, C.3.6.2 and C.3.6.3, in the elements h) 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 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 più soluzioni di Protezione Anti-Malware in cascata, in osservanza alle "security-practice" vigenti (si veda § 2.6.1).

La gestione del Malware 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 viene gestito tramite la generazione di una o più REM receipt, ognuna, a sua volta, 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, viene generata una REM receipt con allegata una ERDS Evidence caratterizzata

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 follows a different flow depending if 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 REM receipts, each, in turn, containing the appropriate ERDS Evidence according to the following details.

come dal seguente stralcio esemplificativo ed i valori della **Table 11**.

L'evento di **SubmissionRejection** viene restituito al mittente tramite REM receipt.

Malware detected by the sender's REMSP

In case of Malware detected by the sender's REMSP, a REM 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 REM 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 319 522-2 **[6]**, 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 7
MDD4	EventReason/Details	Malware found in ERD original message	EN 319 522-2 **[6]**, Table 7
MDD5	EventReason/Details	Further details	Free custom text (optional)

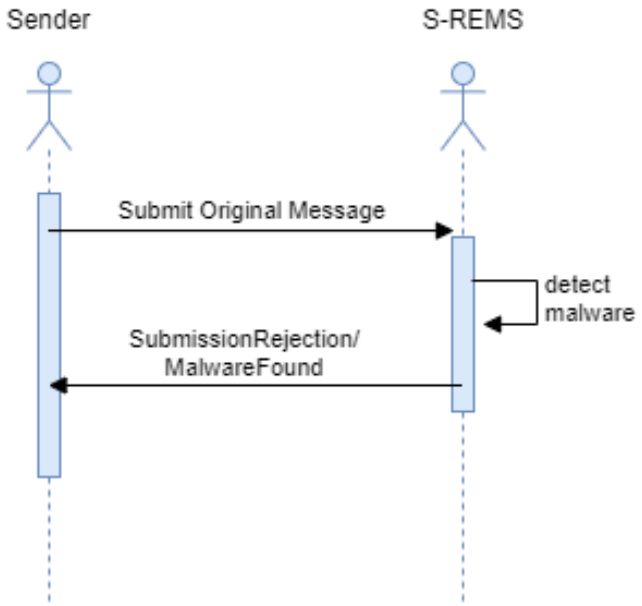

Figure 29 – Malware detected by S-REMS

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 REM 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 REM 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 319 522-2 **[6]**, 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 7
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 7
MID5	EventReason/Details	Further details	Free custom text (optional)

```
<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 319 522-2 **[6]**, Table 2
MID7	**EventReason/Code**	http://uri.etsi.org/19522/EventReason/**R_ERDS_MessageRejectedForMalware**	EN 319 522-3 **[7]**, Table 3
MID8	EventReason/Details	**RB03**	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 7
MID10	EventReason/Details	Further details	Free custom text (optional)

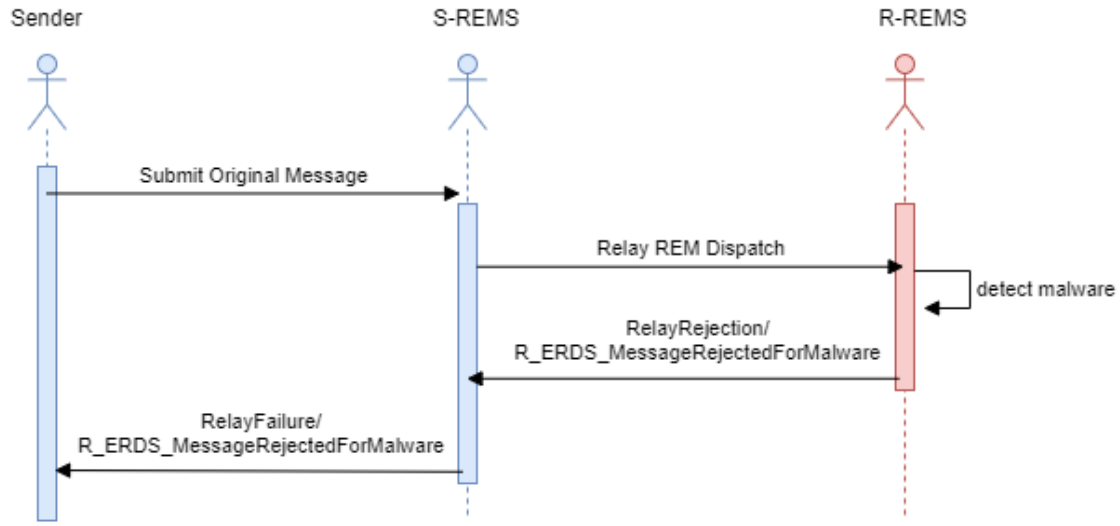

Figure 32 – Malware detected by R-REMS

2.4.2.10 Formato Subject e nome XML ERDS evidence | Subject format and ERDS evidence XML name

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. 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. La seguente **Table 14** definisce il mapping completo.

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. 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 **Table 14** for the full mapping.

Table 14 – Subject and Evidence formats in REM-Policy-IT

Id	Subject:	REM_EVIDENCE_NAME	Note
SEF1	**REM SubmissionAcceptance**: <orig subj>	**SubmissionAcceptance**.xml	REM receipt for the sender
SEF2	**REM SubmissionRejection**: <orig subj>	**SubmissionRejection**.xml	REM receipt for the sender
SEF3	**REM dispatch**: <orig subj>	**SubmissionAcceptance**.xml	REM dispatch for the recipient(s)
SEF4	**REM ContentConsignment**: <orig subj >	**ContentConsignment**.xml	REM receipt for the sender
SEF5	**REM ContentConsignmentFailure**: <orig subj >	**ContentConsignmentFailure**.xml	REM receipt for the sender
SEF6	**REM RelayAcceptance**: <orig subj >	**RelayAcceptance**.xml	REM receipt for S-REMS
SEF7	**REM RelayRejection**: <orig subj >	**RelayRejection**.xml	REM receipt for S-REMS
SEF8	**REM RelayFailure**: <orig subj >	**RelayFailure**.xml	REM receipt for the sender
SEF9	**REM EXTERNAL**: <orig subj >	**ReceivedFromNonERDS**.xml	REM dispatch for the recipient(s)
SEF10	**REM RelayToNonERDS**: <orig subj >	**RelayToNonERDS**.xml	REM receipt for the sender
SEF11	**REM RelayToNonERDSFailure**: <orig subj >	**RelayToNonERDSFailure**.xml	REM 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), e deve avere l'extension X509v3 Subject Alternative Name come indicato in **PP6** della **Table 2** § 2.3.1 e **AP4** della **Table 4** § 2.4.1.
- 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 illustrata in **Figure 33**.

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 digital signature), and must have the extension X509v3 Subject Alternative Name 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 illustrated in **Figure 33**.

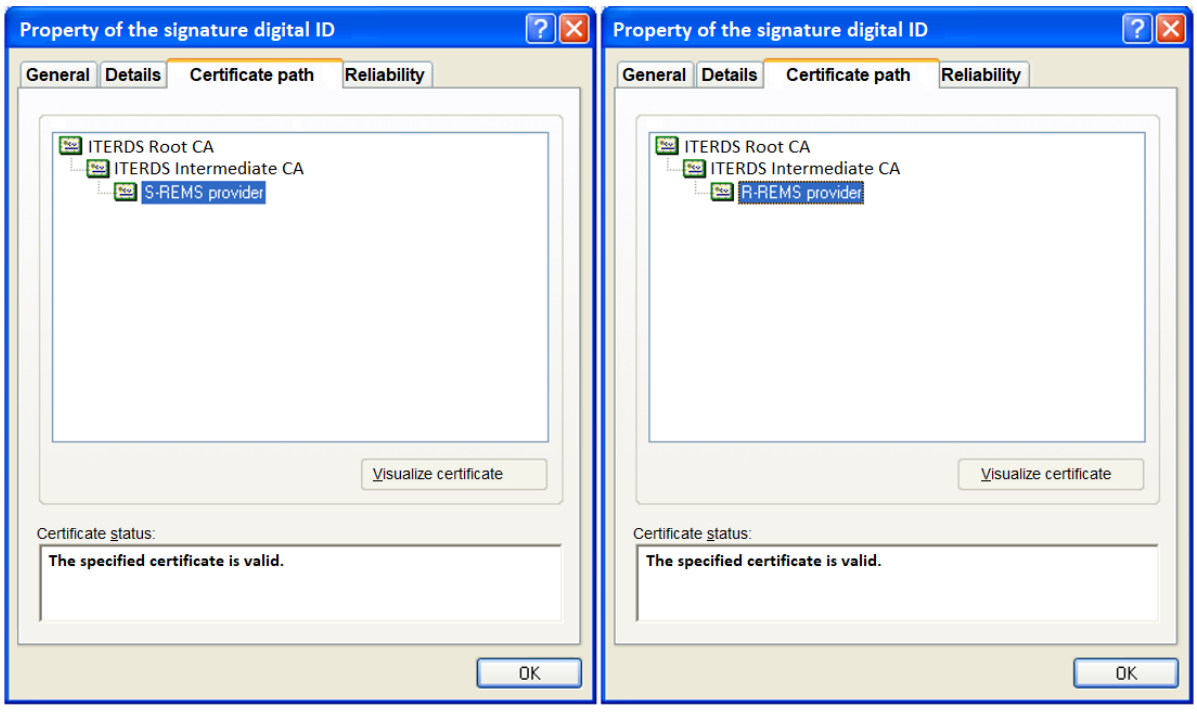

Figure 33 – Digital certificates: hierarchical chain for S-REMS and R-REMS

ITERDS_REM_test_services_S-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 = S-REMS provider
X509v3 extensions:
    X509v3 Certificate Policies:
        Policy: 1.2.840.113549.1.9.16.1.34
    X509v3 Key Usage: critical
        Digital Signature
    X509v3 Extended Key Usage:
        E-mail Protection
    X509v3 Subject Alternative Name:
        email:rem-service@s-rems-only-for-test.it
```

ITERDS_REM_test_services_R-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 = R-REMS provider
X509v3 extensions:
    X509v3 Certificate Policies:
        Policy: 1.2.840.113549.1.9.16.1.34
    X509v3 Key Usage: critical
        Digital Signature
    X509v3 Extended Key Usage:
        E-mail Protection
    X509v3 Subject Alternative Name:
        email:rem-service@r-rems-only-for-test.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 extensions:
    X509v3 Key Usage:
        Certificate Sign, CRL Sign
    X509v3 Certificate Policies:
        Policy: 1.2.840.113549.1.9.16.1.34
    X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
```

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 Basic Constraints: critical
        CA:TRUE
```

Figure 34 – Digital certificates: Main properties

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 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*.

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 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*.

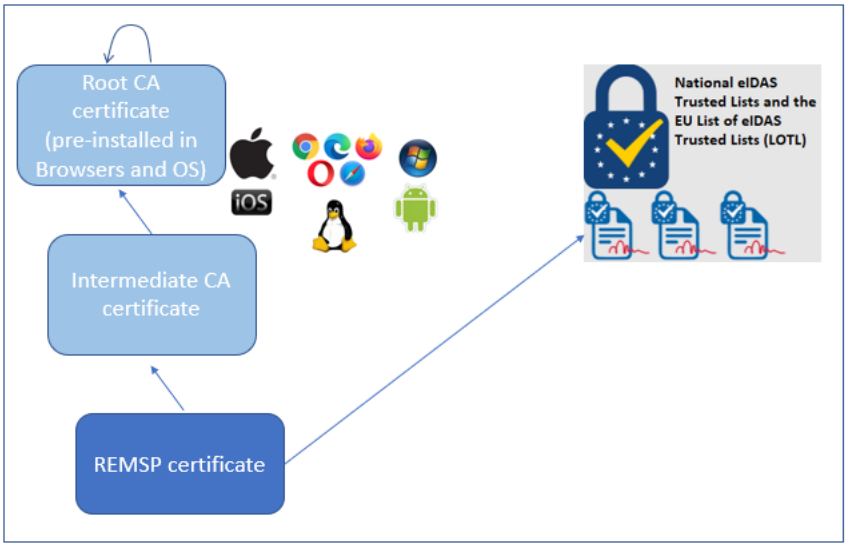

Figure 35 – Digital certificates: cross-certification system

Per realizzare il *qualification trust anchor* è necessario che il certificato "foglia" venga assicurato nell'elemento <ServiceDigitalIdentity> della TL così come specificato nella **REM baseline** in EN 319 532-4 **[4]**, Clause C.2.3.3.3, element 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 allegato alla firma digitale assieme al certificato "foglia" per permettere la ricomposizione dell'intera catena.

Si noti che, tipicamente il certificato utilizzato dal REMSP per la firma digitale dei REM message e delle ERDS evidence ha una durata limitata (es. 3 anni). 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

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.2.3.3.3, element 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*, 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 ERDS evidences has a limited period of validity (e.g. 3 years). 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 evidences 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.

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 degli ERDS evidence XML sia all'interno della TL, nella sezione dedicata alla definizione del servizio REM (TSPService con identificativo tipologia 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 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

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 (service 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 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

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)	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">REM Provider 1 CC</Name>
          <Name xml:lang="cc">TBD in CC language</Name>
        </ServiceName>
        <ServiceDigitalIdentity>
          <DigitalId>
            <X509Certificate>QUJDMTIzCg==</X509Certificate> <!-- Current Certificate-->
          </DigitalId>
          <DigitalId>
             <X509SubjectName>CN=REM Provider 1 CC, O=Org 1 CC, C=CC</X509SubjectName>
          </DigitalId>
          <DigitalId>
            <X509SKI>bDdPQjdoMFVYREhGNDNZakFzbFhzPQo=</X509SKI>
          </DigitalId>
        </ServiceDigitalIdentity>
        <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
        <StatusStartingTime>2021-12-30T22:00:00Z</StatusStartingTime>
        <SchemeServiceDefinitionURI>
        <!--[OMISSIS]-->
        </SchemeServiceDefinitionURI>
        <ServiceSupplyPoints>
          <ServiceSupplyPoint>smtp:rem-provider-1-MX-record.cc:25</ServiceSupplyPoint>
          <ServiceSupplyPoint>https://rem-provider-1-
service.cc/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">REM Provider 1 CC</Name>
          <Name xml:lang="cc">TBD in CC language</Name>
        </ServiceName>
        <ServiceDigitalIdentity>
          <DigitalId>
            <X509Certificate>XWJDNTIzCg==</X509Certificate> <!-- Expired certificate-->
          </DigitalId>
          <DigitalId>
             <X509SubjectName>CN=REM Provider 1 CC, O=Org 1 CC, C=CC</X509SubjectName>
          </DigitalId>
          <DigitalId>
```

```
            <X509SKI>aBdPRjeoMFVYREhGNDNZakFzbFhzPQo=</X509SKI>
          </DigitalId>
        </ServiceDigitalIdentity>
        <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
        <StatusStartingTime>2021-12-30T22:00:00Z</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 Politiche generali di identificazione e autenticazione | General policy of dentification and authentication

Le politiche relative all'identificazione e autenticazione fanno riferimento agli standard e alle norme vigenti. Si vedano per più dettagli il § 2.2 nelle sezioni Utenza Registrata, Identificata e Autenticata, la nota[27] a pag. 11 e il § 2.4.2.7 per l'autenticazione da client di posta elettronica standard.

The policy relevant to identification and authentication makes reference to the standards and the regulation in force. For more details see § 2.2 in Registered, Identified and Authenticated Users sections, the note[27] at pag. 11 and § 2.4.2.7 for the authentication from standard e-mail client.

2.4.2.13 Politiche 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

In order to ensure the maximum degree of interoperability (especially with regard to that cross-border), for the types of transmission between registered users

tipologia **TUC1** in **Table 1**), il livello di assurance (LoA da qui in avanti), richiesto per il sender nell'elemento **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 44, element 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 al punto 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 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

account (i.e. as per the type **TUC1** in **Table 1**), the level of assurance (LoA hereinafter), required for the sender in the element **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 44, element 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 point 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 higer level and, meanwhile, to 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 S-REMS, on the base of its

base della propria policy, non può richiedere un **REM-RecipientAssuranceLevel**, all'utenza ricevente, differente da "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 ul suddetto header è assente nella **REM baseline**.

policies, or of specific requests from the sender cannot require a **REM-RecipientAssuranceLevel** to the recipient that is different from "substantial". 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

2.5 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

The **Table 15** contains a compact and correlated version of events and error codes

errore presenti ed usati in più punti del presente documento.

present and used in many points of the present document.

Table 15 – Events and Reason codes in REM-Policy-IT

Event and (code) Table 1 EN 319 522-1 [5]	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
	RA04	http://uri.etsi.org/19522/EventReason/SenderSigningCertExpiredOrRevoked	N
	RA05	http://uri.etsi.org/19522/EventReason/S_ERDS_PolicyViolation	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
RelayFailure (B.3)	RB06	http://uri.etsi.org/19522/EventReason/R_ERDS_PolicyViolation	Y
	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
	RB51	*http://uri.etsi.org/19522/EventReason/R_ERDS_MessageNotAcceptedInTime*	*N*
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
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

The events F.1, F.2 e F.3 are not part of the **REM baseline** (and then of the cross-

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).

Si noti che i seguenti error code non sono 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, e quindi per questa ragione, per uniformità vengono posti sempre sotto la stessa URI base di ETSI), a livello di **REM-Policy-IT** può risultare comodo definire i seguenti:

RB51 *http://uri.etsi.org/19522/EventReason/R_ERDS_MessageNotAcceptedInTime*
RF51 *http://uri.etsi.org/19522/EventReason/RelayToNonERDSNotAllowed*

Invece, l'evento **RA04** si riferisce alla firma digitale incorporata nel messaggio originale che è out-of-scope rispetto al trasporto del messaggio e pertanto non previsto che il REMS usi tale codice nella **REM baseline**

border interoperability) but are used at **REM-Policy-IT** level for the interoperability with the ordinary email (see § 2.4.2.2).

The following error codes are not part of the **REM baseline** but since the standard allows to define new CustomCodes (as it clearly follows from the tables of the document EN 319 522-2 **[6]**, Clause 8.3.3, and then for this reason they are put for uniformity under the same ETSI base URI), can be useful to define, at **REM-Policy-IT**, the following codes:

RB51 *http://uri.etsi.org/19522/EventReason/R_ERDS_MessageNotAcceptedInTime*
RF51 *http://uri.etsi.org/19522/EventReason/RelayToNonERDSNotAllowed*

Whereas the event **RA04** 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 REMS uses such code in 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 (quali ad esempio parametri di competenza, password policy, lunghezza/durata token e

Regarding the general and security practices (such as, for example, reference parameters, password policy,

chiavi, certificati, TL, DNS, misure anti-malware, ma anche parametri aggiornati anche se già specificati come valore iniziale nel presente documento) fare riferimento alle apposite note emesse dalla REMID Authority.

length/duration of tokens and keys, TL, DNS, anti-malware measures, but also updated parameters even if already specified as initial value in the present document) refer to the appropriate notes issued by REMID Authority.

2.7 Esempi di formati REM | Examples of REM formats

2.7.1 Generalità e struttura | General properties and structure

Viene fornito, assieme all'allegato tecnico, lo zip file `STESSO-NOME-DEL-DOCUMENTO.latest_version.zip` contenente vari esempi che racchiudono un semplice ed intero ciclo di interscambio di tipo REM (in accordo alla **REM baseline**) 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). Per comodità sono fornite, oltre che allegate ovviamente in ognuno dei REM message, le ERDS evidence come XML stand-alone.

The zip file `SAME-NAME-OF-DOCUMENT.latest_version.zip` is provided as an attachment of the present document. It contains a set of examples of a simple and full cycle of REM interchange (according to the **REM baseline**), 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). The ERDS evidence XMLs are provided as stand-alone files, for the convenience of the users of these examples.

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.

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.

All the files provided with the examples, besides being bound to the respective applications associated to any filename extension, are also in pure text format. So they can be opened and inspected by any common text editor.

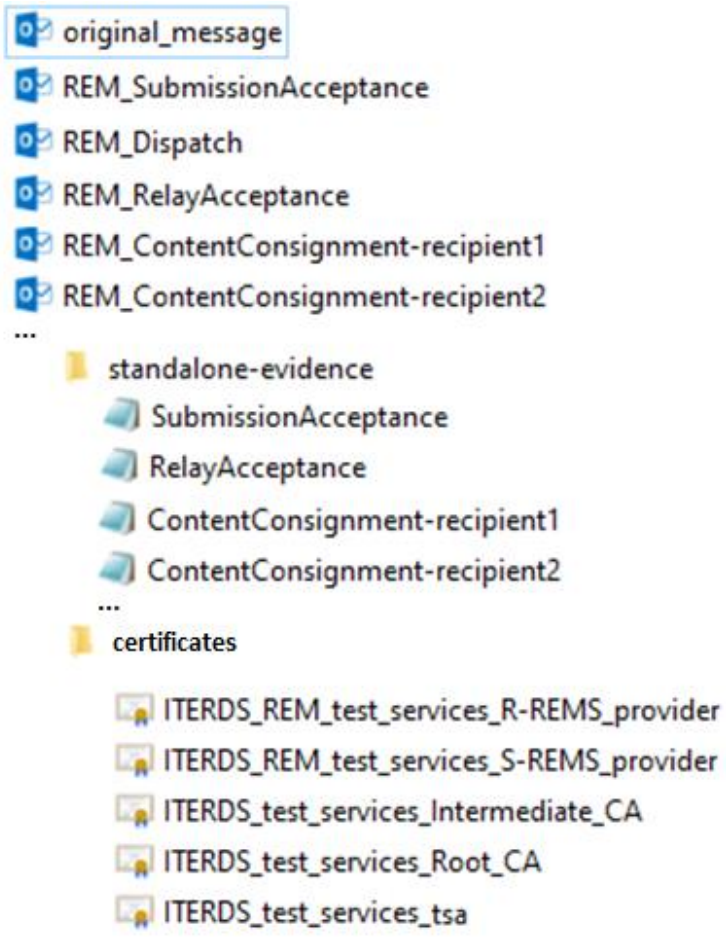

Figure 38 – Examples: structure of the folders

2.7.2 original messages

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

Used inside REM baseline circuit flows:

`original_message.clean_from_user(.eml)`
`original_message.eml.to_attach`
`original_message.eml.to_attach.digest`

Used for flow towards NonERDS systems:

`original_messageExt.clean_from_user(.eml)`
`original_messageExt.eml.to_attach`
`original_messageExt.eml.to_attach.digest`

Used for flow from NonERDS systems:

`original_messageFromExt.clean_from_user(.eml)`
`original_messageFromExt.eml.to_attach`
`original_messageFromExt.eml.to_attach.digest`

2.7.3 REM dispatch

Si veda l'esempio contenuto nel file:

See the example contained in the file:

`REM_Dispatch.RA01(.eml)`

2.7.4 REM receipt - full set

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)

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)

2.7.4.5 REM_ RelayFailure

Si vedano gli esempi contenuti nei seguenti file:	See the examples contained in the following files:

REM_RelayFailure.RB07(.eml)

```
REM_RelayFailure.RB08(.eml)
REM_RelayFailure.RB09(.eml)
REM_RelayFailure.RB10(.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_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]
```

2.7.5 ERDS evidence – (standalone) full set

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
```

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)
RelayFailure.RB07(.xml)
RelayFailure.RB08(.xml)
RelayFailure.RB09(.xml)
RelayFailure.RB10(.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]
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]
```

2.7.5.4 RelayToNonERDS - RelayToNonERDSFailure

Si vedano gli esempi contenuti nei seguenti file:

See the examples ontained in the following files:

```
SubmissionAcceptanceExt.RA01(.xml)
RelayToNonERDS.RF01(.xml)   [for the first user]
RelayToNonERDSFailure.RF02(.xml)   [for the second user]
RelayToNonERDSFailure.RF03(.xml)   [for the second user]
RelayToNonERDSFailure.RF51(.xml)   [for the second user]
```

2.7.5.5 ReceivedFromNonERDS

Si vedano gli esempi contenuti nei seguenti file:

See the examples contained in the following files:

```
ReceivedFromNonERDS.RF04(.xml)
```

2.7.6 REM messages from/to ordinary email

2.7.6.1 REM_EXTERNAL (ReceivedFromNonERDS)

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
REM_EXTERNAL.RF04(.eml)
```

2.7.6.2 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)
```

2.7.6.3 REM_RelayToNonERDS

Si veda l'esempio contenuto nel file:

See the example contained in the file:

```
REM_RelayToNonERDS.RF01(.eml)
```

2.7.6.4 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)
```

2.8 Raccomandazioni per sviluppatori ed integratori | Recommendation for developers and system integrators

2.8.1 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.

2.8.2 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 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.

Ciò è di per sé una considerevole forma di 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.

Le seguenti raccomandazioni forniscono delle linee guida 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

In case of a message that comes from outside the border or from other policy (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.

This is per sé a considerable form of interoperability. Said that, the legal effects and/or the applicative uses that can effectively arise from such transport are out of scope in respect to the present policy.

The following recommendations gives some guidelines 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 a 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

firma digitale (cioè esterni alla sezione protetta 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**" 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 decisioni da prendere su di essi è sempre la

section). The reference to these headers 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

miglior strategia. Spesso, per avere un dato certo, risulterà quindi necessario effettuare un fallback 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 conduct a fallback to the ERDS evidence (that is authoritative) or to 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.

2.8.3 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 § 2.8.2 sugli header. Solo che in questo caso l'attenzione è concentrata sulla presenza o meno di MIME part addizionali che rientrino nelle suddette estensioni.

Così come per le raccomandazioni del § 2.8.2, i sistemi REM (e quindi anche le varie applicazioni che vi afferiscono come utilizzatori) 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.

Even in case of the S/MIME extensions outlined in the REM standard are valid the similar considerations as per the § 2.8.2 on the headers. Except in this case the attention is concentrated on the presence of additional MIME parts that fall in the aforementioned extensions.

As per the recommendations of § 2.8.2, the REM systems (and so also the various applications that use them), inside the REMID policy=**REM-Policy-IT**, have to reveal forms of resilience in respect to additional body parts (in the MIME structure of incoming REM messages) that fall in the REM standard S/MIME extension scheme.

Anche in questo caso è necessario che il REM service 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.

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.

Even in this case, it is necessary that the REM service 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.

This constitutes a second considerable form of flexibility during the interoperability. Then, the legal effects and/or the applicative uses that can effectively arise from such transport are out of scope in respect to the present policy.