AGID | Agenzia per l'Italia Digitale

Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici

lettera b) comma 3-ter articolo 73 e dell'articolo 51 del Decreto Legislativo 7 marzo 2005, n. 82

Versione 2.0 del 13/12/2022

Versione	Data	Tipologia modifica
1	21/05/2021	Prima emissione
2	13/12/2022	Allineamento ad avviso AgID nr. 18 del 15 aprile 2021

Sommario

Introduzione **5**
Capitolo 1 Ambito di applicazione **6**
1.1 Soggetti destinatari 6
Capitolo 2 Riferimenti e sigle **7**
2.1 Note di lettura del documento 7
2.2 Struttura 7
2.3 Riferimenti Normativi 8
2.4 Termini e definizioni 8
Capitolo 3 Principi generali **9**
3.1 Dominio di interoperabilità 9
3.2 Erogatore 9
3.3 e-service 9
3.4 Fruitore 9
Capitolo 4 Sicurezza a livello di trasporto **10**
Capitolo 5 Sicurezza a livello applicativo **11**
5.1 Tecnologia REST 11
5.1.1 JSON - JavaScript Object Notation 12
5.1.2 JWS - JSON Web Signature 12
5.1.3 JWK - JSON Web Key 13
5.1.4 JWE - JSON Web Encryption 13
5.1.5 JWT - JSON Web Token 14
5.1.6 JWA - JSON Web Algorithms 15
5.1.7 OAuth 2.0 15
5.2 Tecnologia SOAP 16
5.2.1 XML - eXtensible Markup Language 16
5.2.2 XML-canonicalization 17
5.2.3 XML-signature 17
5.2.4 XML-encryption 17
5.2.5 WS-security 18
Capitolo 6 Costituzione trust tra soggetti interessati **19**
6.1 Certificati digitali utilizzabili 20
6.1.1 Tipologia certificati digitali 20

6.1.2 Object identifier per l'identificazione delle pubbliche amministrazioni 20
6.2 Modalità di emissione e distribuzione dei certificati digitali 23
6.2.1 Certificati digitali emessi da CAQ eIDAS 23
6.2.2 Certificati digitali emessi all'interno di domini di interoperabilità specifici .. 24
6.2.3 Principi per la scelta delle modalità di emissione dei certificati digitali..... 25

Introduzione

Le Linee Guida, si focalizzano sulle tecnologie e le loro modalità di utilizzo al fine di garantire la sicurezza delle transazioni digitali realizzate tra e verso le pubbliche amministrazioni che utilizzano le application programming interface tramite rete di collegamento informatica (di seguito API).

Le Linee Guida contribuiscono alla definizione del modello di interoperabilità delle pubbliche amministrazioni (di seguito ModI), definito da AgID ai sensi della lettera b) comma 3-ter articolo 73 del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni (di seguito CAD).

Le Linee Guida sono adottate ai sensi dell'articolo 71 e della Determina AgID n. 160 del 2018 recante "Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale".

Capitolo 1

Ambito di applicazione

Le Linee Guida individuano, ai sensi della lettera b) comma 3-ter articolo 73 e dell'articolo 51 del CAD, le soluzioni tecniche idonee a garantire l'autenticazione dei soggetti coinvolti e la protezione, l'integrità e la riservatezza dei dati scambiati nelle interazioni tra sistemi informatici della pubblica amministrazione e di questi con i sistemi informatici di soggetti privati per il tramite di API.

Le interazioni tra sistemi informatici oggetto del ModI prevedono che i soggetti coinvolti possano svolgere la funzione di erogatore di servizi, quando il soggetto mette a disposizione servizi digitali utilizzati da altri soggetti, e la funzione di fruitore, quando il soggetto utilizza i servizi digitali messi a disposizione da un altro soggetto.

1.1 Soggetti destinatari

Le Linee Guida sono destinate ai soggetti di cui al comma 2 dell'articolo 2 del CAD, che la attuano nella realizzazione dei propri sistemi informatici che fruiscono o erogano dati e/o servizi digitali di/ad altri soggetti tramite API.

Le Linee Guida sono rivolte ai soggetti privati che devono interoperare con la Pubblica Amministrazione per fruire di dati e/o servizi tramite sistemi informatici tramite API.

Capitolo 2

Riferimenti e sigle

2.1 Note di lettura del documento

Conformemente alle norme ISO/IEC Directives, Part 3 per la stesura dei documenti tecnici la presente linea guida utilizzerà le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «DOVREBBE», «NON DOVREBBE», «PUO'», «POSSONO» e «OPZIONALE», la cui interpretazione è descritta di seguito.

- **DEVE** o **DEVONO**, indicano un requisito obbligatorio per rispettare la linea guida;
- **NON DEVE** o **NON DEVONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE** o **NON DOVREBBE**, indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi;
- **PUÓ** o **POSSONO** o l'aggettivo **OPZIONALE**, indica che il lettore può scegliere di applicare o meno senza alcun tipo di implicazione la specifica.

2.2 Struttura

Le Linee Guida includono i seguenti Allegati:

- Raccomandazioni in merito allo standard Transport Layer Security (TLS);
- Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST.

Considerata la velocità dell'innovazione, le Linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di prevedere un testo "statico" che contenga la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" potranno adeguarsi agevolmente all'evoluzione tecnologica. Tale processo di costante adeguamento degli «allegati» è realizzato in coerenza con il quadro normativo e attuativo in materia di digitalizzazione e nello specifico ai sensi della lettera a del comma 2 dell'articolo 14-bis del CAD che assegna ad AgID la funzione di "emanazione di Linee guida contenenti regole, standard e guide tecniche, nonche" di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di

atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea".

2.3 Riferimenti Normativi

Sono riportati di seguito gli atti normativi di riferimento del presente documento.

[CAD] decreto legislativo 7 marzo 2005, n. 82 recante «Codice dell'Amministrazione Digitale»

[EIF] European Interoperability Framework (EIF)

[CE 2008/1205] Regolamento (CE) n. 1205/2008 della Commissione del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati

[D.lgs. 196/2003] Codice in materia di protezione dei dati personali

[UE 679/2016] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR)

[UE 910/2014] Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (in breve eIDAS)

2.4 Termini e definizioni

Di seguito si riportano gli ACRONIMI che verranno utilizzati nella presente Linee Guida:

[AgID] Agenzia per l'Italia Digitale

[API] Application Programming Interface

[IPA] Elenco di cui all'articolo 6-ter del CAD

[ModI] Modello di Interoperabilità delle Pubbliche Amministrazioni Italiane

[OID] Object identifier

[REST] Representational State Transfer

[SOAP] Simple Object Access Protocol

[WS-*] Lo stack degli standard emanati relativi alle tecnologie SOAP, tra cui SOAP, WSDL, WS-Security, WS-Addressing e WS-I

[XML] eXtensible Markup Language

Capitolo 3

Principi generali

3.1 Dominio di interoperabilità

Con dominio di interoperabilità si indica uno specifico contesto in cui più pubbliche amministrazioni e/o soggetti privati abbiamo l'esigenza di scambiare dati e/o integrare i propri processi per il tramite API.

Il dominio di interoperabilità può essere regolato da specifici accordi che DEVONO essere conformi al ModI.

3.2 Erogatore

Un'organizzazione che rende disponibile e-service ad altre organizzazioni, per la fruizione di dati in suo possesso, o l'integrazione dei processi da esso realizzati.

3.3 e-service

I servizi digitali realizzati da un Erogatore, attraverso l'implementazione delle necessarie API conformi al ModI per assicurare l'accesso ai propri dati e/o l'integrazione dei propri processi ai Fruitori.

3.4 Fruitore

Un'organizzazione che utilizza gli e-service messi a disposizione da un Erogatore.

Capitolo 4

Sicurezza a livello di trasporto

Al fine di garantire autenticazione, integrità dei dati e confidenzialità tra ente fruitore, le comunicazioni DEVONO avvenire utilizzando il protocollo di comunicazione HTTPS (HTTP over TLS).

Il Transport Layer Security (TLS) è un protocollo che permette di stabilire un canale con le proprietà di integrità e riservatezza in senso crittografico tra un client e un server. Dopo aver stabilito una connessione sicura tramite il protocollo TLS, le applicazioni possono utilizzarla per scambiare dati. TLS viene utilizzato in molteplici contesti applicativi come ad esempio HTTPS, SMTPS, e altri ancora.

I requisiti crittografici minimi per stabilire una connessione sicura, riguardanti la versione del protocollo TLS e le cipher suite da utilizzare sono contenuti nell'allegato "Raccomandazioni in merito allo standard Transport Layer Security (TLS)".

Data la continua evoluzione tecnologica e la possibile scoperta di nuove vulnerabilità, l'allegato "Raccomandazioni in merito allo standard Transport Layer Security (TLS)" verrà aggiornato periodicamente nei modi indicati al paragrafo Struttura .

In caso di evidenza di vulnerabilità di nuova scoperta che richiedano un intervento immediato in merito alle indicazioni fornite nell'allegato "Raccomandazioni in merito allo standard Transport Layer Security (TLS)" verranno emanati specifici avvisi di sicurezza.

[SIC_ API_01] I soggetti destinatari DEVONO utilizzare la versione TLS e le cipher suite indicate nell'allegato "Raccomandazioni AgID in merito allo standard Transport Layer Security (TLS)".

Capitolo 5

Sicurezza a livello applicativo

Il livello applicativo include gli standard e best practice, utilizzati dai sistemi informatici per fornire dati e servizi ad un attore umano (comunicazione human-to-machine) o scambiare dati con altri sistemi informatici (comunicazione machine-to-machine) sulle connessioni di rete stabilite a livello di trasporto.

Il ModI individua SOAP e REST quali tecnologie da utilizzare per implementare le interazioni tra erogatori e fruitori.

Di seguito sono riportati, raggruppati per le tecnologia, gli standard da utilizzare per assicura la sicurezza delle interazioni nel ModI.

[SIC_API_02] I soggetti destinatari DEVONO utilizzare gli standard indicati per assicurare la sicurezza delle transazioni implementate tramite API.

5.1 Tecnologia REST

REST individua, accettando il livello 1 del Richardson Maturity Model[1], una modalità per implementare servizi basati sul protocollo HTTP che operano sulle risorse definite secondo la sintassi e la semantica previste per le URI e, sulle quali, si opera invocando delle operazioni (HTTP method) che agiscono su di esse. Il ModI include tale tecnologia per l'implementazione delle API.

Nel contesto delle tecnologie REST, in relazione ai temi oggetto delle Linee Guida, si evidenziano le specifiche JSON-based JWT (JSON Web Token), JWS (JSON Web Signatures), JWK (JSON Web Key), JWE (JSON Web Encryption) e JWA (JSON Web Algorithms) per assicurare la sicurezza dei messaggi scambiati tramite API REST.

[1] Cf. https://martinfowler.com/articles/richardsonMaturityModel.html

5.1.1 JSON - JavaScript Object Notation

JSON è un formato di interscambio di dati leggero, basato su testo e indipendente dal linguaggio di programmazione.

JSON è basato su due strutture:

- gli oggetti, cioè una serie non ordinata di nomi/valori
- gli array, cioè una raccolta ordinata di valori

Dove i valori possono essere stringhe, numeri, valori booleani (true/false), oggetti o array.

JSON è definito dall'Internet Engineering Task Force nell'RFC 8259[2], a cui si rimanda per approfondimenti.

Come tutti i formati di interscambio general-purpose e che permettono l'utilizzo di strutture nidificate, in alcuni ambiti può essere opportuno limitare l'espressività della notazione (eg. limitando il numero di oggetti nidificati in fase di processamento o di serializzazione). Si veda a questo riguardo RFC 7493[3], che definisce un sottoinsieme interoperabile di JSON e che include tra l'altro raccomandazioni su:

- unicode code points da evitare;
- quando serializzare numeri in formato di stringa;
- accortezze riguardo la gestione di chiavi duplicate.

Per casi d'uso specifici come gli header HTTP, sono di recente stati creati di recente formati di serializzazione appositi con delle librerie di processamento e serializzazione dedicate: si veda Structured Field Values for HTTP RFC 8941[4].

5.1.2 JWS - JSON Web Signature

JWS rappresenta il contenuto firmato utilizzando strutture dati JSON e codifica base64url.

La serializzazione compatta, la rappresentazione maggiormente utilizzata, è composta da tre parti:

- JWS Header, descrive il metodo di firma e i parametri utilizzati;

[2] Cf. https://tools.ietf.org/html/rfc8259
[3] Cf. https://tools.ietf.org/html/rfc7493
[4] Cf. https://tools.ietf.org/html/rfc8941

- JWS Payload, il contenuto del messaggio da proteggere;
- JWS Signature, garantisce l'integrità del JWS Header e del JWS Payload;

ed è rappresentata dalla concatenazione:

```
BASE64URL(UTF8(JWS Header)) ||'.' || BASE64URL(JWS Payload) || '.' || BASE64URL(JWS Signature)
```

Quando si firma un messaggio, si DEVONO prendere in considerazione una serie di possibili minacce, tra cui: - la contraffazione delle firme o l'alterazione del contenuto; - errati processi di validazione e verifica; - il riuso non autorizzato di messaggi firmati. Questo è particolarmente importante quando si utilizzano JWS nei processi di autenticazione o autorizzazione. JWS è definito dall'Internet Engineering Task Force nell'RFC 7515[5], a cui si rimanda per approfondimenti.

5.1.3 JWK - JSON Web Key

JWK definisce delle strutture dati per rappresentare una o più chiavi crittografiche associate a dei Json Web Algorithm, a supporto dei meccanismi di firma definiti in JWS o di cifratura definiti in JWE.

I tipi di chiavi supportate sono indicate nel JSON Object Signing and Encryption (JOSE) IANA Registry[6] che viene periodicamente aggiornato (eg. RFC 8037[7] ha aggiunto il supporto per l'algoritmo Ed25519).

JWK è definito dall'Internet Engineering Task Force nell'RFC 7517[8], a cui si rimanda per approfondimenti.

5.1.4 JWE - JSON Web Encryption

JWE rappresenta il contenuto crittografato utilizzando strutture dati JSON e codifica base64url.

[5] Cf. https://tools.ietf.org/html/rfc7515
[6] Cf. https://www.iana.org/assignments/jose/jose.xhtml
[7] Cf. https://tools.ietf.org/html/rfc8037
[8] Cf. https://tools.ietf.org/html/rfc7517

La serializzazione compatta, la rappresentazione maggiormente utilizzata, è composta da cinque parti:

- JWE Header, descrive il metodo di cifratura e i parametri utilizzati;
- JWE Encrypted Key, valore della chiave di crittografia del contenuto crittografato;
- JWE Initialization Vector, vettore di inizializzazione utilizzato durante la crittografia del testo;
- JWE Ciphertext, testo cifrato risultante dalla crittografia;
- JWE Authentication Tag, valore del tag di autenticazione risultante dalla crittografia autenticata del testo in chiaro;

ed è rappresentata dalla concatenazione:

```
BASE64URL(UTF8(JWE Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag)
```

JWE è definito dall'Internet Engineering Task Force nell'RFC 7516[9], a cui si rimanda per approfondimenti.

5.1.5 JWT - JSON Web Token

JWT veicola asserzioni da trasmettere (JWT Claims Set) utilizzando strutture JSON e codificando in base64url. I JWT sono firmati digitalmente e/o crittografati rispettivamente utilizzando JWS e JWE.

Il JOSE Header contiene le operazioni crittografiche applicate al JWT Claims Set:

- in un JWS, esso indica come è stato firmato il JWT Claims Set incluso nel JWS Payload;
- in un JWE, indica come è stato cifrato il JWT Claims Set incluso nel JWE Ciphertext.

Un JWT può anche prevede la possibilità di essere racchiuso in un'altra struttura JWE o JWS per creare un JWT annidato, consentendo l'esecuzione della firma e della crittografia annidate. JWT è definito dall'Internet Engineering Task Force nell'RFC 7519[10], a cui si rimanda per approfondimenti.

[9] Cf. https://tools.ietf.org/html/rfc7516
[10] Cf. https://tools.ietf.org/html/rfc7519

I JWT DEVONO essere usati rispettando le indicazioni di sicurezza indicate in RFC 8725[11].

5.1.6 JWA - JSON Web Algorithms

JWA individua gli algoritmi crittografici da utilizzare con le specifiche JWS e JWE.

JWA è definito dall'Internet Engineering Task Force nell'RFC 7518[12], a cui si rimanda per approfondimenti.

Le Linee Guida include, quale strumento operativo, l'allegato «Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST» in cui sono tabellati anche gli algoritmi crittografici individuati in JWA.

5.1.7 OAuth 2.0

OAuth 2.0 è un protocollo che consente alle applicazioni di accedere alle risorse protette di un servizio per conto di un soggetto e permette di proteggere risorse HTTP come un'API REST.

OAuth 2.0 prevede per ogni ruolo un compito ben definito, permettendo una più robusta sicurezza dell'architettura di autorizzazione.

- Resource Owner: è il proprietario dell'informazione esposta via HTTP.
- Client: è l'applicazione autorizzata dal Resource Owner che richiede l'accesso alla risorsa HTTP.
- Authorization Server: è il modulo che firma e rilascia i token di accesso.
- Resource Server: è il server che detiene l'informazione esposta via HTTP.

Un Grant Type è il processo da seguire per ottenere il cosiddetto Authorization Grant, ovvero la prova inoppugnabile che il Resource Owner ha autorizzato l'applicazione Client ad accedere ad una risorsa protetta. OAuth 2.0 definisce 4 Grant Type: Authorization Code Grant Type, Implicit Grant Type, Resource Owner Password Credentials Grant Type e Client Credentials Grant Type.

OAuth 2.0 è definito dall'Internet Engineering Task Force nell'RFC 6749[13], a cui si rimanda per approfondimenti.

[11] Cf. https://tools.ietf.org/html/rfc8725
[12] Cf. https://tools.ietf.org/html/rfc7518
[13] Cf. https://tools.ietf.org/html/rfc6749

Visto che il contesto di interesse è machine-to-machine, dei suddetti Grant Type sono applicabili il Resource Owner Password Credentials e il Client Credentials.

Il Grant Type Resource Owner Password Credentials comporta la cessione a terzi delle credenziali, quindi NON DEVE essere usato.

5.2 Tecnologia SOAP

Il Simple Object Access Protocol (SOAP) è un protocollo basato su XML che consente a due applicazioni di comunicare tra loro sul Web. Pubblicato come Working Draft dal W3C, SOAP definisce il formato dei messaggi che due applicazioni possono scambiarsi utilizzando i protocolli Internet, come ad esempio HTTP, per fornire dati e richiedere elaborazioni. Il protocollo è indipendente dalla piattaforma hardware e software ed è indipendente dal linguaggio di programmazione utilizzato per sviluppare le applicazioni comunicanti.

Nel contesto delle tecnologie SOAP, in relazione ai temi oggetto delle Linee Guida, si evidenziano le specifiche XML (eXtensible Markup Language), XML-canonicalization, XML-signature e WS-security per assicurare la sicurezza dei messaggi scambiati.

5.2.1 XML - eXtensible Markup Language

XML è un linguaggio di markup creato dal World Wide Web Consortium (W3C) per definire una sintassi per la codifica dei documenti che sia gli umani che le macchine potrebbero leggere. XML si fonda sull'uso di tag che definiscono la struttura del documento, nonché il modo in cui il documento deve essere memorizzato e trasportato.

XML è definito dal World Wide Web Consortium (W3C) nella raccomandazione Extensible Markup Language (XML) 1.0[14], a cui si rimanda per approfondimenti.

Come tutti i formati di interscambio general-purpose e che permettono l'utilizzo di strutture nidificate, in alcuni ambiti può essere opportuno limitare l'espressività della notazione (eg. limitando il numero di oggetti nidificati in fase di processamento o di serializzazione) tramite opportuni controlli. Si veda a riguardo OWASP XML Security Cheat Sheet[15].

[14] Cf. https://www.w3.org/TR/xml/
[15] Cf. https://cheatsheetseries.owasp.org/cheatsheets/XML_Security_Cheat_Sheet.html

5.2.2 XML-canonicalization

La canonicalizzazione è un metodo per generare una rappresentazione fisica, la forma canonica, di un documento XML che tiene conto delle modifiche sintattiche consentite dalla specifica XML. In altre parole, indipendentemente dalle modifiche che potrebbero essere apportate a un dato documento XML in trasmissione, la forma canonica sarà sempre identica, byte per byte. Questa sequenza di byte è fondamentale quando si firma un documento XML o si verifica la sua firma.

XML-canonicalization è definito dal World Wide Web Consortium (W3C) nella raccomandazione Canonical XML Version 1.1[16], a cui si rimanda per approfondimenti.

Le Linee Guida include, quale strumento operativo, l'allegato "Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST" in cui sono tabellati anche gli algoritmi di XML-canonicalization.

5.2.3 XML-signature

Lo standard XML-signature fornisce un insieme di tecniche per il calcolo della firma digitale specifiche per l'utilizzo di documenti XML. XML-signature definisce uno schema per la rappresentazione in formato XML del risultato di un'operazione di firma digitale. XML Signature è stato progettato tenendo in considerazione le caratteristiche peculiari del linguaggio XML e le modalità con cui i documenti XML vengono distribuiti e recuperati sulla rete Internet.

XML-signature è definito dal World Wide Web Consortium (W3C) nella raccomandazione XML Signature Syntax and Processing Version 1.1[17], a cui si rimanda per approfondimenti.

Le Linee Guida include, quale strumento operativo, l'allegato "Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST" in cui sono tabellati anche gli algoritmi di XML-canonicalization..

5.2.4 XML-encryption

Insieme a XML-signature, XML-encryption rappresenta la principale specifica nell'ambito della sicurezza XML. Lo standard consiste in una metodologia flessibile per la cifratura e per la rappresentazione dei dati cifrati in formato XML.

---

[16] Cf. https://www.w3.org/TR/xml-c14n11/
[17] Cf. https://www.w3.org/TR/xmldsig-core1/

XML-encryption è definito dal World Wide Web Consortium (W3C) nella raccomandazione XML Encryption Syntax and Processing Version 1.1[18], a cui si rimanda per approfondimenti.

Le Linee Guida include, quale strumento operativo, l'allegato "Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST" in cui sono tabellati anche gli algoritmi di XML-canonicalization.

5.2.5 WS-security

Web Services Security (WS-Security) è una suite di standard che descrivono i meccanismi per fornire la protezione dei messaggi SOAP attraverso l'integrità dei messaggi, la riservatezza dei messaggi e l'autenticazione di un singolo messaggio. WS-Security è uno standard a livello di messaggio basato sulla protezione dei messaggi SOAP tramite XML-signature, riservatezza tramite XML-encryption e propagazione delle credenziali tramite token di sicurezza. WS-Security descrive come codificare i token di sicurezza binari e allegarli ai messaggi SOAP, in particolare, le specifiche relative ai profili WS-Security descrivono come codificare i seguenti token:

- certificati X.509;
- asserzioni SAML.

La suite WS-security è definita dalla Organization for the Advancement of Structured Information Standards (OASIS) tra cui segnaliamo WS-Security SOAP Message Security 1.1[19] e i profili:

- X.509 Token Profile 1.1;
- SAML Token Profile 1.1.

[18] Cf. https://www.w3.org/TR/xmlenc-core1/
[19] Cf. http://docs.oasis-open.org/wss/v1.1/

Capitolo 6

Costituzione trust tra soggetti interessati

Le tecnologie da utilizzare indicate in precedenza fanno uso della crittografia asimmetrica.

Nel contesto della crittografia asimmetrica lo standard di riferimento è rappresentato dall'ITU-T X.509 che definisce il formato dei certificati a chiave pubblica (di seguito certificati digitali) e delle autorità di certificazione.

La fiducia delle interazioni erogatore-fruitore è assicurata dalla costituzione di un trust tra essi al fine di riconoscere la validità dei certificati digitali utilizzati per assicurare la sicurezza delle comunicazioni realizzate tramite API.

In quanto segue si individuano le tipologie e le caratteristiche dei certificati digitali per applicare le tecnologie indicate in precedenza e, non di meno, i possibili modelli di emissione e distribuzione degli stessi certificati raccomandati per la costituzione dei trust tra erogatori e fruitori.

[SIC_API_03] I soggetti destinatari DOVREBBERO utilizzare le tipologie dei certificati digitali e, per essi, assicurare il popolamento degli object identifier indicati al paragrafo Tipologia certificati digitali.

[SIC_API_04.a] I soggetti destinatari DOVREBBERO utilizzare le modalità di emissione e distribuzione dei certificati digitali indicati ai paragrafi Certificati digitali emessi da CAQ eIDAS e Certificati digitali emessi all'interno di domini di interoperabilità specifici.

[SIC_API_04.b] I soggetti destinatari DEVONO considerare i principi indicati al paragrafo Principi per la scelta delle modalità di emissione dei certificati digitali per la determinazione delle modalità di emissione e distribuzione dei certificati digitali.

6.1 Certificati digitali utilizzabili

Le tecnologie e gli standard indicate nei precedenti capitoli trovano fondamento sull'utilizzo di certificati digitali. In quanto segue si riportano le raccomandazioni in merito alla tipologia dei certificati digitali e gli object identifier che caratterizzano gli stessi. In quanto segue si applicano le linee guida "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate"[20], adottate con Determinazione AgID nr. 147/2019, e le raccomandazioni in merito agli elementi da prevedere nei certificati qualificati di sigillo elettronico e di autenticazione di siti Web[21], Avviso AgID nr. 18 del 15 aprile 2021.

6.1.1 Tipologia certificati digitali

La tipologia di certificati digitali (certificati qualificati o non qualificati) da utilizzare è determinata dal livello entro cui gli stessi sono utilizzati, nel dettaglio:

- per l'applicazione della sicurezza di canale si utilizzano Website Authentication Certificates, detti anche certificati TLS, che forniscono un metodo per autenticare i server e client coinvolti ed abilitano i meccanismi per crittografare le comunicazioni;
- per l'applicazione della sicurezza a livello applicativo si utilizzano Electronic Seal Certificates che identificano il soggetto giuridico a cui il sigillo è associato, abilitando la determinazione dell'origine, della correttezza e dell'integrità dei messaggi oggetto delle interazioni.

6.1.2 Object identifier per l'identificazione delle pubbliche amministrazioni

Usare certificati digitali per identificare le pubbliche amministrazioni, permette di automatizzare la verifica della persona giuridica a cui il certificato è associato.

Ricordando che la fonte autoritativa dell'elenco delle pubbliche amministrazioni è rappresentato dall'elenco di cui all'articolo 6-ter del CAD (di seguito IPA), in quanto segue sono riportate le raccomandazioni in merito al popolamento degli OID 2.5.4.97 organizationIdentifier

[20] Cf. https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche_e_raccomandazioni_v1.1_0.pdf

[21] Cf https://www.agid.gov.it/sites/default/files/repository_files/avviso_n.18_-_raccomandazioni_certificati_qseal_e_qwac.pdf

e OID 2.5.4.11 organizationalUnitName attraverso cui la controparte ricevente il certificato X.509 può effettuare il riscontro sui dati contenuti in IPA.

6.1.2.1 OID 2.5.4.97 organizationIdentifier

La pubblica amministrazione al momento della generazione del certificato X.509 assicura il popolamento dell'OID 2.5.4.97 organizationIdentifier nel rispetto della raccomandazione presente nelle "Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" in merito ai certificati digitali emessi per soggetti giuridici (legal person) e le raccomandazioni in merito agli elementi da prevedere nei certificati qualificati di sigillo elettronico e di autenticazione di siti Web.

Nello specifico le indicate raccomandazioni, coerentemente a quanto disposto dalla norma ETSI EN-319-412-1, prevedono che OID 2.5.4.97 organizationIdentifier DEVE essere popolato con il codice fiscale della persona giuridica a cui il certificato X.509 è associato nel rispetto della seguente sintassi:

- CF:IT - <codice_fiscale> dove <codice_fiscale> è il codice fiscale della persona giuridica

o in alternativa, per le sole pubbliche amministrazioni, con il codice IPA rispettando la seguente sintassi:

- PA:IT - <codice IPA dell'ente> dove <codice IPA dell'ente> è il codice IPA assegnato alla pubblica amministrazione nell'IPA.

6.1.2.2 OID 2.5.4.11 organizationalUnitName

Nel caso in cui il certificato X.509 sia riferito ad un'unità organizzativa o area organizzativa omogenea di una specifica pubblica amministrazione, cosi come registrato nell'IPA, la pubblica amministrazione al momento della generazione dello stesso certificato assicura, oltre a quanto indicato al paragrafo precedente, il popolamento dell'OID 2.5.4.11 organizationalUnitName, e nello specifico:

- nel caso di unità organizzativa, IPAIT - UO_<Codice_uni_uo> dove <Codice_uni_uo> è il codice univoco dell' unità organizzativa così come risulta dall'IPA;

- nel caso di area organizzativa omogenea, IPAIT - AOO_<Codice_uni_aoo> dove <Codice_uni_aoo> è codice univoco dell' area organizzativa omogenea così come risulta dall'IPA.

6.1.2.3 Verifica associazione di certificato X.509 ad una pubblica amministrazione

Il popolamento dei suddetti OID permette di verificare se la persona giuridica è una pubblica amministrazione oppure una unità organizzativa o area organizzativa omogenea di una specifica pubblica amministrazione.

La verifica è realizzata attraverso i seguenti passi:

1. consultazione dei dati dell'IPA in una delle modalità previste dalla piattaforma che implementa lo stesso IPA;
2. nel caso di certificato X.509 associato a una pubblica amministrazione verifica:
    a. la presenza nell'elenco delle amministrazioni dell'IPA del codice fiscale o in alternativa del codice IPA indicato nell'OID 2.5.4.97 organizationIdentifier;
3. nel caso di certificato X.509 associato a una unità organizzativa di una specifica pubblica amministrazione verifica:
    a. la presenza nell'elenco delle amministrazioni dell'IPA del codice fiscale o in alternativa del codice IPA indicato nell'OID 2.5.4.97 organizationIdentifier e recupera il codice IPA dell'amministrazione;
    b. la presenza nell'elenco delle unità organizzative dell'IPA del codice univoco dell'unità organizzativa indicato nell'OID 2.5.4.11 organizationalUnitName riferito all'amministrazione verificata al precedente passo 1;
4. nel caso di certificato X.509 associato a una area organizzativa omogenea di una specifica pubblica amministrazione verifica:
    a. la presenza nell'elenco delle amministrazioni dell'IPA del codice fiscale o in alternativa del codice IPA indicato nell'OID 2.5.4.97 organizationIdentifier e recupera il codice IPA dell'amministrazione;
    b. la presenza nell'elenco delle unità organizzative dell'IPA del codice univoco dell'area organizzativa omogenea indicato nell'OID 2.5.4.11 organizationalUnitName riferito all'amministrazione verificata al precedente passo 1.

6.2 Modalità di emissione e distribuzione dei certificati digitali

La costituzione del trust tra i soggetti erogatori e fruitori delle API, entro cui le parti riconoscono i certificati digitali, è il presupposto per realizzare uno scambio sicuro basato sulle API.

Di seguito si riportano le modalità per l'emissione di certificati digitali.

I soggetti che rendono disponibile API e/o utilizzano API nell'ambito di un dominio di interoperabilità, determinano i presupposti per abilitare l'accesso ai dati scambiati per il tramite delle API nel rispetto della normativa vigente ed in particolare il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 e il Decreto legislativo 30 giugno 2003 n. 196 e successive modificazioni e integrazioni.

6.2.1 Certificati digitali emessi da CAQ eIDAS

L'utilizzo di certificati qualificati emessi da Certification Authority qualificate ai sensi del Regolamento UE n° 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 (di seguito Regolamento eIDAS) rappresenta la modalità di emissione dei certificati nell'Unione europea con prefissati requisiti sicurezza e di interoperabilità.

In tale ipotesi le garanzie e le regole da adottare per l'utilizzo dei certificati qualificati emessi sono conformi alle disposizioni del Regolamento eIDAS.

Premesso che ai sensi del Regolamento eIDAS, vige il mutuo riconoscimento dei certificati qualificati:

[SIC_ API_05] Gli Erogatori DEVONO accettare i certificati qualificati emessi da una CAQ eIDAS per autenticare i Fruitori.

[SIC_ API_06] Gli Erogatori DEVONO verificare la validità dei certificati qualificati emessi da una CAQ, compresa l'eventuale revoca degli stessi. La frequenza di validazione viene stabilita dalle parti nel rispetto della normativa vigente e valutando gli impatti prestazionali e di sicurezza delle scelte.

6.2.2 Certificati digitali emessi all'interno di domini di interoperabilità specifici

Nell'ambito di un dominio di interoperabilità i soggetti afferenti, in alternativa a quanto indicato al precedente paragrafo, possono individuare tra essi uno o più soggetti abilitati all'emissione di certificati digitali (di seguito CA del dominio di interoperabilità).

La costituzione del trust è formalizza dalle regole del dominio di interoperabilità in cui sono definite:

- Il dettaglio implementativo dei processi di quanto indicato ai successivi paragrafi Gestione dell'emissione dei certificati digitali, Gestione della revoca dei certificati digitali e Gestione della distribuzione dei certificati digitali della CA;
- Le modalità con cui i soggetti afferenti al dominio di interoperabilità (di seguito soggetto richiedente) inoltrano alla CA del dominio di interoperabilità la richiesta di emissione di un certificato;
- Le verifiche in carico alla CA del dominio di interoperabilità per dare seguito all'identificazione del soggetto richiedente l'emissione di un certificato digitale.

[SIC_ API_07] Gli Erogatori DEVONO accettare i certificati digitali emessi da una CA del dominio di interoperabilità per autenticare gli altri soggetti utilizzatori delle stesse API..

[SIC_ API_08] Gli Erogatori DEVONO verificare la validità dei certificati digitali emessi da una CA del dominio di interoperabilità, compresa l'eventuale revoca degli stessi. La frequenza di validazione viene stabilita dalle parti nel rispetto della normativa vigente e valutando gli impatti prestazionali e di sicurezza delle scelte.

6.2.2.1 Gestione dell'emissione dei certificati digitali

Il processo di emissione di certificati digitali da parte di una CA del dominio di interoperabilità è caratterizzato dai seguenti passi:

1. Il soggetto richiedente provvede, in autonomia, alla generazione di una coppia di chiavi asimmetriche nel rispetto delle regole definite nel dominio di interoperabilità;

2. Il soggetto richiedente inoltra nei modi definiti nelle regole del dominio di interoperabilità alla CA del dominio di interoperabilità la richiesta di certificazione CSR, in formato PKCS#10;
3. La CA del dominio di interoperabilità identifica il soggetto richiedente e, in caso positivo, provvede a generare il certificato e a fornirlo al soggetto richiedente.

6.2.2.2 Gestione della revoca dei certificati digitali

La CA del dominio di interoperabilità assicura la disponibilità dei necessari servizi per permettere ai soggetti afferenti ad un dominio di interoperabilità di verificare l'eventuale revoca di certificati digitali emessi.

A tal fine si DOVREBBE utilizzare le Online Certificate Status Protocol (OCSP) RFC 6960[22] o la Certificate Revocation List (CRL) RFC 5280[23] con i relativi aggiornamenti.

6.2.2.3 Gestione della distribuzione dei certificati digitali della CA

La CA del dominio di interoperabilità, nelle modalità indicate nelle regole del dominio di interoperabilità, inoltra al soggetto richiedente il certificato firmato e/o assicura la distribuzione dei certificati digitali emessi ai soggetti afferenti al dominio di interoperabilità.

6.2.3 Principi per la scelta delle modalità di emissione dei certificati digitali

La scelta della modalità di emissione dei certificati digitali, tra quelle indicate in precedenza, è nella responsabilità dei soggetti afferenti ad un dominio di interoperabilità.

I soggetti afferenti ad un dominio di interoperabilità individuano la modalità di emissione dei certificati digitali nel rispetto principi indicati di seguito.

[SIC_ API_09] Economicità, efficacia ed efficienza della modalità individuata, e nello specifico di quanto indicato in precedenza comparando i costi di emissione dei certificati digitali dovuti alle CAQ, nel caso indicato al paragrafo Certificati digitali emessi da CAQ eIDAS, e i costi per la gestione dei processi e delle infrastrutture per la loro implementazione indicati al paragrafo Certificati digitali emessi all'interno di domini di interoperabilità specifici.

[22] Cf. https://tools.ietf.org/html/rfc6960
[23] Cf. https://tools.ietf.org/html/rfc5280

[SIC_ API_10] Nell'ipotesi in cui i dati scambiati per il tramite delle API hanno effetti su soggetti esterni al dominio di interoperabilità (ad esempio servizi per l'emissione di certificazione utilizzati in contesti privati da cittadini e imprese) o siano oggetto dell'interoperabilità transfrontaliera con altri stati delle CE, si DEVE utilizzare la modalità indicata al paragrafo Certificati digitali emessi da CAQ eIDAS per assicurare l'accettazione dei certificati digitali emessi.