Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST

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

Nel presente allegato sono riportate gli algoritmi per XML Canonicalizzazione e per Digest and signature public key relativamente alle tecnologie SOAP e REST raccomandati dal modello di interoperabilità delle pubbliche amministrazioni.

Capitolo 1

Ambito di applicazione

1.1 Soggetti destinatari

L'Allegato è destinato 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.

L'Allegato è rivolto 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 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)

2.3 Termini e definizioni

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

[AgID] Agenzia per l'Italia Digitale

Capitolo 3

XML Canonicalization

SIGLA	URI
Canonical XML 1.0	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Canonical XML 1.1	http://www.w3.org/2006/12/xml-c14n11
Exclusive XML Canonicalization 1.0	Exclusive XML Canonicalization 1.0

Capitolo 4

Digest SOAP

SIGLA	URI
SHA-256	http://www.w3.org/2001/04/xmlenc#sha256
SHA-384	http://www.w3.org/2001/04/xmldsig-more#sha384
SHA-512	http://www.w3.org/2001/04/xmlenc#sha512
HMAC-SHA-256	http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
HMAC-SHA-384	http://www.w3.org/2001/04/xmldsig-more#hmac-sha384
HMAC-SHA-512	http://www.w3.org/2001/04/xmldsig-more#hmac-sha512

Capitolo 5

Signature public key SOAP

SIGLA	URI
DSA-SHA-256	http://www.w3.org/2009/xmldsig11#dsa-sha256
RSA-SHA-256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
RSA-SHA-384	http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
RSA-SHA-512	http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
ECDSA-SHA-256	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
ECDSA-SHA-384	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384
ECDSA-SHA-512	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512

Capitolo 6

Digest and signature public key REST

SIGLA	DETAILS
HS256	HMAC using SHA-256 hash algorithm
HS384	HMAC using SHA-384 hash algorithm
HS512	HMAC using SHA-512 hash algorithm
RS256	RSA using SHA-256 hash algorithm
RS384	RSA using SHA-384 hash algorithm
RS512	RSA using SHA-512 hash algorithm
ES256	ECDSA using P-256 curve and SHA-256 hash algorithm
ES384	ECDSA using P-384 curve and SHA-384 hash algorithm
ES512	ECDSA using P-521 curve and SHA-512 hash algorithm

Capitolo 7

Digest REST

SIGLA	DETAILS
S256	SHA-256 hash algorithm
S384	SHA-384 hash algorithm
S512	SHA-512 hash algorithm