AGID | Agenzia per l'Italia Digitale

Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate

AGID

13 feb 2020

Indice dei contenuti

Nota: Linee guida contenenti regole tecniche ex art. 71 del CAD

CAPITOLO 1

Definizioni

Ai fini del presente regolamento, oltre ad applicarsi le definizioni di cui all'articolo 1 del CAD, si intende per:

- **Agenzia**: l'Agenzia per l'Italia Digitale;
- **CAD**: D.Lgs. 7 marzo 2005 №82[1], *Codice dell'Amministrazione Digitale*, e successive modificazioni;
- **servizi**: i servizi di cui all'art.29 comma 1 del CAD;
- **regolamento eIDAS**: Regolamento (UE) №910/2014[2] 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;
- **QTSP**: prestatore di servizi fiduciari qualificati ai sensi del regolamento eIDAS.

[1] https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2018-09-28/
[2] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32014R0910

CAPITOLO 2

Scopo e ambito di applicazione

Il *regolamento eIDAS* (pagina 3) dispone alcuni obblighi in capo ai *QTSP* (pagina 3) che emettono certificati qualificati per la generazione di firme e sigilli, individua i requisiti per la convalida delle firme elettroniche qualificate (art. 32) e *mutatis mutandis*, dei sigilli elettronici qualificati (art. 40), come anche i requisiti per la validazione temporale elettronica qualificata (art. 42).

Tali disposizioni individuano dei requisiti minimi che possono risultare non adeguati per la fruizione di servizi in rete offerti nello specifico contesto italiano. Un esempio in tal senso è l'assenza dell'obbligo di indicare nel certificato qualificato per la generazione della firma il codice fiscale del titolare, elemento indispensabile per diverse pubbliche amministrazioni italiane.

Pertanto, il presente provvedimento, emanato ai sensi dell'articolo 71 del CAD, contiene nel *paragrafo 3* (pagina 7) (Obblighi) alcune previsioni rese obbligatorie in forza o in attuazione del regolamento eIDAS, mentre nel *paragrafo 4* (pagina 9) (Raccomandazioni) indicazioni volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete nel contesto italiano. Sebbene indicate come "raccomandazioni" devono essere interpretate nel significato previsto nella **RFC 2119**[3], pertanto la loro applicazione è fortemente consigliata. È evidente che trattandosi di raccomandazioni e non di obblighi, la loro disapplicazione non possa comportare l'invalidità di firme o sigilli elettronici qualificati. Il *paragrafo 5* (pagina 13) contiene alcune indicazioni per il processo di convalida di firme e sigilli elettronici.

Le disposizioni contenute nelle presenti regole tecniche che risultino in contrasto con future versioni del *regolamento eIDAS* (pagina 3) o dei regolamenti esecutivi derivanti, devono essere disapplicate.

[3] https://tools.ietf.org/html/rfc2119.html

CAPITOLO 3

Obblighi

3.1 Articolo 24, paragrafo 2, lettera *e* del regolamento eIDAS

Nell'ambito dei servizi fiduciari qualificati volti all'emissione di certificati qualificati e ai sistemi di validazione temporale elettronica qualificata, i prestatori di servizi fiduciari qualificati sono liberi di utilizzare le funzioni di *hash* e gli algoritmi crittografici con lunghezza delle chiavi purché adeguati al fine di ottemperare a quanto prescritto dall'articolo 24, paragrafo 2, lettera *e* del *regolamento eIDAS* (pagina 3).

Ai fini dell'articolo 21, paragrafo 2, e dell'articolo 24, paragrafo 2, lettera *a* del *regolamento eIDAS* (pagina 3), detti prestatori di servizi devono informare l'*Agenzia* (pagina 3) in merito alla scelta effettuata e di come soddisfi quanto prescritto dall'articolo 24, paragrafo 2, lettera *e* del *regolamento eIDAS* (pagina 3).

3.2 Articolo 24, paragrafo 2, lettera *d* del regolamento eIDAS

Ai sensi dell'art. 24, paragrafo 2, lettera *d* del *regolamento eIDAS* (pagina 3), i destinatari dei servizi devono essere informati in modo chiaro e completo anche in merito all'applicazione o eventuale disapplicazione delle raccomandazioni di cui al successivo *paragrafo 4* (pagina 9) e delle possibili conseguenze.

CAPITOLO 4

Raccomandazioni

I QTSP che si impegnano a fornire – salvo diversa richiesta degli interessati - i servizi oggetto del presente regolamento applicando le raccomandazioni di cui al paragrafo 4, lo comunicano all'Agenzia, che pubblica tali informazioni sul proprio sito web istituzionale.

4.1 Profilo dei certificati qualificati

Per la generazione dei certificati qualificati, sono indicate le seguenti raccomandazioni:

1. Conformità con quanto stabilito nella specifica **RFC 5280**[4] e nelle norme ETSI EN 319-412-1[5] versione 1.1.1, EN 319-412-2[6] versione 2.1.1, EN 319-412-3[7] versione 1.1.1, EN 319-412-4[8] versione 1.1.1 e EN 319-412-2[9] versione 2.1.1.
2. L'estensione `KeyUsage` è presente e marcata *critica*. Il solo `KeyUsage` ammesso per i certificati qualificati di firma elettronica è il "*Type A*," come descritto nella citata norma ETSI EN 319-412-2[10].
3. Al fine di ottemperare a quanto prescritto negli allegati I (lettera *h*), III (lettera *h*) e IV (lettera *i*) del *regolamento eIDAS* (pagina 3), è utilizzato l'`accessMethod` `id-ad-caIssuers`, con `accessLocation` `uniformResourceIdentifier`.
4. L'estensione `authorityKeyIdentifier` (2.5.29.35[11]) contiene almeno il campo `keyIdentifier`, *non* marcata critica.
5. Il campo `SubjectDN` (dati identificativi del titolare) è caratterizzato da:
    a. Il `serialNumber` (2.5.4.5[12]) - nei certificati di firma elettronica e autenticazione di siti web rilasciati a persone fisiche - contiene il codice fiscale del titolare indicato con il prefisso `TIN`, come prescritto dalla norma ETSI EN 319-412-1[13] (es. `TINIT-CCCNNN64T30H501H`). Esclusivamente nel caso in cui al titolare non sia stato assegnato un codice fiscale dall'autorità italiana è possibile indicare analogo numero di identificazione fiscale rilasciato da altra autorità dell'Unione utilizzando

[4] https://tools.ietf.org/html/rfc5280.html
[5] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[6] http://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.01.01_60/en_31941202v020101p.pdf
[7] http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf
[8] http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf
[9] http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.01.01_60/en_31941205v020101p.pdf
[10] http://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.01.01_60/en_31941202v020101p.pdf
[11] http://oid-info.com/get/2.5.29.35
[12] http://oid-info.com/get/2.5.4.5
[13] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf

il prefisso `TIN` ovvero gli estremi di un documento di riconoscimento utilizzando i prefissi `IDC` o `PAS` ovvero un numero di registrazione nazionale utilizzando il prefisso `PNO`, come prescritto dalla norma EN 319-412-1[14]. Nel caso in cui il titolare sia una persona fisica non dotata di codice fiscale o carta di identità italiana, ma dotata di permesso di soggiorno, si applica quanto previsto dal punto 6 del paragrafo 5.1.3 della norma EN 319-412-1[15] utilizzando il prefisso `RP`. Nei casi in cui la legge dello Stato di residenza della persona fisica non consenta l'utilizzo di nessuno dei precedenti codici, si applica quanto previsto dal punto 6 del paragrafo 5.1.3 della norma EN 319-412-1[16] utilizzando il prefisso `NS` per identificare lo schema nazionale. In tale evenienza, il pre- statore di servizi fiduciari deve inserire un codice univoco, eventualmente derivato da uno dei predetti.

b. L'`organizationName` (2.5.4.10[17]) dei certificati di firma elettronica, eventual- mente utilizzato per indicare l'appartenenza o l'affiliazione del titolare all'organiz- zazione e esclusivamente nel caso in cui il prestatore di servizi fiduciari abbia avuto e conservi prova della volontà dell'organizzazione medesima a tale uso e che la stessa si assuma l'obbligo di richiedere la revoca del certificato nel caso in cui il titolare del certificato lasci l'organizzazione. Nel caso in cui l'`organizationName` sia presente, i medesimi vincoli si applicano anche all'eventuale codifica dell'attributo `title`. L'attributo `title`, se presente, contiene il ruolo del titolare in linguaggio naturale e, facoltativamente, una seconda parte costituita da un codice numerico derivato dai codici delle professioni pubblicati da ISTAT. Nel caso in cui sia presente, il codice ISTAT della professione è preceduto dalla stringa `::` (esadecimale 0x3A3A, e `title=descrizioneInLinguaggioNaturale::codiceNumerico`). L'`organizationName` non è utilizzato nel caso in cui il titolare sia un semplice cliente dell'organizzazione.

c. Il `dnQualifier` (2.5.4.46[18]) che contiene il codice identificativo del titolare presso il prestatore del servizio. Tale codice è univoco nell'ambito del prestatore del servizio.

d. La possibilità di inserire nell'attributo `description` (2.5.4.13[19]) il codice EORI (*Economic Operator Registration and Identification*) di cui al Regolamento (UE) №312/2009 del 16 aprile 2009 e successive modificazioni. In tal caso il codice stesso è preceduto dal testo `EORI` e dal carattere "`:`" (esadecimale 0x3A).

6. Al fine di normalizzare l'uso della sintassi dall'identificatore '*legal person semantics identifier*' descritto nel paragrafo 5.1.4 della norma ETSI EN 319-412-1[20], nel caso di organizzazioni non dotate né di partita IVA né di NTR, ma solamente del codice fiscale, è possibile utilizzare la modalità descritta al numero 3 del paragrafo 5.1.4, utilizzando i due caratteri "`CF`" (esempio: `CF:IT-97735020584`).

7. Salvo quanto disposto nelle citate norme ETSI, eventuali ulteriori limiti d'uso sono inseriti nell'attributo `explicitText` del campo `userNotice` dell'estensione `certificatePolicies`. Sul sito istituzionale dell'Agenzia sono pubblicati i testi e le codifiche delle limitazioni d'uso che è auspicabile siano garantite agli utenti.

8. È fortemente sconsigliato l'utilizzo dei caratteri *wildcard* come `*` (esadecimale 0x2A) in tutti i nomi di dominio nei certificati qualificati di autenticazione di siti web.

9. Ulteriori estensioni possono essere inserite nel certificato purché conformi agli standard citati nel presente provvedimento e *non* marcate critiche.

4.2 Profilo dei certificati di certificazione e validazione temporale

1. Il profilo dei certificati di certificazione è conforme alla specifica **RFC 5280**[21].

2. Il profilo dei certificati di marcatura temporale è conforme alla norma ETSI EN 319-422[22] versione 1.1.1.

[14] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[15] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[16] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[17] http://oid-info.com/get/2.5.4.10
[18] http://oid-info.com/get/2.5.4.46
[19] http://oid-info.com/get/2.5.4.13
[20] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[21] https://tools.ietf.org/html/rfc5280.html
[22] http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

3. Per la codifica dei certificati deve essere utilizzato il formato ASN.1 – DER (ISO/IEC 8824, 8825) in rappresentazione binaria o alfanumerica, ottenuta applicando la trasformazione *Base64* (**RFC 1421**[23] e successive modifiche); l'intestazione e la coda previsti in RFC 1421 possono essere assenti. Nel primo caso il file contenente il certificato deve assumere l'estensione `cer` o `der`, nel secondo caso `b64`.
4. I certificati di certificazione contengono le seguenti estensioni:
   a. `keyUsage` (2.5.29.15[24]) — contenente i valori `keyCertSign` e `CRLSign` (bit #5 e #6 impostati a `1`); l'estensione è marcata *critica*;
   b. `basicConstraints` (2.5.29.19[25]) — contenente il valore `CA=true`; l'estensione è marcata *critica*;
   c. `certificatePolicies` (2.5.29.32[26]) — contenente uno o più identificativi delle `PolicyIdentifier:code e le URL dei relativi CPS. Può contenere l'OID geerico previsto dall'\ :RFC:`5280` (2.5.29.32.0[27])); l'estensione *non* è marcata critica;
   d. `subjectKeyIdentifier` (2.5.29.14[28]) — contenente il valore `keyIdentifier` per identificare il certificato l'estensione *non* è marcata critica;
   e. Ulteriori estensioni possono essere inserite nel certificato purché conformi agli standard citati nel presente provvedimento e *non* marcate critiche.
5. I certificati di marcatura temporale contengono le seguenti estensioni:
   a. `keyUsage` (2.5.29.15[29]) — contenente il valore `digitalSignature` (bit #0 impostato a `1`); l'estensione è marcata *critica*;
   b. `extendedKeyUsage` (2.5.29.37[30]) — contenente esclusivamente il campo `keyPurposeId` impostato su `timeStamping`; l'estensione è marcata *critica*;
   c. `certificatePolicies` (2.5.29.32[31]) — contenente uno o più identificativi delle `PolicyIdentifier` e le URL del relativo CPS; l'estensione *non* è marcata critica;
   d. `authorityKeyIdentifier` (2.5.29.35[32]) — contenente almeno il valore `keyIdentifier` corrispondente al :code:‘subjectKeyIdentifier: del certificato di certificazione utilizzato per sottoscrivere il certificato di marcatura temporale; l'estensione *non* è marcata critica;
   e. `subjectKeyIdentifier` (2.5.29.14[33]) — contenente il valore `keyIdentifier` per identificare il certificato; l'estensione *non* è marcata critica;
   f. Ulteriori estensioni possono essere inserite nel certificato purché conformi agli standard citati nel presente provvedimento e *non* marcate critiche.

4.3 Formati di firme e sigilli elettronici qualificati

Nella realizzazione di servizi e applicazioni per la generazione di firme e sigilli elettronici qualificati, i prestatori di servizi fiduciari qualificati si attengono alle disposizioni emanate con la Decisione di Esecuzione (UE) № 1506/2015[34] dell'8 settembre 2015 e successive modificazioni.

[23] https://tools.ietf.org/html/rfc1421.html
[24] http://oid-info.com/get/2.5.29.15
[25] http://oid-info.com/get/2.5.29.19
[26] http://oid-info.com/get/2.5.29.32
[27] http://oid-info.com/get/2.5.29.32.0
[28] http://oid-info.com/get/2.5.29.14
[29] http://oid-info.com/get/2.5.29.15
[30] http://oid-info.com/get/2.5.29.37
[31] http://oid-info.com/get/2.5.29.32
[32] http://oid-info.com/get/2.5.29.35
[33] http://oid-info.com/get/2.5.29.14
[34] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32015D1506

4.4 Informazioni sullo stato dei certificati qualificati di firma e sigillo

Le informazioni afferenti lo stato del certificato preferibilmente sono rese disponibili attraverso il servizio OCSP ed eventualmente anche tramite liste di revoca (CRL). A tal fine i certificati qualificati contengono l'estensione `authorityInfoAccess` (1.3.6.1.5.5.7.1.1[35]) contenente il campo `accessDescription` con l'attributo `accessMethod`, che contiene l'identificativo `id-ad-ocsp` (1.3.6.1.5.5.7.48.1[36]) e l'attributo `accessLocation`, che contiene l'URI che punta all'*OCSP Responder* e, eventualmente, l'estensione `CRLDistributionPoints` (2.5.29.31[37]). Le estensioni *non* sono marcate critiche.

Le CRL contengono l'estensione `ExpiredCertsOnCRL` (2.5.29.60[38]), prevista dallo standard X.509.

Le informazioni sulla revoca e sospensione dei certificati sono liberamente accessibili in rete.

[35] http://oid-info.com/get/1.3.6.1.5.5.7.1.1
[36] http://oid-info.com/get/1.3.6.1.5.5.7.48.1
[37] http://oid-info.com/get/2.5.29.31
[38] http://oid-info.com/get/2.5.29.60

CAPITOLO 5

Convalida di firme e sigilli elettronici qualificati

1. Il processo di convalida di una firma elettronica qualificata o di un sigillo elettronico qualificato conferma la validità delle stesse purché siano verificate le condizioni di cui all'articolo 32 del *regolamento eIDAS* (pagina 3) e siano generate conformemente a quanto stabilito negli atti di esecuzione emanati dalla Commissione Europea ai sensi del *paragrafo 5* (pagina 13) degli articoli 27 o 37 del *regolamento eIDAS* (pagina 3).
2. Si raccomanda che il processo di convalida della validazione temporale sia in grado di effettuare la verifica delle marche detached e dei formati **RFC 5544**[39].

[39] https://tools.ietf.org/html/rfc5544.html

CAPITOLO 6

Norme transitorie e abrogazioni

1. Salvo quanto disposto al successivo comma 2, la Deliberazione CNIPA №45 del 21 maggio 2009 è abrogata e sostituita dal presente regolamento.
2. Le presenti regole tecniche sono adottate dai prestatori di servizi fiduciari entro 30 giorni dalla data di pubblicazione della notizia della loro emanazione sulla *Gazzetta Ufficiale della Repubblica Italiana*.
3. Fino all'adozione delle presenti regole tecniche nei termini stabiliti dal precedente comma 2, i prestatori di servizi fiduciari qualificati continuano ad applicare le regole tecniche di cui alla Deliberazione №45/2009.
4. Le presenti regole tecniche non producono alcun effetto sui certificati emessi prima della loro adozione.

Indice

R