Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

REGOLAMENTO

Regole e raccomandazioni afferenti la generazione di certificati qualificati, firme e sigilli elettronici qualificati e validazione temporale elettronica qualificata.

1. Definizioni

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

a) Agenzia: l'Agenzia per l'Italia Digitale;

b) CAD: il D.lgs. 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale" e successive modificazioni;

c) servizi: i servizi di cui all'art.29 comma 1 del CAD;

d) regolamento eIDAS: il Regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

e) QTSP: prestatore di servizi fiduciari qualificati ai sensi del regolamento eIDAS.

2. Scopo e ambito di applicazione

Il regolamento eIDAS dispone alcuni obblighi in capo ai QTSP 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. Un esempio 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.

Pertanto, il presente provvedimento contiene nel paragrafo 3 (Obblighi) alcune previsioni rese obbligatorie in forza o in attuazione del regolamento eIDAS, mentre nel paragrafo 4 (Raccomandazioni) indicazioni volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete. Sebbene indicate come "raccomandazioni" devono essere interpretate nel significato previsto nella RFC 2119, 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.

3. Obblighi

3.1 Lunghezza delle chiavi crittografiche

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 utilizzano funzioni di hash e algoritmi crittografici con lunghezza delle chiavi ritenuti sufficientemente robusti allo stato della tecnologia. I prestatori di servizi fiduciari informano l'Agenzia circa le scelte effettuate allegando un'analisi di sicurezza volta a dimostrare la robustezza della scelta effettuata. Utilizzando la funzione di hash SHA-256, gli algoritmi RSA (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 2048 bit e ECDSA (Elliptic Curve Digital Signature Algorithm) con lunghezza chiave non inferiore a 224 bit, sono ritenuti essere sufficientemente robusti fino al 2021, pertanto non è richiesta la consegna della copia dell'analisi di sicurezza.

3.2 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) 2015/1506 della Commissione dell'8 settembre 2015.

3.3 Formato dei certificati qualificati

I prestatori di servizi fiduciari che emettono certificati qualificati applicano quanto disposto dal Regolamento eIDAS.

3.4 Informazioni sullo stato dei certificati qualificati di firma e sigillo

I prestatori dei servizi fiduciari qualificati rendono disponibili le informazioni afferenti lo stato del certificato attraverso il servizio OCSP ed eventualmente anche tramite CRL. A tal fine i certificati qualificati contengono l'estensione *authorityInfoAccess* (OID: 1.3.6.1.5.5.7.1.1) contenente il campo *accessDescription* con l'attributo *accessMethod,* che contiene l'identificativo *id-ad-ocsp* (OID: 1.3.6.1.5.5.7.48.1) e l'attributo *accessLocation*, che contiene l'URI che punta all'OCSP *Responder* e, eventualmente, l'estensione *CRLDistributionPoints* (OID: 2.5.29.31). Le estensioni non sono marcate critiche.

I certificati revocati o sospesi devono permanere nelle eventuali CRL, anche dopo la loro naturale scadenza, fino alla scadenza del relativo certificato di certificazione.

Le eventuali liste di revoca (CRL) contengono l'estensione *ExpiredCertsOnCRL* (OID 2.5.29.60), prevista dallo standard X.509.

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

3.5 Obbligo informativo

Le eventuali raccomandazioni di cui al paragrafo 4 che i prestatori di servizi fiduciari qualificati adottano devono essere descritte nei rispettivi CPS affinché tutte le parti interessate ne siano al corrente. I prestatori di servizi fiduciari qualificati che intendono fornire un servizio oggetto del presente provvedimento disapplicando le raccomandazioni di cui al paragrafo 4, informano preventivamente in modo compiuto e chiaro i soggetti cui offrono tali servizi in merito alle possibili conseguenze derivanti dalla disapplicazione di dette raccomandazioni ponendo particolare enfasi alle possibili problematiche in termini di fruizione dei servizi offerti dalle pubbliche amministrazioni.

4. Raccomandazioni

4.1 Profilo dei certificati qualificati firme e sigilli elettronici qualificati

Per la generazione dei certificati qualificati per firme e sigilli elettronici, sono indicate le seguenti raccomandazioni:

1. Conformità con quanto stabilito nella specifica RFC 5280 e nelle norme ETSI EN 319412-1 v1.1.1, EN 319412-2 v2.1.1, EN 319412-3 v1.1.1, EN 319412-4 v1.1.1 e EN 319412-5 v2.1.1.

2. L'estensione *KeyUsage* è presente e marcata critica. Il solo key usage ammesso è il *Type A*, come descritto nella citata norma ETSI EN 319412-2.

3. Al fine di ottemperare a quanto prescritto negli allegati I (lettera h), III (lettera h) e IV (lettera i) del Regolamento eIDAS, è utilizzato l'*accessMethod id-ad-caIssuers*, con *accessLocation uniformResourceIdentifier* via HTTP o FTP.

4. L'estensione *authorityKeyIdentifier* (OID:2.5.29.35) contiene almeno il campo *keyIdentifier*, non marcata critica.
5. Il campo *SubjectDN* (Dati identificativi del titolare) è caratterizzato da:

   a) il *serialNumber* (OID: 2.5.4.5) contiene il codice fiscale del titolare indicato con il prefisso TIN, come prescritto dalla norma EN 319412-1 (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 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 319412-1. 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 319412-1 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 319412-1 utilizzando il prefisso "NS" per identificare lo schema nazionale. In tale evenienza, il prestatore di servizi fiduciari deve inserire un codice univoco, eventualmente derivato da uno dei predetti;
   b) l'*organizationName*, eventualmente utilizzato per indicare l'appartenenza o l'affiliazione del titolare all'organizzazione 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'*organizationName* non è utilizzato nel caso in cui il titolare sia un semplice cliente dell'organizzazione;
   c) il *dnQualifier* (OID: 2.5.4.46) 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* (OID: 2.5.4.13) il codice E.O.R.I. (Economic Operator Registration and Identification) di cui al Regolamento (CE) N. 312/2009 del 16 aprile 2009. In tal caso, il codice stesso è preceduto dal testo "EORI" e dal carattere ":" (in notazione esadecimale "0x3A");

6. Al fine di normalizzare l'uso del Legal person semantics identifier previsto nel paragrafo 5.1.4 della norma ETSI EN 319412-1, 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. La piena applicazione delle raccomandazioni oggetto del presente provvedimento è dichiarata attraverso la codifica nel campo CertificatePolicies del certificato qualificato del seguente elemento: *PolicyIdentifier object identifier* (OID) 1.3.76.16.4;
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;
2. Il profilo dei certificati di marcatura temporale è conforme alla norma ETSI EN 319422 v1.1.1;
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 BASE 64 (RFC 1421 e successive modifiche). La testata e la coda previsti in RFC 1421 possono essere assenti. Nel primo caso il file contenente il certificato deve assumere l'estensione *der* o *cer*, nel secondo caso *b64*.
4. I certificati di certificazione contengono le seguenti estensioni:

   a) *keyUsage* (OID 2.5.29.15) – contenente i valori *keyCertSign* e *cRLSign* (bit 5 e 6 impostati a 1). L'estensione è marcata critica;

   b) *basicConstraints* (OID 2.5.29.19) - contenente il valore CA=*true*. L'estensione è marcata critica;

   c) *certificatePolicies* (OID 2.5.29.32) - contenente uno o più identificativi delle *policyIdentifier* e le URL dei relativi CPS. Può contenere l'OID generico previsto dall'RFC 5280 (2.5.29.32.0). L'estensione non è marcata critica;

   d) *subjectKeyIdentifier* (OID 2.5.29.14) - 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* (OID 2.5.29.15) – contenente il valore *digitalSignature* (bit 0 impostato a 1). L'estensione è marcata critica;

   b) *extendedKeyUsage* (OID 2.5.29.37) – contenente esclusivamente il campo

keyPurposeId=timeStamping. L'estensione è marcata critica;

c) *certificatePolicies* OID 2.5.29.32) – contenente uno o più identificativi delle *policyIdentifier* e le URL del relativo CPS. L'estensione non è marcata critica;

d) *authorityKeyIdentifier* (OID 2.5.29.35) – contenente almeno il valore *keyIdentifier* corrispondente al subjectKeyIdentifier del certificato di certificazione utilizzato per sottoscrivere il certificato di marcatura temporale. L'estensione non è marcata critica;

e) *subjectKeyIdentifier* (OID 2.5.29.14) – contiene 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 Processi di convalida

I

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'art. 32 del Regolamento eIDAS e siano generate conformemente a quanto stabilito negli atti di esecuzione emanati dalla Commissione europea ai sensi del paragrafo 5 degli articoli 27 o 37 del Regolamento eIDAS.
2. Si raccomanda che il processo di convalida della validazione temporale sia in grado di effettuare la verifica delle marche *detached* anche nei formati RFC 5544.

5. Disposizioni finali

1. Il presente regolamento abroga la deliberazione CNIPA n 45 del 21 maggio 2009
2. I prestatori di servizi fiduciari qualificati che forniscono servizi qualificati oggetto del presente regolamento si adeguano alle disposizioni ivi contenute entro trenta giorni dalla data di emanazione.