AVVISI SERVIZI FIDUCIARI QUALIFICATI

Si ricorda agli utilizzatori che per generare firme conformi alla normativa vigente è necessario mantenere aggiornate le applicazioni di firma digitale/firma elettronica qualificata.
Si sottolinea l'importanza di usare applicazioni di verifica delle firme digitali e qualificate sempre aggiornate, in caso contrario firme digitali/firme elettroniche qualificate perfettamente valide potranno risultare non valide con conseguenze di natura non solo economica.

Pertanto, si suggerisce ai soggetti che ricevono e verificano documenti sottoscritti con firma digitale o firma elettronica qualificata di accertarsi che l'applicazione in uso sia aggiornata prima di ritenere non valida una sottoscrizione elettronica.

In caso di dubbio, si suggerisce di ripetere la verifica con la soluzione resa disponibile dalla Commissione europea che garantisce di poter verificare firme elettroniche qualificate basate su certificati rilasciati in altri Stati membri dell'Unione e/o con le applicazioni indicate nella apposita sezione di questo sito.

****

Avviso n. 16 – Servizio fiduciario qualificato per emissione certificati qualificati di autenticazione di siti web

Premesso che il Regolamento 910/2014 (eIDAS) entrato in vigore dal 01 luglio 2016, alla Sezione 8 dell'articolo 45 norma i requisiti per i certificati qualificati di autenticazione di siti web.

Considerato che il DPCM 22 febbraio 2013 è stato emanato prima del citato regolamento UE.

Viste il lavoro di standardizzazione svolto dall'organizzazione non governativa internazionale World Wide Web Consortium (W3C).

Ritenuto che la disposizione contenuta nell'art 17 comma 2 del DPCM 22 febbraio 2013 ("*Per ciascuna chiave di certificazione il certificatore genera un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce*") debba essere ritenuta applicabile esclusivamente ai certificati di certificazione per l'emissione di certificati per la generazione di firme e di validazione temporale.

Al fine di agevolare l'emissione dei certificati elettronici qualificati di autenticazione siti web, si informano i QTSP qualificati per il rilascio di tali certificati che è possibile chiedere la pubblicazione sull'Elenco di Fiducia di cui all'articolo 22 del Regolamento eIDAS, dei certificati di certificazione per l'emissione di certificati qualificati di autenticazione siti web non self-signed.

****

Avviso n. 15 - Modalità di verifica della firma della Trust List (TL)

La Decisione di esecuzione (UE) 2015/1505 della Commissione europea, stabilisce che gli Stati membri debbano notificare alla Commissione due o più certificati a chiave pubblica utilizzabili per verificare la sottoscrizione dell'elenco di fiducia (TL) nazionale. La Commissione pubblica tali certificati nel proprio elenco di fiducia. La verifica della firma degli elenchi di fiducia è quindi basata sulla presenza di un opportuno certificato nell'elenco pubblicato dalla Commissione europea.

Pertanto è improprio cercare la lista di revoca (CRL) ove verificare eventuali revoche di detti certificati: la verifica deve avere come fonte la lista di fiducia della Commissione europea.
Ciononostante, in considerazione che alcune implementazioni considerano ancora necessario accedere alla lista di revoca (CRL), al fine di evitare problemi e fornire tempo per apportare le modifiche necessarie, l'Agenzia continua a rendere disponibile una lista di revoca (https://eidas.agid.gov.it/TL/IT_CRL.crl). Questa lista di revoca è verificabile con un certificato dedicato a tale scopo.

****

Avviso n. 14 - Modifiche alla Deliberazione CNIPA n. 45 - Consultazione pubblica

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 provvedimento in corso di emanazione - che sostituirà le attuali regole tecnologiche emanate con la Deliberazione CNIPA n.45/2009 - contiene alcuni obblighi e raccomandazioni volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete.
La bozza del provvedimento è resa disponibile per 15 giorni per la consultazione pubblica.
Fino al 16 marzo 2018 è quindi possibile visionare e inviare eventuali commenti inviando una mail a consultazione-pubblica@agid.gov.it .
Il termine ultimo per la partecipazione alla consultazione pubblica è scaduto, si ringrazia tutti per la partecipazione**.**

****

Avviso n. 13 - Nuova modalità pubblicazione elenco dei prestatori di servizi fiduciari
Si informa che a far data dal 2 maggio 2018, come pubblicato su Gazzetta Ufficiale della Repubblica Italiana serie generale n.31 del 07-02-2018, l'Agenzia per l'Italia Digitale continuare la pubblicazione dell'elenco di fiducia in un'unica ubicazione, all'indirizzo: https://eidas.agid.gov.it/TL/TSL-IT.xml.

Restano invariati il certificato di certificazione e i due certificati che potranno essere utilizzati per la verifica del citato elenco, già pubblicati nella Gazzetta Ufficiale della Repubblica Italiana serie generale n. 130 del 6 giugno 2016

****

Avviso n. 12 - Crittografia documentazione riservata da inviare all'Agenzia
Si informano i Certificatori accreditati che la documentazione riservata inviata a questa Agenzia deve essere cifrata con il seguente certificato.

****

Avviso n. 11 - Emazione Determina n. 185/2017 (Modalità presentazione istanze servizi qualificati) e n. 189/2017 (modifiche alla deliberazione n. 45/2009)
Si informa che sono state emanate la Determinazione n. 185/2017 recante "Le modalità con cui i soggetti che intendono avviare la prestazione di servizi fiduciari qualificati presentano all'AgID domanda di qualificazione ai sensi dell'art. 29 del decreto legislativo 7 marzo 2005, n. 82" e la Determinazione n.189/2017 recante "Modifiche alla Deliberazione n. 45 del 21 maggio 2009".

Si informa che, in considerazione che la norma ETSI EN 319412-5, prevede che il esi4-qcStatement-5 QC-STATEMENT presente nei certificati qualificati al fine di indicare dove è reperibile il PKI Disclosure Statements possa contenere diverse entrate per diverse lingue, in deroga a quanto prescritto nell'allegato alla Determinazione n. 185/2017 che prescrive che tale documento sia redatto in un unico documento in lingua italiana e inglese, è possibile utilizzare due documenti che verranno referenziati con due qcStatement-5, rispettivamente per la lingua inglese e italiana.

In data 19 settembre 2017 è stato pubblicato nella Gazzetta Ufficiale della Repubblica Italiana (serie generale n. 219) l'Avviso di emanazione della Determinazione n. 185/2017.

****

Avviso n. 10 - Nuova modalità di pubblicazione dell'elenco pubblico dei certificatori in conformità al Regolamento eIDAS
Con l'emanazione del Regolamento eIDAS, dal 1 luglio 2016, l'Agenzia ha dovuto utilizzare due nuovi certificati per la verifica sottoscrizione dell'elenco pubblico dei certificatori e modificare la modalità di pubblicazione dell'elenco (Trusted List/Elenco di fiducia).
Ulteriori informazioni sono disponibili nella sezione Certificati.

****

Avviso n. 9 - Il codice fiscale del titolare nel certificato qualificato di firma digitale

Fin dal 2005, i certificati afferenti la firma digitale contengono nell'attributo serialNumber del campo Soggetto (SubjectDN) il codice fiscale del titolare del certificato preceduto dal codice della nazione che lo ha emesso e dal carattere ":" (es. **IT:CCCNNN64T30H501H**).

Con la piena efficacia del regolamento eIDAS, tale informazione può essere codificata in altro modo, in particolare come prescritto dalla norma ETSI EN 319412-1 che prevede l'uso di diversi prefissi.

In particolare, per il codice fiscale, prescrive l'uso del prefisso "TIN" seguito dal codice nazione (es. IT) e dal carattere separatore "-".

La codifica del contenuto del serialNumber (il codice fiscale) può quindi assumere la seguente forma **TINIT-CCCNNN64T30H501H**

Al fine di formalizzare tale possibilità e normalizzare l'indicazione del codice fiscale in ottica europea, nel mese di giugno l'Agenzia emanerà un provvedimento di modifica dell'art. 12 della Deliberazione n. 45 del 21 maggio 2009.

Si invitano tutti i soggetti che utilizzano il codice fiscale del soggetto che sottoscrive con firma digitale o firma elettronica qualificata documenti estraendolo dal certificato qualificato a prendere atto di quanto sopra.

****

Avviso n. 8 - Formati di firma digitale obbligatoriamente accettati dalle pubbliche amministrazioni

La normativa attualmente vigente (Deliberazione n. 45) impone alle pubbliche amministrazioni di accettare alcuni formati di firma digitale. Fra questi, non vi è il formato PAdES (PDF - ISO 32000) che può essere accettato o meno.

A decorrere dal 1° luglio 2016 con la piena efficacia del Regolamento eIDAS (n. 910/2014) diviene obbligatorio per tutte le pubbliche amministrazioni che accettano firme digitali accettare tutti i formati definiti nella DECISIONE DI ESECUZIONE (UE) 2015/1506 DELLA COMMISSIONE dell'8 settembre 2015, fra quelli previsti, anche il formato PDF.

Oltre a sottolineare l'opportunità di accettare tale diffuso formato di firma, si evidenzia che la Decisione può essere applicata anche prima della decorrenza del citato obbligo. Si invitano le pubbliche amministrazioni a considerare tale opportunità.

Si ricorda che, al fine di verificare la validità delle firme elettroniche qualificate basate su certificati rilasciati da tutti i soggetti autorizzati in Europa, la Commissione europea ha reso disponibile un'applicazione open source che questa Agenzia rende disponibile per l'utilizzo online nella sezione "Software di verifica", direttamente accessibile qui.

****

Avviso n. 7 - Indicazione del Codice Fiscale nel certificato di firma digitale

Visto che il Codice Fiscale è elemento indispensabile in taluni procedimenti amministrativi, considerando che soggetti residenti all'estero sono dotati di Codice Fiscale rilasciato in Italia, si precisa che nell'attributo serialNumber (OID: 2.5.4.5) del campo SubjectDN, presente nei certificati qualificati di firma digitale conformemente alla Deliberazione n. 45/2009, può essere indicato il Codice Fiscale rilasciato in Italia anche nel caso in cui il titolare del certificato sia residente all'estero. Il codice fiscale è, in questo caso, preceduto dal country code ISO 3166 "IT" e dal carattere ":"(in notazione esadecimale "0x3A").

****

Avviso n. 6 - CAD, articolo 35 comma 5: Linee guida

Sulla G.U. Serie Generale n.271 del 21-11-2014 è stato comunicato che l'Agenzia ha pubblicato le Linee guida per la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma previste dall'articolo 35, comma 5, del decreto legislativo 7 marzo 2005, n. 82.

****

Avviso n. 5 - Firma digitale verificata ab origine

E' stata emanata la Determinazione Commissariale n. 63/2014 che stabilisce, ai sensi dell'articolo 19, comma 7, del DPCM 22 febbraio 2013, le modalità con cui rendere noto nel certificato qualificato che l'utilizzo della chiave privata per la generazione della firma è subordinato alla verifica da parte del certificatore della validità del certificato qualificato e dell'eventuale certificato di attributo. Il provvedimento consente di generare firme digitali con la particolarità di essere direttamente verificabili senza la necessità di accedere alle liste di revoca o sospensione dei certificati in quanto è il certificatore che garantisce che ogni firma digitale basata su tali certificati qualificati è stata generata durante il periodo di validità degli stessi.

Le applicazioni di verifica fornite dai certificatori accreditati dovranno essere aggiornate non oltre il 30 aprile 2015.

****

Avviso n. 4 - DPCM 22 febbraio 2013, articolo 63 comma 3 - Codifica firma XAdES

In Italia, le caratteristiche delle applicazioni di generazione della firma XML fornite dai certificatori accreditati sono definite nella Deliberazione CNIPA n. 45 del 21 maggio 2009. La deliberazione prescrive (art. 21, comma 16) che "Ai sensi del comma 8, sono altresì riconosciuti il formato di busta crittografica e di firma descritti nei documenti ETSI TS 101 903 – XAdES (versione 1.4.1) e ETSI TS 102 904 (versione 1.1.1)." .

L'art. 9 della Deliberazione prescrive che "L'elemento KeyInfo, opzionale nella specifica RFC 3275, deve essere sempre presente nella busta crittografica.".

La specifica ETSI TS 101 903 prescrive che possa essere usato l'elemento KeyInfo ovvero il SigningCertificate.

Visto quanto disposto al sopra citato art. 21 della deliberazione, considerata l'esigenza di salvaguardare la validità delle firme XML generate con strumenti forniti da certificatori accreditati in altri Stati membri dell'Unione, si chiarisce che, fermo restando il rispetto della citata specifica ETSI, l'assenza dell'elemento KeyInfo non ha come conseguenza l'invalidità della firma XAdES.

****

Avviso n. 3 - DPCM 22 febbraio 2013, articolo 63 comma 3 - Codifica dell'algoritmo di hash

In Italia, come anche in diversi Paesi europei, è previsto l'uso dello SHA256 nel processo di generazione della firma. Le regole sulle codifiche DER e BER degli oggetti ASN.1 sono specificati nel documento ITU Standards (X.690). In particolare, per quanto riguarda la codifica DER, al paragrafo 11.5 (Set and sequence components with default value) viene esplicitamente riportato: "The encoding of set value of sequence value shall not include an encoding for any component value which is equal to its default value". Gli standard di riferimento prescrivono quindi che per default l'algoritmo i hash utilizzato nel processo di generazione della firma sia lo SHA256 e che, in questo caso, l'attributo contenente tale informazione (hashAlgorithm) non debba essere presente, peraltro, la presenza di tale informazione non introduce alcun problema di sicurezza. Ciò premesso, chiarendo che i certificatori accreditati devono rispettare anche tale previsione nella realizzazione dei prodotti di generazione della firma digitale, ai sensi dell'articolo 63 comma 3 del DPCM 22 febbraio 2013, si evidenzia che qualora tale informazione fosse comunque presente attraverso la codifica del campo ESSCerIDv2 (hashAlgorithm), le firme digitali prodotte sono valide.

****

Avviso n. 2 - DPCM 22 febbraio 2013, articolo 63 comma 3 - La marca temporale

La marca temporale consiste nella predisposizione di un oggetto contenente l'hash (riferimento univoco al contenuto del documento) del documento informatico al quale si vuole associare un riferimento temporale opponibile a terzi per dimostrarne l'esistenza. Gli algoritmi di hash generalmente in uso per la generazione dell'hash del documento sono lo SHA-1 e lo SHA-256. Tale hash, generato dalle applicazioni in uso dagli utenti, è inviato ai sistemi di marcatura temporale che i certificatori rendono obbligatoriamente disponibili che generano un oggetto (marca temporale) contenente l'hash del documento e un riferimento temporale (di altissima precisione). La marca temporale è sottoscritta con firma elettronica dai certificatori. Per generate tale firma i certificatori hanno l'obbligo di utilizzare l'algoritmo di hash SHA-256.

I certificatori rendono disponibili le applicazioni per generare richieste di marca temporale basate sull'algoritmo SHA-256, ma è compito degli utenti mantenere aggiornate le proprie postazioni di lavoro. Purtroppo numerosi sono gli utenti che non hanno ancora provveduto a tale aggiornamento. Ciò considerato, come stabilito dall'articolo 63 comma 3 del DPCM 22 febbraio 2013, si informa che anche le marche temporali che contengono hash di documenti calcolati con l'algoritmo SHA-1 sono valide, purché la sottoscrizione delle stesse avvenga con il previsto algoritmo SHA-256. L'uso dell'algoritmo SHA-1 non introduce ancora problemi sulla robustezza della marca temporale poiché la stessa è protetta da sottoscrizione con il più robusto algoritmo SHA-256 e, allo stato attuale, utilizzando l'algoritmo SHA-1, non è possibile generare due valori di hash identici che afferiscano a documenti diversi contenenti testo di senso compiuto. Comunque, si suggerisce di non usare l'algoritmo SHA-1 (il cui uso è generalmente personalizzabile dagli utenti), il cui utilizzo non sarà più consentito con l'emanazione delle nuove regole tecnologiche. Si coglie l'occasione per ribadire agli utilizzatori di mantenere aggiornate le applicazioni di firma digitale e marcatura temporale.

****

Avviso n. 1 - DPCM 22 febbraio 2013, articolo 63 comma 3 – Attributo SigningCertificateV2 e marca temporale

Le regole tecnologiche vigenti al febbraio 2014 prescrivono l'uso dell'algoritmo di hash SHA-256 nel processo di generazione delle marche temporali e la conformità con la RFC 3161. Tale RFC, a seguito della modifica apportata con la RFC 5816, prescrive la presenza dell'attributo SigningCertificateV2.

Premesso che le applicazioni di generazione delle marche temporali devono rispettare tali specifiche, si informa che le marche temporali contenenti l'attributo *SigningCertificate* anziché *SigningCertificateV2* sono valide in quanto tale difformità non ne mette a rischio la sicurezza.

****