Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Linee guida per la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma elettronica– CAD art. 35, comma 5

Indice

1 Acronimi e definizioni

Agenzia	Agenzia per l'Italia Digitale
CAD	D.Lgs. 7 marzo 2005, n. 82, recante "Codice dell'Amministrazione digitale"
documenti di certificazione	I documenti pubblicati a seguito della certificazione di sicurezza eseguita ai sensi dell'art. 35 comma 4 del CAD, quali il traguardo di sicurezza, il rapporto di certificazione, eventuali note integrative e, comunque, qualunque documento che correda la certificazione dell'SSCD
documenti di conformità	I documenti pubblicati a seguito dell'accertamento di conformità eseguito dall'OCSI ai sensi dell'art. 35 comma 5 del CAD, o dagli organismi di cui all'art. 35, comma 6, quali l'attestato di conformità, il rapporto di accertamento, eventuali note integrative e, comunque, qualunque documento che correda l'accertamento di conformità dell'SSCD
DPCM	Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013
firma	Firma elettronica qualificata e firma digitale come definite nel CAD
OCSI	Organismo di Certificazione della Sicurezza Informatica (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) del Ministero dello Sviluppo Economico
OTP	One Time Password
SSCD	Dispositivo sicuro per la generazione della firma
SYA	Something You Are: una caratteristica peculiare del soggetto, tipicamente biometrica
SYH	Something You Have: un oggetto posseduto da un soggetto che fornisce o costituisce una credenziale di autenticazione
SYK	Something You Know: un segreto conosciuto da un soggetto
titolare	L'utente titolare del certificato di firma

2 Premessa

Il Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni, recante il "Codice dell'amministrazione digitale", di seguito indicato anche come "CAD", all'art. 35 prescrive che i dispositivi SSCD debbano essere dotati di certificazione di sicurezza in conformità a criteri di valutazione riconosciuti in ambito europeo ed internazionale (comma 4) e che la conformità di tali dispositivi ai requisiti prescritti dall'allegato III della direttiva 1999/93/CE – salvo quanto disposto al comma 6 - è accertata in Italia dall'OCSI (comma 5).

Inoltre, l'articolo 35 dispone che la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma sia effettuata dall'Agenzia in conformità ad apposite linee guida da questa emanate, acquisito il parere obbligatorio dell'Organismo di certificazione della sicurezza informatica.

Le presenti linee guida, acquisito il parere dell'OCSI, sono pertanto emanate ai sensi dell'art. 35, comma 5, del CAD.

3 Scopo delle linee guida

Nel presente documento sono individuate le modalità con cui i certificatori accreditati ai sensi dell'art. 29 del CAD richiedono il riconoscimento della conformità del sistema e degli strumenti di autenticazione resi disponibili dai medesimi ai propri utenti al fine di utilizzare i dispositivi sicuri per la creazione della firma.

4 Applicabilità delle Linee guida

La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma, oggetto delle presenti linee guida, è necessaria solo nel caso in cui tali sistemi e/o strumenti non siano presenti nei documenti di certificazione o di conformità degli apparati di firma.

5 Obiettivo della valutazione

La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma è volta ad accertare la possibilità del titolare di mantenere, con ragionevole certezza, il controllo esclusivo della chiave privata utilizzata per la generazione della firma.

6 Dispositivi di firma utilizzabili

I dispositivi per la generazione della firma a cui sono applicabili le presenti linee guida devono aver ottenuto la certificazione di sicurezza e l'attestato di conformità ai sensi dell'art. 35 del CAD.

7 Presentazione della domanda

I certificatori accreditati ai sensi dell'art. 29 del CAD sottopongono all'Agenzia apposita richiesta inviandola all'Ufficio di Protocollo, all'indirizzo di posta elettronica certificata pubblicato sul sito istituzionale dell'Agenzia.

La richiesta contiene:

1. Marca, modello e versione dell'SSCD
2. Configurazione dell'SSCD utilizzata (solo nel caso in cui la certificazione del dispositivo consenta diverse configurazioni)
3. Eventuali limitazioni d'uso dei certificati di firma
4. Tipologie degli utilizzatori titolari dei certificati di firma
5. Descrizione delle credenziali o dei dispositivi di autenticazione (SYK e SYH/SYA) e delle misure atte alla loro protezione
6. Descrizione dell'interazione fra titolare e sistema di firma
7. Descrizione dell'interazione fra sistema di firma e SSCD
8. Descrizione di eventuali applicazioni di generazione di codici OTP
9. Modalità di verifica delle credenziali di autenticazione
10. Descrizione dei protocolli di sicurezza utilizzati
11. Analisi del sistema sottoposto alla valutazione di conformità, volta a dimostrare che lo stesso garantisce all'utente il controllo esclusivo della chiave privata di firma.
12. Descrizione dell'ambiente funzionale/operativo in cui agisce il sottoscrittore.

8 Iter istruttorio

L'istruttoria relativa alle domande e la valutazione della documentazione prodotta sono effettuate dall'Agenzia ai sensi dell'art. 35 del CAD e dell'art. 3, comma 7, del DPCM.

L'iter istruttorio prevede quanto segue:

1. la domanda di valutazione della conformità si considera accolta qualora non venga comunicato al certificatore un provvedimento di diniego entro sessanta giorni dalla data di presentazione della stessa;

2. il termine di sessanta giorni di cui al punto precedente, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità dell'Agenzia o che questa non possa acquisire autonomamente presso altre pubbliche amministrazioni. Il periodo di sospensione si conclude al momento della ricezione della documentazione integrativa da presentare improrogabilmente entro centottanta giorni dalla data di sospensione;

3. l'Agenzia si riserva, secondo quanto previsto al precedente punto 2, di richiedere integrazioni alla documentazione presentata e di effettuare le opportune verifiche su quanto dichiarato;

4. al termine dell'istruttoria, l'Agenzia accoglie la domanda ovvero la respinge, con provvedimento motivato, e ne dà apposita comunicazione al richiedente.

9 Validità della valutazione

La favorevole valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma, di cui al punto 8, resta in vigore fino al verificarsi di uno o più dei seguenti eventi che interessano le misure utilizzate dal sistema di autenticazione valutato positivamente dall'Agenzia:

1) Viene apportata una qualsiasi rilevante modifica a tali misure di autenticazione;

2) Viene riscontrata la sopraggiunta inadeguatezza delle misure di autenticazione approvate, anche a seguito di segnalazioni da parte dell'Agenzia.

Al fine di salvaguardare la validità della valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma, il certificatore interessato sottopone all'Agenzia nuova domanda, strutturata come indicato al punto 7, che indichi le misure correttive atte ad ovviare alla sopraggiunta inadeguatezza.

Tale domanda è esaminata dall'Agenzia con lo stesso iter indicato al punto 8.