Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC)

Ufficio federale delle comunicazioni UFCOM

Allegato dell'ordinanza dell'UFCOM del 23 novembre 2016 sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali (RS 943.032.1)

Prescrizioni tecniche e amministrative

concernenti

i servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali

1ª edizione: 23.11.2016
Entrata in vigore: 1.1.2017

Indice

1 In generale

1.1 Campo d’applicazione

Le presenti prescrizioni tecniche e amministrative (PTA) costituiscono l'allegato dell’ordinanza dell’UFCOM del 23 novembre 2016 sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali (RS 943.032.1). Si basano su:

- l’articolo 21 capoverso 2 della legge del 18 marzo 2016 sulla firma elettronica (FiEle) [1];
- gli articoli 3 capoverso 2, 4 capoverso 1, 10 e 15 dell’ordinanza del 23 novembre 2016 sulla firma elettronica (OFiEle) [2].

Esse precisano le condizioni preliminari e le esigenze fondamentali derivanti dalla legge e dall’ordinanza, al cui rispetto è tenuto, affinché possa ottenere il riconoscimento, il prestatore di servizi di certificazione (CSP), che rilascia certificati qualificati e che può fornire altri servizi nell’ambito della firma elettronica e delle altre applicazioni dei certificati digitali.

Una grande parte del presente documento è basata sui principi e sulle procedure descritti nelle norme internazionali riportate al capitolo 1.2.

1.2 Riferimenti

[1] RS 943.03, FiEle
Legge del 18 marzo 2016 sulla firma elettronica

[2] RS 943.032, OFiEle
Ordinanza del 23 novembre 2016 sulla firma elettronica

[3] ETSI EN 319 411-2 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[4] FIPS 140-2 (2001)
Security Requirements for Cryptographic Modules

[5] CWA 14169 (2004)
Secure Signature-Creation Devices "EAL 4+"

[6] EN 419211-2:2013
Protection profiles for secure signature creation device. Part 2: Device with key generation

[7] EN 419211-3:2013
Protection profiles for secure signature creation device. Part 3: Device with key import

[8] EN 419211-4:2014
Protection profiles for secure signature creation device. Part 4: Extension for device with key generation and trusted channel to certificate generation application

[9] EN 419211-5:2014
Protection profiles for secure signature creation device. Part 5: Extension for device with key generation and trusted channel to signature creation application

[10] EN 419211-6:2014
Protection profiles for secure signature creation device. Part 6: Extension for device with key import and trusted channel to signature creation application

[11] ISO/IEC 15408:2005
Information technology – Security techniques. Evaluation criteria for IT security

[12] ISO/IEC 15408-3:2008
Information technology – Security techniques. Evaluation criteria for IT security —Part 3: Security assurance components

[13] CEN/TS 419241:2014
Security Requirements for Trustworthy Systems Supporting Server Signing

[14] ETSI EN 319 412-1 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[15] ETSI EN 319 412-2 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[16] ETSI EN 319 412-3 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[17] ETSI EN 319 412-4 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[18] ETSI EN 319 412-5 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[19] RFC 5280 (mai 2008)
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile

[20] Common PKI Specifications for Interoperable Applications. Version 2.0 – 20 January 2009

[21] ETSI EN 319 421 V1.1.1 (2016-03)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[22] ETSI EN 319 422, V1.1.1 (2016-03)
Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

I documenti indicati nei riferimenti sono disponibili presso le seguenti organizzazioni:

Testi legali con riferimento RS	Ufficio federale delle costruzioni e della logistica (UFCL) Servizio di diffusione delle pubblicazioni federali CH-3003 Berna www.bundespublikationen.admin.ch
Documenti ETSI	ETSI, Istituto Europeo per gli Standard di Telecomunicazioni 650 route des Lucioles 06921 Sophia Antipolis, France www.etsi.org
Documenti FIPS	National Institute of Standards and Technology (NIST) csrc.nist.gov/publications
Documenti del CEN	Comité européen de normalisation (CEN) 36, rue de Stassart B - 1050 Brussels, Belgique www.cenorm.be
Norme EN	Associazione svizzera di normalizzazione (SNV) Bürglistr. 29 CH-8400 Winterthur www.snv.ch
Norme ISO	Secrétariat central de l'Organisation internationale de normalisation (ISO)

	1, rue de Varembé 1211 Ginevra www.iso.org
Documenti RFC	Internet Engineering Task Force (IETF) http://www.ietf.org
Common PKI Specifications for Interoperable Applications	T7 (Arbeitsgemeinschaft von deutschen Trustcenterbetreibern und Zertifizierungsdiensteanbietern) www.t7ev.org
Prescrizioni tecniche e amministrative	UFCOM Rue de l'Avenir 44 Casella postale 2501 Bienne www.ofcom.admin.ch

1.3 Abbreviazioni

CEN	Comitato europeo di normalizzazione
CP	*Certification Policy* – Politica di certificazione
CPS	*Certification Practice Statement* – Dichiarazione delle pratiche di certificazione
CRL	*Certificate Revocation List* – Lista dei certificati annullati
CSP	*Certification Service Provider* – Prestatore di servizi di certificazione
CWA	*CEN Workshop Agreement* – Accordo di laboratorio del CEN
EAL	*Evaluation Assurance Level* – Livello di garanzia della valutazione
EN	*European Normative* – Ordinamento normativo europeo
ETSI	*European Telecommunications Standards Institute* – Istituto europeo delle norme di telecomunicazione
FiEle	Legge sulla firma elettronica [1]
FIPS	*Federal Information Processing Standards*
IDI	Numero d'identificazione delle imprese
IEC	*International Electrotechnical Commission* – Commissione Elettrotecnica Internazionale
IETF	*Internet Engineering Task Force*
ISO	*International Standardization Organization* – Organizzazione internazionale per la standardizzazione
LIDI	Legge federale sul numero d'identificazione delle imprese
OID	*Object Identifier*
OFiEle	Ordinanza sulla firma elettronica [2]
PIN	*Personal Identification Number* – numero di identificazione personale
PKI	*Public Key Infrastructure* – infrastruttura a chiave pubblica
RFC	*Request for Comments*
RS	Raccolta sistematica

2 Requisiti essenziali

2.1 Organizzazione e principi operativi

2.1.1 Politica di certificazione e dichiarazione delle pratiche di certificazione

Il CSP deve redigere e gestire una politica di certificazione (CP) e una dichiarazione relativa alle pratiche di certificazione (CPS) conformemente alla norma ETSI EN 319 411-2 [3], capitoli 5 *General Provisions On Certificate Pratice Statement* and *Certificate Policies* e 7 *Framework for the definition of other certificate policies*.

2.1.2 Gestione della sicurezza

Il CSP mette in atto un sistema di gestione della sicurezza conformemente alla norma ETSI EN 319 411-2 [3], capitoli 6.4 *Facility, Management, and Operational Controls*, 6.5.5 *Computer Security Controls*, 6.5.6 *Life Cycle Security Controls*, 6.5.7 *Network Security Controls*.

2.1.3 Aspetti finanziari e legali

Il CSP agisce conformemente alla norma ETSI EN 319 411-2 [3], capitolo 6.8 *Other Business and Legal Matters*.

2.1.4 Altri aspetti organizzativi e operativi

Il CSP agisce conformemente alla norma ETSI EN 319 411-2 [3], capitolo 6.9 *Other Provisions*.

2.2 Gestione delle chiavi

2.2.1 Gestione e utilizzazione delle chiavi del CSP

Il CSP deve gestire e utilizzare le proprie chiavi conformemente alla norma ETSI EN 319 411-2 [3], capitoli 6.5.1 *Key Pair Generation and Installation*, 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls*, 6.5.3 *Other Aspects of Key Pair Management*, 6.5.4 *Activation Data.*

2.2.2 Generazione da parte del CSP, delle chiavi della persona che richiede il certificato

a) Se il CSP genera la coppia di chiavi della persona che richiede il certificato, questo processo deve essere conforme alla norma ETSI EN 319 411-2 [3], capitoli 6.5.1 *Key Pair Generation and Installation,* 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls,* 6.5.4 *Activation Data*.

b) Se il CSP genera la coppia di chiavi del richiedente, tale generazione deve essere realizzata in uno dei dispositivi seguenti:

- dispositivo con attestato di conformità ai requisiti del documento FIPS 140-2 [4] livello 3 o superiore;
- dispositivo che soddisfa i requisiti del documento CWA 14169 [5] e valutato come livello EAL 4 della norma ISO/IEC 15408:2005 [11] potenziato con i componenti di sicurezza ADV-IMP.2 (*implementation of the TSF*), AVA-CCA.1 (*vulnerability assessment, covert channel analysis*) e AVA_VLA.1 (*vulnerability assessment, highly resistant*) o le componenti di assicurazione corrispondenti della norma ISO/IEC 15408-3:2008 [12];
- dispositivo che soddisfa i requisiti prescritti nella norma EN 419211-2 [6], EN 419 211-4 [8] o EN 419211-5 [9] e valutato come livello EAL 4 della norma ISO/IEC 15408-3:2008 [12] potenziato con i componenti di sicurezza AVA_VAN.5 (*Advanced methodical vulnerability analysis*) o altri criteri di valutazione equivalenti e riconosciuti nel campo della sicurezza;
- dispositivo valutato come livello EAL 4 della norma ISO/IEC 15408-3:2008 [12] potenziato con i componenti di sicurezza AVA_VAN.5 (*Advanced methodical vulnerability analysis*) o altri criteri di valutazione equivalenti e riconosciuti nel campo della sicurezza. In questo caso deve essere fornito un obiettivo di valutazione che soddisfa i requisiti definiti nei documenti sopraccitati.

2.2.3 Dispositivi sicuri per la creazione di firme e sigilli

a) Il CSP deve assicurarsi che la persona che richiede un certificato utilizzi dispositivi sicuri per la creazione di firme e sigilli conformi ai requisiti minimi di cui all'articolo 6 capoverso 2 FiEle [1] o fornirglieli. I documenti seguenti presuppongono la conformità ai requisiti di cui all'articolo 6 capoverso 2 FiEle [1]:

- CWA 14169 [5]
- EN 419211-2 [6]
- EN 419211-3 [7]
- EN 419211-4 [8]
- EN 419211-5 [9]
- EN 419211-6 [10]

Inoltre, i dispositivi sicuri per la creazione di firme e sigilli devono essere conformi ai requisiti seguenti:

- dopo che è stato effettuato un numero predeterminato di tentativi di attivazione errati e successivi, deve essere bloccato l'utilizzo della chiave crittografica privata. Questo numero

non può superare i 4 tentativi per un PIN di 6 caratteri. Per PIN composti di un maggior numero di caratteri, può essere previsto un numero superiore di tentativi, a condizione che ciò sia previsto nella documentazione messa a disposizione dallo sviluppatore del dispositivo sicuro e certificato per la creazione di firme e sigilli;

- il CSP può sbloccare l'uso della chiave crittografica privata solo dopo aver verificato che la domanda di sblocco proviene dal titolare delle chiavi.

b) La certificazione dei dispositivi sicuri per la creazione di firme e sigilli deve essere ottenuta per ciascuno dei requisiti citati alla lettera a:

- al livello EAL 4 della norma ISO/IEC 15408:2005 [11] potenziato con i componenti di sicurezza ADV-IMP.2 (*implementation of the TSF*), AVA-CCA.1 (*vulnerability assessment, covert channel analysis*) e AVA_VLA.1 (*vulnerability assessment, highly resistant*), o

- al livello di valutazione EAL 4 della norma ISO/IEC 15408-3:2008 [12] potenziato con i componenti di sicurezza AVA_VAN.5 (*Advanced methodical vulnerability analysis*).

c) Se il CSP fornisce i dispositivi sicuri per la creazione di firme e sigilli, è tenuto a effettuarne la manutenzione conformemente alla norma ETSI EN 319 411-2 [3], capitoli 6.5.1 *Key Pair Generation and Installation,* 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls* e 6.5.4 *Activation Data*.

d) Un sistema che permette di creare firme elettroniche e sigilli tramite un dispositivo che non è in possesso del titolare del certificato di firma è considerato un dispositivo sicuro per la creazione di firme ai sensi dell'articolo 6 FiEle a condizione che sia conforme ai requisiti della norma CEN/TS 419241 [13]. Il sistema deve assicurare l'autenticazione del titolare della chiave crittografica privata secondo il livello 2 (*Level 2 sole control*) descritto nel documento CEN/TS 419241 [13].

2.3 Gestione di certificati regolamentati

2.3.1 Rilascio, gestione e annullamento dei certificati regolamentati di terzi

a) Il CSP deve effettuare la registrazione della persona che richiede il certificato nonché gestire e annullare i certificati dei titolari conformemente alla norma ETSI EN 319 411-2 [3], capitoli 6.1 *Publication and Repository Responsibilities*, 6.2 *Identification and Authentication,* 6.3 *Certificate Life-Cycle Operational Requirements*.

b) Il CSP è tenuto ad annullare il certificato se l'organismo che ha confermato la qualifica professionale secondo il capitolo 2.3.2 lettera h lo informa che l'attestato non è più valido.

c) Il CSP che annulla un certificato deve aggiornare le informazioni in suo possesso riguardanti lo stato del certificato.

d) Il CSP deve ottenere l'accordo del titolare del certificato prima di pubblicare i motivi di annullamento di un certificato.

e) La sospensione di un certificato non è autorizzata.

2.3.2 Formato dei certificati regolamentati

a) Il CSP deve generare i certificati regolamentati di persone fisiche conformemente alla norma ETSI EN 319 412-2 [15].

b) Il CSP deve generare i certificati regolamentati di unità IDI conformemente alla norma ETSI EN 319 412-3 [16].

c) Il CSP deve generare i certificati regolamentati che si riferiscono a siti web conformemente alla norma ETSI EN 319 412-4 [17].

d) L'indicazione «*regulated certificate*» segnala che il certificato è rilasciato a titolo di certificato regolamentato e deve figurare nel campo *explicitText* dell'estensione *certificatePolicies* secondo la norma RFC 5280 [19], capitolo 4.2.1.4.

e) Il numero unico d'identificazione dell'impresa secondo la LIDI deve essere menzionato per le unità IDI secondo la norma ETSI EN 319 412-1 [14], capitolo 5.1.4.

f) Il bit 1 (*contentCommitment*) dell'estensione *keyUsage* deve essere attivato soltanto per i certificati regolamentati di persone fisiche.

g) Nei certificati regolamentati che si riferiscono a una chiave per la verifica della firma o del sigillo, l'indicazione che la chiave crittografica privata è protetta tramite un dispositivo sicuro per la creazione di firme e sigilli deve comparire sotto forma di object identifier (OID) secondo la norma ETSI EN 319 412-5 [18], capitolo 4.2.2.

h) Se necessario, si indica una qualifica professionale nel certificato regolamentato inserendo l'attributo *Admission* nella sequenza *tbsCertificate* conformemente al documento RFC 5280 [19], capitolo 4.2.

L'organismo che conferma la qualifica professionale (art. 5 cpv. 2 OFiEle [2]) deve essere menzionato quale *directoryName* nel campo dati *admissionAuthority* conformemente al documento Common PKI Specification [20], tabella 29b con gli attributi indicati qui sotto e nello stesso ordine:
- *organizationName*: nome dell'organismo;
- *countryName*: stato dell'organismo;
- *postalAddress*: indirizzo dell'organismo.

Il certificato regolamentato può riportare una sola qualifica professionale. La qualifica professionale del titolare del certificato deve essere definita utilizzando il campo dati *professionItems* nella sequenza *professionInfo* conformemente al documento Common PKI Specification [20], tabella 29b.
L'OID della qualifica professionale deve inoltre essere definito utilizzando il campo dati

professionOID nella sequenza *professionInfo* conformemente al documento Common PKI Specification [20], tabella 29b.

i) Se necessario, l'attributo *title* del campo *subject* secondo il documento RFC 5280 [19], capitolo 4.1.2.6 è utilizzato esplicitamente per indicare che il titolare del certificato regolamentato è abilitato a rappresentare l'unità IDI indicata tramite l'attributo *organization* dello stesso campo *subject*.

j) Se necessario, il campo di utilizzazione per il quale il certificato regolamentato è previsto è illustrato nella politica di certificazione indicato nell'estensione *certificatePolicies* secondo il documento RFC 5280 [19], capitolo 4.2.1.5.

k) Se necessario, l'indicazione valore limite delle transazioni è segnalata secondo la norma ETSI EN 319 412-5 [18], capitolo 4.3.2.

2.3.3 Ulteriori requisiti applicabili al formato dei certificati qualificati

a) Il CSP deve generare i certificati qualificati conformemente alla norma ETSI EN 319 412-2 [15].

b) Deve essere utilizzato solo il bit 1(*contentCommitment*) dell'estensione *keyUsage*.

c) L'indicazione «*qualified certificate*» segnala che il certificato è rilasciato a titolo di certificato qualificato e deve figurare nel campo *explicitText* dell'estensione *certificatePolicies* secondo la norma RFC 5280 [19], capitolo 4.2.1.4. Il certificato comprende in più la dichiarazione descritta al capitolo 4.2.3 della norma ETSI EN 319 412-5 [18].

2.3.4 Gestione del certificato del CSP utilizzato per l'emissione di certificati regolamentati

a) Il CSP deve creare i propri certificati regolamentati conformemente alla norma IETF RFC 5280 [19].

b) L'indicazione «*regulated certificate*» segnala che il certificato è rilasciato a titolo di certificato regolamentato e deve figurare nel campo *explicitText* dell'estensione *certificatePolicies* secondo la norma RFC 5280 [19], capitolo 4.2.1.4.

c) Il numero unico d'identificazione dell'impresa ai sensi della LIDI deve essere menzionato secondo la norma ETSI EN 319 412-1 [14], capitolo 5.1.4.

2.4 Sistema marcatempo qualificato

a) Per rilasciare un attestato al fine di certificare l'esistenza di dati digitali a un momento determinato, il CSP deve servirsi di un sistema marcatempo qualificato conforme alla norma ETSI EN 319 421 [21].

b) Il sistema marcatempo qualificato dovrà rilasciare contrassegni temporali conformi al documento ETSI EN 319 422 [22].

Biel/Bienne, il 23 novembre 2016

UFFICIO FEDERALE DELLE COMUNICAZIONI

Philipp Metzger
Direttore