2025/1943

30.9.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/1943 DELLA COMMISSIONE

del 29 settembre 2025

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme di riferimento applicabili ai certificati qualificati di firme elettroniche e ai certificati qualificati di sigilli elettronici

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) n. 910/2014 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 ([1]), in particolare l'articolo 28, paragrafo 6, e l'articolo 38, paragrafo 6,

considerando quanto segue:

(1) I certificati qualificati di firme elettroniche e i certificati qualificati di sigilli elettronici svolgono un ruolo cruciale nell'ambiente imprenditoriale digitale, promuovendo la transizione dai processi cartacei tradizionali ai loro equivalenti elettronici. Collegando i dati di convalida della firma elettronica o i dati di convalida del sigillo elettronico rispettivamente a una persona fisica o giuridica e confermando il nome di tale persona, i certificati qualificati accrescono la certezza circa l'identità del firmatario e del creatore del sigillo.

(2) La presunzione di conformità di cui all'articolo 28, paragrafo 6, e all'articolo 38, paragrafo 6, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi fiduciari qualificati per il rilascio di certificati qualificati di firme elettroniche e i servizi fiduciari qualificati per il rilascio di certificati qualificati di sigilli elettronici sono conformi alle norme stabilite nel presente regolamento. Tali norme dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Esse dovrebbero essere adattate per includere controlli supplementari che garantiscano la sicurezza e l'affidabilità dei servizi fiduciari qualificati e del contenuto dei certificati qualificati.

(3) Se un prestatore di servizi fiduciari rispetta i requisiti di cui all'allegato del presente regolamento, gli organismi di vigilanza dovrebbero presumere la conformità ai pertinenti requisiti del regolamento (UE) n. 910/2014 e tenere debitamente conto di tale presunzione per la concessione o la conferma della qualifica del servizio fiduciario. Un prestatore di servizi fiduciari qualificato può comunque fare affidamento su altre pratiche per dimostrare la conformità ai requisiti del regolamento (UE) n. 910/2014.

(4) La Commissione valuta periodicamente le nuove tecnologie, pratiche, norme o specifiche tecniche. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([2]), la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento per mantenerlo in linea con gli sviluppi globali e le nuove tecnologie, norme o specifiche tecniche e per seguire le migliori pratiche sul mercato interno.

(5) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]) e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([4]) si applicano alle attività di trattamento di dati personali a norma del presente regolamento.

([1]) GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([5]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 6 giugno 2025.

(7) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 48 del regolamento (UE) n. 910/2014,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Norme di riferimento e specifiche applicabili ai certificati qualificati di firme elettroniche e sigilli elettronici

1. Le norme di riferimento e le specifiche di cui all'articolo 28, paragrafo 6, del regolamento (UE) n. 910/2014 figurano nell'allegato I del presente regolamento.

2. Le norme di riferimento e le specifiche di cui all'articolo 38, paragrafo 6, del regolamento (UE) n. 910/2014 figurano nell'allegato II del presente regolamento.

Articolo 2

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 29 settembre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

([5]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ALLEGATO I

Elenco delle norme di riferimento e delle specifiche per i certificati qualificati di firme elettroniche

Le norme ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») ed ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») si applicano con gli adeguamenti seguenti.

1. Per ETSI EN 319 411-2

1) 2.1 Riferimenti normativi

— [1] ETSI EN 319 401 V3.1.1 (2024-06) «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers».

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements», con gli adeguamenti seguenti:

Il punto 2.1 Riferimenti normativi della norma ETSI EN 319 411-1 V1.5.1 è modificato come segue:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers».

— [10] ETSI EN 319 412-2 V2.4.1 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons».

— [14] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures».

— [3] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements».

— [5] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures».

— [6] CEN/TS 419261:2015 «Security requirements for trustworthy systems managing certificates and time-stamps».

— [7] Gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Agreed Cryptographic Mechanisms» (meccanismi crittografici concordati) pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ([1]).

— [8] Regolamento di esecuzione (UE) 2024/482 della Commissione ([2]), recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

— [9] Regolamento di esecuzione (UE) 2024/3144 della Commissione ([3]), che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione.

— [10] ISO/IEC 15408:2022 (parti da 1 a 5): «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security».

— [11] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules».

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) GU L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 5.2 Requisiti della dichiarazione sulla pratica di certificazione

— OVR-5.2-02 La o le CP identificate dalla documentazione del TSP specificano i requisiti relativi ai profili dei certificati da utilizzare.

3) 5.3 Nome e identificazione della politica di certificazione

— OVR-5.3-01 In caso di modifiche apportate a una CP come descritto al punto 4.2.2 che incidono sull'applicabilità, l'identificativo della politica è modificato.

4) 6.1 Responsabilità delle pubblicazioni e dell'archivio

— OVR-6.1-02 Le informazioni identificate in DIS-6.1-04 della norma ETSI EN 319 411-1 [2] sono accessibili al pubblico e disponibili a livello internazionale.

5) 6.2.2 Convalida dell'identità iniziale

— REG-6.2.2-01A La raccolta di attributi e prove sull'identità del soggetto nonché la loro convalida sono specificate conformemente agli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 1 quater, del regolamento (UE) n. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] e [QCP-n-qscd] L'identità della persona fisica e, se opportuno, eventuali attributi specifici della persona sono verificati conformemente agli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 1 quater, del regolamento (UE) n. 910/2014 [i.1].

— NOTA 1 vuota.

6) 6.3.3 Rilascio del certificato

— GEN-6.3.3-01 Si applicano i requisiti da GEN-6.3.3-01 a GEN-6.3.3-10 individuati nella norma ETSI EN 319 411-1 [2], punto 6.3.3.

— GEN-6.3.3-02 [CONDIZIONALE] Se un certificato è rilasciato a una persona fisica identificata in associazione con la persona giuridica, gli attributi del soggetto che identificano l'organizzazione nel certificato rappresentano la persona giuridica o la sottoentità di tale persona giuridica e l'identificativo del soggetto nel certificato è la persona fisica.

— GEN-6.3.3-03 L'identificativo della CP è [SCELTA]:

(a) [QCP-n]

— come specificato al punto 5.3, lettera a), e/o

— un OID, assegnato dal TSP, da un altro portatore di interessi pertinente o da un'ulteriore normazione per una politica di certificazione che rafforzi i requisiti della corrispondente politica applicabile definiti nel presente documento.

(b) [QCP-n-qscd]

— come specificato al punto 5.3, lettera c), e/o

— un OID, assegnato dal TSP, da un altro portatore di interessi pertinente o da un'ulteriore normazione per una politica di certificazione che rafforzi i requisiti della corrispondente politica applicabile definiti nel presente documento.

7) 6.3.5 Coppia di chiavi e uso dei certificati

— SDP-6.3.5-02A [CONDIZIONALE] Se gestisce il QSCD per il soggetto, il TSP è un prestatore di servizi fiduciari qualificato che fornisce un servizio fiduciario qualificato per la gestione di un dispositivo qualificato per la creazione di una firma elettronica a distanza, conformemente al regolamento (UE) n. 910/2014 [i.1].

— SDP-6.3.5-11A Se l'abbonato o soggetto genera le chiavi del soggetto, gli obblighi dell'abbonato (cfr. punto 6.3.4) comprendono:

(a) l'obbligo di generare le chiavi del soggetto utilizzando un algoritmo conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza [7] e pubblicati dall'ENISA per gli usi della chiave certificata individuati nella CP;

(b) l'obbligo di utilizzare la lunghezza e l'algoritmo della chiave conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza [7] e pubblicati dall'ENISA per gli usi della chiave certificata individuati nella CP durante il periodo di validità del certificato.

8) 6.3.10 Servizi relativi alla situazione del certificato

— CSS-6.3.10-08 [CONDIZIONALE] Se sono fornite CRL, il TSP preserva l'integrità e la disponibilità dell'ultima CRL almeno per il periodo specificato nella CPS come richiesto in CSS-6.3.10-12.

9) 6.4.4 Controlli del personale

— OVR-6.4.4-02 Il personale del TSP in ruoli di fiducia e, se del caso, i subcontraenti del TSP in ruoli di fiducia sono in grado di soddisfare il requisito in materia di «competenze, esperienza e qualifiche» mediante formazione e credenziali formali, o effettiva esperienza, o una combinazione di entrambe.

— OVR-6.4.4-03 La conformità al requisito OVR-6.4.4-02 comprende aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza.

— OVR-6.4.4-04 Oltre ai ruoli di fiducia individuati nella norma ETSI EN 319 401 [1] (punto 7.2-15), sono supportati i ruoli di fiducia dei funzionari addetti alla registrazione e alla revoca con responsabilità definite nella norma TS 419261 [6]. Nei casi in cui il QTSP è gestito direttamente da uno Stato membro o da un organismo del settore pubblico o per suo conto, tali ruoli di fiducia aggiuntivi possono essere svolti da uno o più rappresentanti formali che agiscono per conto di funzionari addetti alla registrazione e alla revoca operanti presso le amministrazioni locali o regionali.

10) 6.4.9 Cessazione di CA o RA

— OVR-6.4.9-02 Il piano di cessazione del TSP è conforme ai requisiti stabiliti negli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014 [i.1].

11) 6.5.1 Generazione e installazione della coppia di chiavi

— OVR-6.5.1-01A La generazione della coppia di chiavi della CA è effettuata utilizzando un algoritmo conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [7] ai fini della firma della CA.

— OVR-6.5.1-01B La lunghezza della chiave e l'algoritmo selezionati per la chiave di firma della CA sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [7] ai fini della firma della CA.

— OVR-6.5.1-01C [CONDIZIONALE] Se la CA genera le chiavi del soggetto, le chiavi del soggetto generate dalla CA sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [7] ai fini indicati nella CP durante il periodo di validità del certificato.

12) 6.5.2 Protezione delle chiavi private e controlli tecnici dei moduli crittografici

— GEN-6.5.2-01 Si applicano tutti i requisiti individuati nella norma ETSI EN 319 411-1 [2], punto 6.5.2, ad eccezione dei requisiti OVR-6.5.2-01, OVR-6.5.2-03 e OVR-6.5.2-04.

— GEN-6.5.2-02 La generazione della coppia di chiavi del TSP, comprese le chiavi utilizzate dai servizi di revoca e registrazione, è effettuata all'interno di un dispositivo crittografico sicuro, che è un sistema affidabile certificato conformemente a quanto segue:

— criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, quali definiti nella norma ISO/IEC 15408 [10] o in «Common Criteria for Information Technology Security Evaluation», versione CC:2002, parti da 1 a 5, pubblicato dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security», e certificato a livello EAL 4 o superiore; o

— sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) [8][9], e certificato a livello EAL 4 o superiore; o

— fino al 31.12.2030, FIPS PUB 140-3 [11] livello 3.

Tale certificazione riguarda un obiettivo di sicurezza o un profilo di protezione, o la progettazione di un modulo e la documentazione di sicurezza, che soddisfano i requisiti del presente documento, sulla base di un'analisi dei rischi e tenendo conto delle misure di sicurezza fisiche e di altre misure di sicurezza non tecniche.

Se il dispositivo crittografico sicuro beneficia di una certificazione EUCC [8][9], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— GEN-6.5.2-03 La chiave di firma privata della CA è detenuta e utilizzata all'interno di un dispositivo crittografico sicuro che soddisfa i requisiti di GEN-6.5.2-01 e GEN-6.5.2-02.

13) 6.5.7 Controlli di sicurezza della rete

— OVR-6.5.7-02 La scansione delle vulnerabilità richiesta dal requisito REQ-7.8-13 della norma ETSI EN 319 401 [1] è eseguita almeno una volta a trimestre.

— OVR-6.5.7-03 Il test di penetrazione richiesto dal requisito REQ-7.8-17X della norma ETSI EN 319 401 [1] è eseguito almeno una volta all'anno.

— OVR-6.5.7-03 I firewall sono configurati in modo da impedire tutti i protocolli e gli accessi non richiesti per il funzionamento del TSP.

14) 6.6.1 Profilo del certificato

— GEN-6.6.1-05 Il certificato comprende uno degli identificativi della politica individuati in GEN-6.3.3-03 [SCELTA]. Il certificato può comprendere altri OID assegnati dal TSP.

2. Per ETSI EN 319 412-2

1) 2.1 Riferimenti normativi

— [2] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements».

— [9] Gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia, «Agreed Cryptographic Mechanisms» (meccanismi crittografici concordati) pubblicati dall'ENISA.

2) 4.2.2 Firma

— GEN-4.2.2-2 L'algoritmo di firma è selezionato conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [9].

— NOTA vuota.

3) 4.2.3.1 Emittenti persone giuridiche

— GEN-4.2.3.1-3 Se è nota l'esistenza di un numero di registrazione appropriato, l'identità dell'emittente contiene un organizationIdentifier con un valore di tale numero di registrazione quale indicato nel corrispondente registro ufficiale che stabilisce tale numero di registrazione.

4) 4.2.5 Informazioni sulla chiave pubblica del soggetto

— GEN-4.2.5-2 La chiave pubblica del soggetto è selezionata conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [9].

— NOTA vuota.

5) 4.2.6 Numero di serie

— GEN-4.2.6-01 Il numero serialNumber del certificato (come specificato in IETF RFC 5280 [1], punto 4.1.2.2) è unico per ciascun certificato rilasciato dal TSP.

ALLEGATO II

Norme di riferimento e specifiche per i certificati qualificati di sigilli elettronici

Le norme ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-3 V1.3.1 («ETSI EN 319 412-3»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») e ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») si applicano con gli adeguamenti seguenti:

1. Per ETSI EN 319 411-2

1) 2.1 Riferimenti normativi

— [1] ETSI EN 319 401 V3.1.1 (2024-06) «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers».

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements», con gli adeguamenti seguenti:

Il punto 2.1 Riferimenti normativi della norma ETSI EN 319 411-1 V1.5.1 è modificato come segue:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers».

— [10] ETSI EN 319 412-2 V2.4.1 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons».

— [14] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures».

— [3] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements».

— [5] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures».

— [6] CEN/TS 419261:2015 «Security requirements for trustworthy systems managing certificates and time-stamps» (prodotta dal CEN).

— [7] Gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Meccanismi crittografici concordati» pubblicati dall'ENISA.

— [8] Regolamento di esecuzione (UE) 2024/482 recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

— [9] Regolamento di esecuzione (UE) 2024/3144 che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione.

— [10] ISO/IEC 15408:2022 (parti da 1 a 5) «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security».

— [11] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules».

2) 5.2 Requisiti della dichiarazione sulla pratica di certificazione

— OVR-5.2-02 La o le CP identificate dalla documentazione del TSP specificano i requisiti relativi ai profili dei certificati da utilizzare.

3) 5.3 Nome e identificazione della politica di certificazione

— OVR-5.3-01 In caso di modifiche apportate a una CP come descritto al punto 4.2.2 che incidono sull'applicabilità, l'identificativo della politica è modificato.

4) 6.1 Responsabilità delle pubblicazioni e dell'archivio

— OVR-6.1-02 Le informazioni identificate in DIS-6.1-04 della norma ETSI EN 319 411-1 [2] sono accessibili al pubblico e disponibili a livello internazionale.

5) 6.2.2 Convalida dell'identità iniziale

— REG-6.2.2-01A La raccolta di attributi e prove sull'identità del soggetto nonché la loro convalida sono specificate conformemente agli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 1 quater, del regolamento (UE) n. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] e [QCP-l-qscd] L'identità della persona giuridica e, se opportuno, eventuali attributi specifici della persona sono verificati conformemente agli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 1 quater, del regolamento (UE) n. 910/2014 [i.1].

— NOTA 3 cfr. nota 2.

6) 6.3.3 Rilascio del certificato

— GEN-6.3.3-01 Si applicano i requisiti da GEN-6.3.3-01 a GEN-6.3.3-10 individuati nella norma ETSI EN 319 411-1 [2], punto 6.3.3.

— GEN-6.3.3-02 L'identificativo della CP è [SCELTA]:

(a) [QCP-l]

— come specificato al punto 5.3, lettera b), e/o

— un OID, assegnato dal TSP, da un altro portatore di interessi pertinente o da un'ulteriore normazione per una politica di certificazione che rafforzi i requisiti della corrispondente politica applicabile definiti nel presente documento.

(b) [QCP-l-qscd]

— come specificato al punto 5.3, lettera d), e/o

— un OID, assegnato dal TSP, da altri portatori di interessi pertinenti o da un'ulteriore normazione per una politica di certificazione che rafforzi i requisiti della corrispondente politica applicabile definiti nel presente documento.

7) 6.3.5 Coppia di chiavi e uso dei certificati

— SDP-6.3.5-02A [CONDIZIONALE] Se gestisce il QSCD per il soggetto, il TSP è un prestatore di servizi fiduciari qualificato che fornisce un servizio fiduciario qualificato per la gestione di un dispositivo qualificato per la creazione di un sigillo elettronico a distanza, conformemente al regolamento (UE) n. 910/2014 [i.1].

— SDP-6.3.5-11A Se l'abbonato o soggetto genera le chiavi del soggetto, gli obblighi dell'abbonato (cfr. punto 6.3.4) comprendono:

(a) l'obbligo di generare le chiavi del soggetto utilizzando un algoritmo conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [7] per gli usi della chiave certificata individuati nella CP; e

(b) l'obbligo di utilizzare la lunghezza e l'algoritmo della chiave conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [7] per gli usi della chiave certificata individuati nella CP durante il periodo di validità del certificato.

8) 6.3.10 Servizi relativi alla situazione del certificato

— CSS-6.3.10-08 [CONDIZIONALE] Se sono fornite CRL, il TSP preserva l'integrità e la disponibilità dell'ultima CRL almeno per il periodo specificato nella CPS come richiesto in CSS-6.3.10-12.

9) 6.4.4 Controlli del personale

— OVR-6.4.4-02 Il personale del TSP in ruoli di fiducia e, se del caso, i subcontraenti del TSP in ruoli di fiducia sono in grado di soddisfare il requisito in materia di «competenze, esperienza e qualifiche» mediante formazione e credenziali formali, o effettiva esperienza, o una combinazione di entrambe.

— OVR-6.4.4-03 La conformità al requisito OVR-6.4.4-02 comprende aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza.

— OVR-6.4.4-04 Oltre ai ruoli di fiducia individuati nella norma ETSI EN 319 401 [1] (punto 7.2-15), sono supportati i ruoli di fiducia dei funzionari addetti alla registrazione e alla revoca con responsabilità definite nella norma TS 419261 [6]. Nei casi in cui il QTSP è gestito direttamente da uno Stato membro o da un organismo del settore pubblico o per suo conto, tali ruoli di fiducia aggiuntivi possono essere svolti da uno o più rappresentanti formali che agiscono per conto di funzionari addetti alla registrazione e alla revoca operanti presso le amministrazioni locali o regionali.

10) 6.4.9 Cessazione di CA o RA

— OVR-6.4.9-02 Il piano di cessazione del TSP è conforme ai requisiti stabiliti negli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014 [i.1].

11) 6.5.1 Generazione e installazione della coppia di chiavi

— OVR-6.5.1-01A La generazione della coppia di chiavi della CA è effettuata utilizzando un algoritmo conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza pubblicati dall'ENISA [7] ai fini della firma della CA.

— OVR-6.5.1-01B La lunghezza della chiave e l'algoritmo selezionati per la chiave di firma della CA sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza pubblicati dall'ENISA [7] ai fini della firma della CA.

— OVR-6.5.1-01C [CONDIZIONALE] Se la CA genera le chiavi del soggetto, le chiavi del soggetto generate dalla CA sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza pubblicati dall'ENISA [7] ai fini indicati nella CP durante il periodo di validità del certificato.

12) 6.5.2 Protezione delle chiavi private e controlli tecnici dei moduli crittografici

— GEN-6.5.2-01 Si applicano tutti i requisiti individuati nella norma ETSI EN 319 411-1 [2], punto 6.5.2, ad eccezione dei requisiti OVR-6.5.2-01, OVR-6.5.2-03 e OVR-6.5.2-04.

— GEN-6.5.2-02 La generazione della coppia di chiavi del TSP, comprese le chiavi utilizzate dai servizi di revoca e registrazione, è effettuata all'interno di un dispositivo crittografico sicuro, che è un sistema affidabile certificato conformemente a quanto segue:

  — criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, quali definiti nella norma ISO/IEC 15408 [10] o in «Common Criteria for Information Technology Security Evaluation», versione CC:2002, parti da 1 a 5, pubblicato dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security», e certificato a livello EAL 4 o superiore; o

  — sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) [8][9], e certificato a livello EAL 4 o superiore; o

  — fino al 31.12.2030, FIPS PUB 140-3 [11] livello 3.

Tale certificazione riguarda un obiettivo di sicurezza o un profilo di protezione, o la progettazione di un modulo e la documentazione di sicurezza, che soddisfano i requisiti del presente documento, sulla base di un'analisi dei rischi e tenendo conto delle misure di sicurezza fisiche e di altre misure di sicurezza non tecniche.

Se il dispositivo crittografico sicuro beneficia di una certificazione EUCC [8][9], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— GEN-6.5.2-03 La chiave di firma privata della CA è detenuta e utilizzata all'interno di un dispositivo crittografico sicuro che soddisfa i requisiti di GEN-6.5.2-01 e GEN-6.5.2-02.

13) 6.5.7 Controlli di sicurezza della rete

— OVR-6.5.7-02 La scansione delle vulnerabilità richiesta dal requisito REQ-7.8-13 della norma ETSI EN 319 401 [1] è eseguita almeno una volta a trimestre.

— OVR-6.5.7-03 Il test di penetrazione richiesto dal requisito REQ-7.8-17X della norma ETSI EN 319 401 [1] è eseguito almeno una volta all'anno.

— OVR-6.5.7-03 I firewall sono configurati in modo da impedire tutti i protocolli e gli accessi non richiesti per il funzionamento del TSP.

14) 6.6.1 Profilo del certificato

— GEN-6.6.1-05 Il certificato comprende uno degli identificativi della politica individuati in GEN-6.3.3-02 [SCELTA].

2. Per ETSI EN 319 412-3

1) 2.1 Riferimenti normativi

— [2] ETSI EN 319 412-2 V2.4.1 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons».

2) 4.2.1 Soggetto

— LEG-4.2.1-6 L'attributo organizationIdentifier contiene un identificativo dell'organizzazione interessata diverso dal nome dell'organizzazione. Se è nota l'esistenza di un numero di registrazione appropriato, l'attributo organizationIdentifier contiene un valore di tale numero di registrazione quale indicato nel corrispondente registro ufficiale che stabilisce tale numero di registrazione.

3. Per ETSI EN 319 412-2:

1) 2.1 Riferimenti normativi

— [2] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements».

— [9] Gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Meccanismi crittografici concordati» pubblicati dall'ENISA.

2) 2.2 Riferimenti informativi

— [i.7] vuoto.

3) 4.2.2 Firma

— GEN-4.2.2-2 L'algoritmo di firma è selezionato conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [9].

— NOTA vuota.

4) 4.2.3.1 Emittenti persone giuridiche

— GEN-4.2.3.1-3 Se è nota l'esistenza di un numero di registrazione appropriato, l'identità dell'emittente contiene un organizationIdentifier con un valore di tale numero di registrazione quale indicato nel corrispondente registro ufficiale che stabilisce tale numero di registrazione.

5) 4.2.5 Informazioni sulla chiave pubblica del soggetto

— GEN-4.2.5-2 La chiave pubblica del soggetto è selezionata conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [9].

— NOTA vuota.

6) 4.2.6 Numero di serie

— GEN-4.2.6-01 Il numero serialNumber del certificato (come specificato in IETF RFC 5280 [1], punto 4.1.2.2) è unico per ciascun certificato rilasciato dal TSP.