Regolamento AICT-C n. 2026-03

REGOLAMENTO TECNICO PER LA QUALIFICAZIONE DEI SERVIZI DI FIRMA ELETTRONICA, SIGILLO ELETTRONICO, VALIDAZIONE TEMPORALE E SERVIZI FIDUCIARI CONNESSI

Approvato dall'Autorità ICT-C nella seduta dell'11 settembre 2026 – In vigore dal 15 settembre 2026

TITOLO I — DISPOSIZIONI GENERALI

Art. 1

(Oggetto e finalità)

1. Il presente Regolamento definisce i requisiti tecnici, organizzativi e procedurali specifici per la qualificazione e il mantenimento dei servizi fiduciari qualificati relativi alle firme elettroniche, ai sigilli elettronici e alle validazioni temporali elettroniche prestati da operatori economici di diritto sammarinese.

2. Il Regolamento disciplina, nell'ambito di un unico quadro tecnico, i seguenti servizi, che restano distinti ai fini della qualificazione, della valutazione di conformità e dell'iscrizione negli elenchi di fiducia:

a) rilascio di certificati qualificati per firme elettroniche;

b) rilascio di certificati qualificati per sigilli elettronici;

c) servizi di convalida qualificati delle firme elettroniche qualificate e dei sigilli elettronici qualificati;

d) servizi di validazione temporale elettronica qualificata;

e) servizi fiduciari qualificati per la gestione di dispositivi qualificati per la creazione di firme elettroniche a distanza e di dispositivi qualificati per la creazione di sigilli elettronici a distanza.

3. Il presente Regolamento disciplina inoltre le funzionalità tecniche di creazione, apposizione e verifica di firme e sigilli elettronici quando esse sono comprese nel perimetro dei servizi di cui al comma 2 o sono necessarie alla loro corretta erogazione. Tali funzionalità non assumono, per il solo fatto di essere disciplinate dal presente Regolamento, uno status qualificato autonomo diverso da quello previsto dal Regolamento (UE) n. 910/2014.

4. Il presente Regolamento integra il Regolamento AICT-C n. 2026-01 – Regolamento quadro generale dei servizi fiduciari. Restano disciplinati dal Regolamento quadro i requisiti comuni del prestatore, il procedimento generale di qualificazione, la vigilanza, le sanzioni, le garanzie economiche e assicurative e gli altri obblighi non specificamente riferiti ai servizi disciplinati dal presente Regolamento.

5. Il presente Regolamento non disciplina l'accreditamento di servizi fiduciari non qualificati. Non disciplina inoltre il servizio qualificato di conservazione delle firme elettroniche qualificate e dei sigilli elettronici qualificati né il servizio di archiviazione elettronica, oggetto di distinta disciplina tecnica.

6. Il Regolamento persegue un modello tecnologicamente neutrale e basato sui risultati, evitando di imporre specifici prodotti, fornitori, infrastrutture o modelli organizzativi quando più soluzioni consentano di conseguire con equivalente affidabilità i requisiti previsti.

Art. 2

(Definizioni)

1. Ai fini del presente Regolamento si applicano le definizioni del Decreto Delegato 13 novembre 2024 n. 173 e del Regolamento (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183 e successive modifiche e integrazioni.

2. Ai soli fini redazionali del presente Regolamento si intende inoltre per:

a) famiglia FE-Q: l'insieme dei servizi qualificati elencati all'articolo 1, comma 2; tale espressione non costituisce una categoria autonoma di servizio fiduciario ai sensi del Regolamento eIDAS;

b) certificato Q-Firma: il certificato qualificato per firme elettroniche ai sensi dell'articolo 28 e dell'Allegato I del Regolamento eIDAS;

c) certificato Q-Sigillo: il certificato qualificato per sigilli elettronici ai sensi dell'articolo 38 e dell'Allegato III del Regolamento eIDAS;

d) QSCD: il dispositivo qualificato per la creazione di una firma elettronica;

e) QSealCD: il dispositivo qualificato per la creazione di un sigillo elettronico;

f) gestione remota qualificata: il servizio fiduciario qualificato di gestione di un QSCD o di un QSealCD a distanza per conto, rispettivamente, del firmatario o del creatore del sigillo;

g) RA: la funzione di registrazione incaricata delle attività di identificazione, verifica degli attributi e gestione delle richieste secondo le procedure del prestatore;

h) CA: la funzione o infrastruttura di certificazione incaricata dell'emissione e gestione dei certificati nel perimetro del prestatore;

i) TSA: la funzione o infrastruttura utilizzata per il servizio di validazione temporale elettronica;

l) servizio di convalida qualificato: il servizio di convalida di firme elettroniche qualificate o sigilli elettronici qualificati conforme agli articoli 33 e 40 del Regolamento eIDAS;

m) CAB: l'organismo di valutazione della conformità competente alla valutazione dei prestatori e dei servizi fiduciari qualificati.

Art. 3

(Perimetro e autonomia dei servizi qualificati)

1. Il prestatore definisce in modo chiaro il perimetro di ciascun servizio per il quale richiede o mantiene la qualificazione, indicando le componenti tecniche, le funzioni organizzative, le infrastrutture e gli eventuali soggetti terzi che concorrono alla sua erogazione.

2. La qualificazione di uno dei servizi della famiglia FE-Q non comporta la qualificazione automatica degli altri servizi disciplinati dal presente Regolamento.

3. La domanda, la relazione di valutazione della conformità, il provvedimento dell'Autorità ICT-C e le informazioni destinate agli elenchi di fiducia devono consentire di identificare separatamente ciascun servizio qualificato e il relativo perimetro.

4. Quando più servizi condividono la medesima infrastruttura, documentazione o organizzazione, tali elementi possono essere riutilizzati secondo il principio del fascicolo unico del prestatore, purché sia sempre individuabile la loro relazione con ciascun servizio qualificato.

5. Le funzioni tecniche accessorie, incluse le applicazioni di firma, i portali, le interfacce applicative e le componenti di orchestrazione, sono comprese nel perimetro della valutazione nella misura in cui possano incidere sulla conformità, sulla sicurezza o sull'affidabilità del servizio qualificato.

Art. 4

(Efficacia delle disposizioni sulla qualificazione)

1. Le disposizioni del presente Regolamento relative alla domanda e al conseguimento della qualificazione acquistano efficacia a seguito dell'attivazione degli elenchi di fiducia secondo quanto previsto dall'articolo 28 del Decreto Delegato n. 173/2024 e dal Regolamento quadro.

2. Prima di tale momento possono essere svolte attività tecniche e organizzative preparatorie, incluse progettazione, predisposizione delle policy, test, audit e valutazioni di conformità, senza che esse attribuiscano lo status di prestatore o servizio fiduciario qualificato.

3. La qualificazione nazionale e l'eventuale riconoscimento del servizio nel quadro europeo restano subordinati alle condizioni previste dal Decreto Delegato n. 173/2024 e dagli accordi applicabili.

TITOLO II — REQUISITI COMUNI AI SERVIZI DELLA FAMIGLIA FE-Q

Art. 5

(Documentazione del servizio)

1. Il prestatore mantiene una documentazione aggiornata che descrive il funzionamento dei servizi qualificati, le responsabilità, le procedure operative, le misure di sicurezza e le modalità con cui sono soddisfatti i requisiti applicabili.

2. Le informazioni possono essere organizzate in uno o più documenti, quali Trust Service Practice Statement, Certificate Policy, Certification Practice Statement, policy di validazione temporale, manuale del servizio, piano di sicurezza, procedure operative, schede tecniche o documentazione equivalente. Non è richiesta la duplicazione delle medesime informazioni in documenti diversi.

3. La documentazione deve consentire di comprendere almeno:

a) l'architettura e il perimetro di ciascun servizio;

b) i ruoli e le responsabilità del prestatore e degli eventuali soggetti terzi;

c) le procedure di identificazione, registrazione e gestione degli attributi, ove applicabili;

d) il ciclo di vita dei certificati e delle chiavi crittografiche;

e) le modalità di gestione dei dispositivi qualificati e delle credenziali di autenticazione, ove applicabili;

f) le modalità di revoca, sospensione e pubblicazione dello stato dei certificati;

g) le caratteristiche dei servizi di convalida e di validazione temporale eventualmente prestati;

h) le misure di sicurezza, continuità e cessazione specifiche del servizio;

i) le interfacce, i formati, i protocolli e le evidenze tecniche rilevanti ai fini dell'interoperabilità e dell'audit.

4. Le parti della documentazione necessarie agli utenti e alle parti facenti affidamento sulla certificazione per comprendere caratteristiche, responsabilità, condizioni e limiti del servizio devono essere facilmente accessibili. Le informazioni riservate relative alla sicurezza possono essere mantenute separate.

Art. 6

(Infrastruttura a chiave pubblica e gestione delle chiavi)

1. Il prestatore progetta e gestisce l'infrastruttura crittografica in modo da assicurare la riservatezza, l'integrità, l'autenticità e la disponibilità delle chiavi e delle informazioni utilizzate per l'erogazione dei servizi qualificati.

2. Le procedure relative alle chiavi del prestatore e delle componenti di servizio devono disciplinare, in relazione al rischio e al ruolo della chiave:

a) generazione, attivazione e messa in esercizio;

b) custodia, utilizzo e controllo degli accessi;

c) eventuale duplicazione e backup nei soli casi consentiti;

d) rotazione, rinnovo, sostituzione e cessazione;

e) compromissione, revoca e distruzione sicura;

f) tracciabilità delle operazioni e separazione delle funzioni critiche.

3. Le operazioni critiche sono eseguite mediante sistemi affidabili, con livelli di protezione coerenti con la funzione svolta e con gli standard richiamati dal quadro europeo. Le procedure devono impedire che una singola persona possa, senza adeguati controlli, compromettere chiavi o componenti critiche del servizio.

4. Il prestatore mantiene un processo per l'aggiornamento degli algoritmi, delle lunghezze delle chiavi e dei meccanismi crittografici, tenendo conto degli atti europei applicabili e delle indicazioni tecniche riconosciute nel quadro europeo, senza rendere dipendente il servizio da parametri non più adeguati allo stato dell'arte.

Art. 7

(Identificazione e registrazione)

1. Prima del rilascio di un certificato qualificato il prestatore verifica l'identità e, ove rilevante, gli attributi della persona o del soggetto cui il certificato si riferisce secondo l'articolo 24 del Regolamento eIDAS e l'articolo 17 del Decreto Delegato n. 173/2024.

2. Le modalità di identificazione possono essere svolte direttamente dal prestatore o tramite soggetti terzi nei casi consentiti dalla normativa applicabile. In ogni caso il prestatore qualificato mantiene la responsabilità dell'identificazione e deve poter dimostrare il metodo utilizzato, l'identità dell'operatore o del sistema che ha eseguito la verifica e le evidenze prodotte.

3. Il processo di registrazione deve garantire che i dati utilizzati per il certificato siano riconducibili alla persona o al soggetto verificato e che gli eventuali attributi, poteri di rappresentanza, qualifiche professionali o altri elementi aggiuntivi siano verificati presso fonti adeguate prima della loro inclusione.

4. Le evidenze di identificazione e registrazione sono protette da alterazioni non autorizzate, rese disponibili al CAB e all'Autorità ICT-C nei limiti delle rispettive competenze e conservate per il periodo richiesto dalla normativa applicabile.

5. Dal 19 agosto 2027, ai fini della qualificazione e del riconoscimento del servizio nel quadro europeo, la verifica dell'identità e degli attributi per il rilascio dei certificati qualificati soddisfa inoltre i requisiti e le specifiche stabiliti dal Regolamento di esecuzione (UE) 2025/1566. Il rispetto della ETSI TS 119 461 V2.1.1, con gli adattamenti previsti dal medesimo atto, costituisce il riferimento tecnico per la relativa presunzione di conformità.

Art. 8

(Registration Authority e identificazione affidata a terzi)

1. Il prestatore può organizzare la funzione di registrazione mediante una o più RA interne o esterne, anche territorialmente distribuite, purché il relativo modello sia descritto nella documentazione di servizio e rientri nel perimetro della valutazione di conformità.

2. Quando l'identificazione o altre attività di registrazione sono affidate a terzi, il prestatore:

a) definisce contrattualmente compiti, limiti, responsabilità, requisiti di sicurezza e obblighi di riservatezza;

b) assicura la formazione e l'abilitazione degli operatori e la gestione nominativa delle relative autorizzazioni;

c) mantiene il controllo delle procedure e dei criteri utilizzati;

d) può accedere alle evidenze necessarie per la verifica della conformità e per la gestione di contestazioni o incidenti;

e) prevede controlli periodici e la possibilità di sospendere o revocare l'abilitazione della RA o dei singoli operatori.

3. L'affidamento a terzi non trasferisce la responsabilità del prestatore qualificato prevista dall'articolo 17, comma 4, del Decreto Delegato n. 173/2024 e dal Regolamento eIDAS.

Art. 9

(Richiesta ed emissione dei certificati qualificati)

1. Il prestatore adotta procedure documentate per la richiesta, l'approvazione e l'emissione dei certificati qualificati.

2. Prima dell'emissione il prestatore verifica almeno:

a) il completamento dell'identificazione e delle eventuali verifiche degli attributi;

b) la corrispondenza tra il soggetto, i dati di convalida e il certificato da emettere;

c) la legittimazione del richiedente e, ove necessario, i poteri di rappresentanza;

d) l'applicazione della policy e del profilo di certificato pertinenti;

e) la disponibilità delle informazioni e dei servizi necessari alla successiva verifica dello stato del certificato.

3. L'emissione è tracciata in modo da consentire di ricostruire la richiesta, i controlli effettuati, la policy applicata, il profilo utilizzato e il momento di attivazione del certificato.

4. I certificati qualificati devono essere chiaramente distinguibili dai certificati non qualificati e contenere le indicazioni richieste dal Decreto Delegato n. 173/2024, dal Regolamento eIDAS e dagli atti di esecuzione applicabili.

Art. 10

(Profili dei certificati e attributi)

1. Ai fini della qualificazione e del riconoscimento europeo, il certificato Q-Firma è riferito al firmatario persona fisica, mentre il certificato Q-Sigillo è riferito al creatore del sigillo secondo le rispettive definizioni e requisiti del Regolamento eIDAS.

2. Le informazioni relative a organizzazioni, poteri di rappresentanza, qualifiche professionali, appartenenza a ordini o collegi, limiti d'uso, limiti di valore o Codice Operatore Economico possono essere inserite nel certificato o rese disponibili secondo le modalità ammesse dalla normativa applicabile, senza alterare la distinzione tra certificato Q-Firma e certificato Q-Sigillo.

3. Prima dell'inserimento di attributi aggiuntivi il prestatore ne verifica la pertinenza, l'esattezza e, ove richiesto, il consenso del soggetto interessato o del terzo dal quale l'attributo deriva.

4. Il prestatore dispone di una procedura per ricevere e gestire le comunicazioni relative alla modifica o al venir meno degli attributi e per adottare senza ingiustificato ritardo le misure conseguenti sul certificato.

Art. 11

(Ciclo di vita, rinnovo, sospensione e revoca)

1. Il prestatore mantiene procedure documentate per l'intero ciclo di vita del certificato, comprese attivazione, rinnovo, aggiornamento, sostituzione delle chiavi, sospensione, revoca e scadenza.

2. Il rinnovo o l'aggiornamento è preceduto dalle verifiche necessarie ad accertare che le informazioni rilevanti siano ancora valide e che le tecnologie utilizzate mantengano un livello di sicurezza adeguato.

3. La revoca e la sospensione sono gestite nei casi e con gli effetti previsti dall'articolo 16 del Decreto Delegato n. 173/2024 e dagli articoli 28 e 38 del Regolamento eIDAS. Quando è prevista la

sospensione temporanea, il relativo stato e il periodo di sospensione devono risultare verificabili attraverso il servizio di stato del certificato.

4. Un certificato qualificato revocato perde validità dal momento della revoca e non può essere ripristinato. L'eventuale sospensione non può essere utilizzata per eludere tale principio.

5. Le richieste urgenti dovute a compromissione o sospetta compromissione della chiave privata o delle credenziali di utilizzo sono gestite con modalità idonee a ridurre il rischio di utilizzi successivi non autorizzati e a produrre evidenze verificabili dell'operazione.

Art. 12

(Pubblicazione e servizi di informazione sullo stato dei certificati)

1. Il prestatore rende disponibili le informazioni necessarie a verificare la validità e lo stato dei certificati qualificati secondo modalità affidabili, interoperabili e coerenti con le policy pubblicate.

2. I servizi di stato devono consentire di determinare in modo verificabile se un certificato è valido, scaduto, revocato o, ove previsto, sospeso, e devono essere protetti contro alterazioni e risposte non autorizzate.

3. Le liste di revoca, i protocolli di stato online o le tecnologie equivalenti possono essere utilizzati singolarmente o in combinazione, purché soddisfino i requisiti normativi e gli standard applicabili e consentano alle parti facenti affidamento sulla certificazione di effettuare la verifica necessaria.

4. Il momento di pubblicazione degli stati di revoca o sospensione è documentato mediante un riferimento temporale idoneo secondo quanto previsto dall'articolo 16 del Decreto Delegato n. 173/2024.

Art. 13

(Registrazioni ed evidenze)

1. Il prestatore conserva registrazioni sufficienti a ricostruire le operazioni rilevanti effettuate durante il ciclo di vita dei certificati e degli altri servizi della famiglia FE-Q.

2. Le registrazioni comprendono, in relazione al servizio interessato, almeno le evidenze relative a identificazione e registrazione, richieste e approvazioni, emissione, gestione delle chiavi, modifiche degli attributi, revoca e sospensione, accessi amministrativi, operazioni critiche, incidenti, continuità e cessazione.

3. Le registrazioni sono protette contro cancellazioni o alterazioni non autorizzate e devono consentire di individuare il soggetto, il sistema o il ruolo che ha eseguito le operazioni rilevanti e il relativo riferimento temporale.

4. Restano fermi i periodi minimi di conservazione previsti dal Decreto Delegato n. 173/2024. In particolare, le informazioni di cui all'articolo 14, commi 3 e 5, ai sensi del comma 6 del medesimo articolo, sono conservate per almeno venti anni decorrenti dalla scadenza del certificato di firma.

5. La durata delle ulteriori registrazioni è definita nella documentazione del servizio in funzione degli obblighi legali, della vita utile delle evidenze, dei rischi e delle necessità probatorie, senza ridurre i periodi imposti dalla normativa applicabile.

Art. 14

(Informazioni al titolare, al richiedente e alle parti facenti affidamento)

1. Il prestatore rende disponibili, in forma chiara e comprensibile, le condizioni di utilizzo dei servizi, le policy applicabili, gli eventuali limiti d'uso o di valore, le responsabilità delle parti e le modalità per segnalare compromissioni o richiedere la sospensione o revoca.

2. Il titolare del certificato di firma deve essere informato degli obblighi di custodia del dispositivo o delle credenziali di autenticazione utilizzate per l'accesso a un dispositivo remoto e dell'obbligo di comunicare tempestivamente la perdita di controllo, la compromissione o l'inesattezza delle informazioni contenute nel certificato.

3. Per i certificati contenenti attributi o poteri riferibili a terzi, devono essere rese comprensibili le condizioni che determinano l'aggiornamento, la sospensione o la revoca in caso di modifica o cessazione dei relativi presupposti.

4. Restano ferme le disposizioni del Regolamento quadro relative alle condizioni contrattuali, alle limitazioni d'uso e alla responsabilità del prestatore.

Art. 15

(Fornitori tecnologici e affidamento a terzi)

1. Il prestatore può avvalersi di fornitori tecnologici, infrastrutturali o di altri soggetti terzi, inclusi servizi di infrastruttura PKI erogati come servizio, purché il perimetro delle funzioni affidate sia chiaramente definito e valutabile.

2. L'affidamento a terzi non trasferisce la responsabilità del prestatore nei confronti dell'Autorità ICT-C, degli utenti e delle parti facenti affidamento sulla certificazione per le attività comprese nel servizio qualificato.

3. Il prestatore identifica i componenti e le funzioni affidati a terzi e mantiene evidenza dei relativi accordi, dei livelli di servizio, delle misure di sicurezza, della continuità e delle modalità di accesso alle evidenze necessarie al controllo e alla valutazione di conformità.

4. Le componenti, i subfornitori e le entità affiliate che operano elementi del servizio qualificato sono incluse nel perimetro del CAB nella misura prevista dalla disciplina europea applicabile.

5. Non è richiesto che ogni fornitore tecnologico possieda autonomamente lo status di prestatore fiduciario qualificato. Tale status è richiesto quando il soggetto terzo presta direttamente un servizio per il quale il Regolamento eIDAS richiede espressamente la qualifica, fermo restando quanto previsto dal Regolamento quadro.

Art. 16

(Sicurezza, continuità e compromissione)

1. Le misure specifiche di sicurezza dei servizi della famiglia FE-Q sono coordinate con il sistema generale di gestione del rischio e della sicurezza disciplinato dal Regolamento quadro e devono proteggere in particolare le chiavi, i dispositivi qualificati, i sistemi di certificazione, le RA, i servizi di stato, i servizi di convalida e le infrastrutture di validazione temporale.

2. Il prestatore dispone di procedure per rilevare e gestire senza ingiustificato ritardo compromissioni o sospette compromissioni delle chiavi, dei dispositivi, delle credenziali, delle componenti critiche o delle fonti temporali.

3. Le procedure di continuità e ripristino devono evitare, per quanto tecnicamente possibile, la perdita delle evidenze e la creazione di risultati qualificati in condizioni non verificabili o al di fuori del perimetro autorizzato.

4. Il prestatore verifica periodicamente l'effettiva capacità di ripristinare le componenti critiche e mantiene evidenza delle prove eseguite e delle azioni correttive adottate.

TITOLO III — REQUISITI SPECIFICI DEI SINGOLI SERVIZI QUALIFICATI

Art. 17

(Certificati qualificati per firme elettroniche)

1. Il servizio di rilascio di certificati Q-Firma soddisfa i requisiti degli articoli 24 e 28 e dell'Allegato I del Regolamento eIDAS, nonché le disposizioni compatibili del Decreto Delegato n. 173/2024.

2. Ai fini della qualificazione e del riconoscimento del servizio nel quadro europeo, il servizio soddisfa inoltre i requisiti e le specifiche stabiliti dal Regolamento di esecuzione (UE) 2025/1943.

3. Ai fini della presunzione di conformità prevista dal quadro europeo, costituiscono riferimenti tecnici, con gli adattamenti stabiliti dal Regolamento di esecuzione (UE) 2025/1943:

a) ETSI EN 319 411-2 V2.6.1;

b) ETSI EN 319 412-1 V1.6.1;

c) ETSI EN 319 412-2 V2.4.1;

d) ETSI EN 319 412-5 V2.5.1;

e) gli ulteriori riferimenti normativi richiamati dal medesimo atto, tra cui ETSI EN 319 401 V3.1.1 ed ETSI EN 319 411-1 nella versione ivi prevista.

4. Il prestatore documenta il profilo dei certificati, le policy applicabili, le indicazioni di qualifica, le informazioni di stato e gli eventuali attributi aggiuntivi in modo da consentire la verifica automatizzata e l'interoperabilità previste dal quadro eIDAS.

Art. 18

(Creazione e apposizione della firma elettronica qualificata)

1. La firma elettronica qualificata è creata mediante un QSCD e si basa su un certificato Q-Firma valido secondo il Regolamento eIDAS e il Decreto Delegato n. 173/2024.

2. Le procedure di firma assicurano che i dati da sottoscrivere siano presentati al firmatario in modo chiaro e senza ambiguità prima dell'apposizione della firma e che sia acquisita la volontà di firmare, salvo i casi di firma apposta con procedura automatica disciplinati dal comma 3.

3. La firma automatica è ammessa nei limiti dell'articolo 15, comma 5, del Decreto Delegato n. 173/2024, previa autorizzazione del titolare alla procedura. L'autorizzazione, il perimetro della procedura e le condizioni che ne consentono l'esecuzione devono essere documentati e verificabili.

4. Le modalità di firma remota, massiva o riferite a una singola operazione possono essere utilizzate quando garantiscono i requisiti della firma elettronica qualificata, la protezione dei dati per la creazione della firma e l'autenticazione o autorizzazione del firmatario secondo il modello previsto dal servizio.

5. Le applicazioni utilizzate per la creazione o l'apposizione della firma non devono alterare i dati da sottoscrivere né impedire la loro corretta presentazione al firmatario quando tale presentazione è richiesta.

Art. 19

(Certificati qualificati e creazione dei sigilli elettronici)

1. Il servizio di rilascio di certificati Q-Sigillo soddisfa i requisiti degli articoli 24 e 38 e dell'Allegato III del Regolamento eIDAS.

2. Ai fini della qualificazione e del riconoscimento del servizio nel quadro europeo, il servizio soddisfa i requisiti e le specifiche stabiliti dal Regolamento di esecuzione (UE) 2025/1943.

3. Ai fini della presunzione di conformità prevista dal quadro europeo, costituiscono riferimenti tecnici, con gli adattamenti stabiliti dal medesimo atto, ETSI EN 319 411-2 V2.6.1, ETSI EN 319 412-1 V1.6.1, ETSI EN 319 412-2 V2.4.1, ETSI EN 319 412-3 V1.3.1 ed ETSI EN 319 412-5 V2.5.1, oltre agli ulteriori riferimenti normativi ivi richiamati.

4. Il sigillo elettronico qualificato è creato mediante un QSealCD e si basa su un certificato Q-Sigillo valido. Il prestatore assicura che l'utilizzo del dispositivo sia autorizzato secondo le regole organizzative del creatore del sigillo e che le relative operazioni siano tracciabili.

Art. 20

(Gestione qualificata dei dispositivi remoti)

1. La gestione a distanza di un QSCD o di un QSealCD, quando prestata come servizio qualificato, costituisce un servizio fiduciario qualificato distinto dal rilascio dei certificati qualificati e deve essere espressamente ricompresa nella domanda, nel CAR e nell'elenco di fiducia.

2. Il servizio di gestione remota qualificata soddisfa gli articoli 29a e 39a del Regolamento eIDAS e utilizza dispositivi qualificati conformi all'Allegato II, certificati secondo gli articoli 30 e 39 del medesimo Regolamento e le disposizioni applicabili.

3. La generazione o gestione dei dati per la creazione della firma o del sigillo è effettuata per conto e su richiesta del firmatario o del creatore del sigillo. L'eventuale duplicazione dei dati per finalità di backup è consentita esclusivamente nei limiti previsti dal Regolamento eIDAS, con un livello di sicurezza equivalente all'originale e nel numero minimo necessario alla continuità del servizio.

4. Il prestatore applica le condizioni contenute nel rapporto di certificazione dello specifico dispositivo remoto e mantiene la separazione tra le funzioni che consentono la gestione del dispositivo e quelle che autorizzano l'utilizzo dei dati di creazione della firma o del sigillo.

5. Dal 19 agosto 2027, ai fini della qualificazione e del riconoscimento nel quadro europeo, il servizio soddisfa inoltre il Regolamento di esecuzione (UE) 2025/1567. La ETSI TS 119 431-1 V1.3.1, con gli adattamenti ivi previsti e per il profilo applicabile, costituisce il riferimento tecnico per la relativa valutazione di conformità.

Art. 21

(Servizi di convalida qualificati)

1. Il servizio di convalida qualificato di firme elettroniche qualificate soddisfa l'articolo 33 del Regolamento eIDAS; per i sigilli elettronici qualificati si applica l'articolo 40 del medesimo Regolamento.

2. Il servizio consente alle parti facenti affidamento sulla certificazione di ricevere il risultato della convalida in modo automatizzato, affidabile ed efficiente, e il risultato è sottoscritto o sigillato dal prestatore secondo quanto previsto dal Regolamento eIDAS.

3. Ai fini della qualificazione e del riconoscimento nel quadro europeo, il servizio soddisfa i requisiti e le specifiche stabiliti dal Regolamento di esecuzione (UE) 2025/1942.

4. Ai fini della presunzione di conformità prevista dal quadro europeo, costituiscono riferimenti tecnici, con gli adattamenti stabiliti dal medesimo atto, ETSI TS 119 441 V1.2.1 ed ETSI TS 119 172-4 V1.1.1, nonché i relativi riferimenti normativi tra cui ETSI EN 319 102-1 V1.4.1 ed ETSI EN 319 401 V3.1.1.

5. Le policy e i risultati di convalida devono consentire di comprendere i controlli eseguiti, il momento della verifica, le fonti utilizzate per determinare lo stato dei certificati e l'esito complessivo secondo il modello previsto dagli standard applicabili.

Art. 22

(Validazione temporale elettronica qualificata)

1. Il servizio di validazione temporale elettronica qualificata soddisfa l'articolo 42 del Regolamento eIDAS e assicura che la data e l'ora siano collegate ai dati in modo da rendere rilevabili alterazioni

successive, utilizzando una fonte temporale accurata collegata al Tempo Universale Coordinato (UTC).

2. La validazione temporale qualificata è sottoscritta mediante firma elettronica avanzata o sigillata mediante sigillo elettronico avanzato del prestatore qualificato, oppure realizzata con altro metodo equivalente ammesso dal Regolamento eIDAS.

3. Ai fini della qualificazione e del riconoscimento del servizio nel quadro europeo, il servizio soddisfa i requisiti e le specifiche stabiliti dal Regolamento di esecuzione (UE) 2025/1929.

4. Ai fini della presunzione di conformità prevista dal quadro europeo, costituiscono riferimenti tecnici, con gli adattamenti stabiliti dal medesimo atto, ETSI EN 319 421 V1.3.1 ed ETSI EN 319 422 V1.1.1, nonché gli ulteriori riferimenti normativi ivi richiamati.

5. Il prestatore documenta le fonti temporali, la sincronizzazione, le tolleranze, i controlli, le procedure di gestione delle anomalie e le misure di continuità necessarie a dimostrare l'accuratezza e l'affidabilità del servizio.

Art. 23

(Formati e interoperabilità di firme e sigilli)

1. Il prestatore documenta i formati di firma e sigillo supportati dalle applicazioni comprese nel perimetro del servizio e le relative modalità di creazione e convalida.

2. Il presente Regolamento non impone un unico formato quando più formati consentano di soddisfare i requisiti applicabili e di conseguire l'interoperabilità dichiarata dal servizio.

3. Quando il servizio dichiara l'interoperabilità con i formati di firma e sigillo richiesti nel quadro europeo per l'accettazione da parte degli organismi del settore pubblico, si tiene conto del Regolamento di esecuzione (UE) 2026/248 e delle specifiche ivi richiamate, incluse, per i profili correnti, le famiglie XAdES, CAdES, PAdES, JAdES e ASiC.

4. Le date di applicazione e le disposizioni transitorie previste dal Regolamento di esecuzione (UE) 2026/248 sono rispettate ai fini per i quali tale atto è rilevante. Il suo richiamo non trasforma i formati ivi elencati in un requisito generale ulteriore rispetto al perimetro previsto dal Regolamento eIDAS.

TITOLO IV — QUALIFICAZIONE E VALUTAZIONE DELLA CONFORMITÀ

Art. 24

(Domanda di qualificazione e fascicolo tecnico FE-Q)

1. L'operatore che richiede la qualificazione per uno o più servizi disciplinati dal presente Regolamento presenta la domanda secondo il procedimento stabilito dal Regolamento quadro e indica puntualmente ciascun servizio per il quale richiede lo status qualificato.

2. Non devono essere nuovamente prodotti documenti comuni al prestatore già validamente acquisiti dall'Autorità ICT-C, salvo che siano scaduti, modificati o non idonei a dimostrare il requisito nel perimetro richiesto.

3. Alla domanda è associato un fascicolo tecnico FE-Q che contiene o richiama, per i servizi richiesti, almeno:

a) la descrizione del servizio e la sua riconducibilità alle categorie del Regolamento eIDAS;

b) l'architettura logica e il perimetro tecnico, con individuazione delle componenti e dei flussi rilevanti;

c) la documentazione di servizio di cui all'articolo 5;

d) l'organizzazione delle CA, RA, TSA, funzioni di convalida e gestione remota, ove pertinenti;

e) le procedure di identificazione, registrazione e verifica degli attributi;

f) le procedure e le evidenze di gestione delle chiavi e delle operazioni critiche;

g) i profili dei certificati, le policy applicabili e le informazioni destinate alle parti facenti affidamento sulla certificazione;

h) le procedure di emissione, rinnovo, sospensione, revoca e informazione sullo stato dei certificati;

i) le evidenze relative ai QSCD o QSealCD e alla loro certificazione, ove applicabili;

l) la documentazione specifica dei servizi di gestione remota, convalida o validazione temporale richiesti;

m) l'elenco dei fornitori, subfornitori e componenti esterni rilevanti, con le funzioni affidate;

n) le evidenze di test, collaudi, audit, prove di continuità e verifiche di sicurezza pertinenti;

o) le informazioni e gli identificativi tecnici necessari all'iscrizione del servizio negli elenchi di fiducia;

p) il CAR emesso dal CAB e gli eventuali rapporti tecnici di supporto richiesti dalla disciplina applicabile.

4. La documentazione può fare riferimento a sistemi, certificazioni, procedure o evidenze comuni a più servizi, purché sia chiaramente individuato il rapporto con ciascun servizio sottoposto a qualificazione.

Art. 25

(Perimetro del CAB e relazione di valutazione della conformità)

1. La valutazione di conformità è effettuata da un CAB competente e accreditato per il perimetro dei servizi qualificati oggetto della domanda.

2. Ai fini della qualificazione e del riconoscimento nel quadro europeo, la relazione di valutazione della conformità è redatta secondo il Regolamento di esecuzione (UE) 2025/2162 e il relativo schema di riferimento, che richiama ETSI EN 319 403-1 V2.3.1.

3. Il CAR identifica almeno il prestatore, i singoli servizi qualificati valutati, il relativo perimetro, le identità tecniche dei servizi, le componenti rilevanti e, ove applicabile, le controllate, entità affiliate, contraenti e subcontraenti che operano componenti comprese nella valutazione.

4. La presenza di più servizi nel medesimo CAR è ammessa quando il documento consente di determinare senza ambiguità l'esito della valutazione per ciascun servizio. La conformità di un servizio non si estende automaticamente agli altri.

5. Certificazioni e audit ulteriori possono costituire evidenze di supporto se pertinenti, ma non sostituiscono il CAR richiesto dal Regolamento eIDAS.

Art. 26

(Notifica, iscrizione e avvio del servizio qualificato)

1. Il procedimento di qualificazione è coordinato con il Regolamento quadro, con l'articolo 28 del Decreto Delegato n. 173/2024 e con gli articoli 21 e 22 del Regolamento eIDAS.

2. Ai fini dell'allineamento al procedimento europeo, la domanda e le verifiche tengono conto del Regolamento di esecuzione (UE) 2025/1572, applicabile nell'Unione europea a decorrere dal 19 agosto 2026, con particolare riferimento all'individuazione dei singoli servizi, degli identificativi destinati all'elenco di fiducia, del CAR, degli eventuali rapporti tecnici e del piano di cessazione.

3. Il servizio non può essere presentato né avviato come qualificato prima che lo status qualificato sia validamente attribuito e registrato nell'elenco di fiducia competente secondo la disciplina applicabile.

4. L’eventuale inserimento e riconoscimento del servizio sammarinese nel sistema europeo delle Trusted List resta subordinato alle condizioni e agli accordi previsti dall’articolo 28 del Decreto Delegato n. 173/2024.

Art. 27

(Riuso delle evidenze tra più servizi qualificati)

1. Quando il medesimo prestatore richiede o mantiene la qualificazione per più servizi della famiglia FE-Q, le evidenze comuni possono essere acquisite e gestite una sola volta, secondo il principio del fascicolo unico previsto dal Regolamento quadro.

2. Possono essere riutilizzate, quando ancora valide e pertinenti, le evidenze relative a organizzazione, sicurezza generale, gestione del rischio, infrastruttura condivisa, fornitori, continuità, procedure di change management e altre componenti comuni.

3. Il riuso non riduce i requisiti applicabili al singolo servizio e non consente di estendere automaticamente il perimetro o l’esito del CAR oltre quanto espressamente valutato dal CAB.

4. Le eventuali differenze tra i servizi devono essere documentate come requisiti, procedure ed evidenze specifiche del relativo fascicolo tecnico.

Art. 28

(Valutazioni periodiche e modifiche rilevanti)

1. Il prestatore mantiene la conformità dei servizi per l’intera durata della qualificazione e si sottopone alle valutazioni periodiche previste dall’articolo 20 del Regolamento eIDAS e dalla disciplina europea applicabile.

2. Il prestatore dispone di una procedura per identificare e valutare preventivamente le modifiche che possono incidere sul perimetro o sulla conformità dei servizi, comprese in particolare modifiche a:

a) gerarchie di certificazione e chiavi critiche;

b) dispositivi qualificati, HSM o piattaforme di gestione remota;

c) procedure di identificazione e RA;

d) servizi di stato, convalida e validazione temporale;

e) algoritmi e meccanismi crittografici;

f) fornitori, subfornitori o infrastrutture critiche;

g) identità tecniche dei servizi destinate agli elenchi di fiducia.

3. Le modifiche rilevanti sono comunicate al CAB e all’Autorità ICT-C nei casi e nei termini previsti dal Regolamento eIDAS, dagli atti di esecuzione applicabili e dal Regolamento quadro, unitamente alle evidenze necessarie a valutarne l’impatto.

Art. 29

(Cessazione dei servizi FE-Q)

1. La cessazione di uno o più servizi FE-Q è gestita secondo il Decreto Delegato n. 173/2024, il Regolamento quadro, l’articolo 24 del Regolamento eIDAS e gli atti europei applicabili.

2. Il piano di cessazione deve considerare, in relazione al servizio interessato:

a) la revoca o il trasferimento dei certificati ancora validi e la continuità dei servizi di stato;

b) la conservazione e l’accessibilità delle registrazioni e delle evidenze necessarie alla verifica successiva;

c) la gestione e la distruzione sicura delle chiavi e dei dati di creazione del prestatore che non debbano più essere utilizzati;

d) la cessazione delle capacità di generare nuovi risultati qualificati dopo la data prevista;

e) la gestione dei dispositivi remoti e delle credenziali degli utenti, ove applicabile;

f) la continuità delle informazioni necessarie a verificare firme, sigilli, certificati e validazioni temporali già prodotti;

g) l'eventuale trasferimento a un prestatore sostitutivo e le modalità per evitare interruzioni non documentate.

3. Il piano è mantenuto aggiornato e riesaminato secondo i requisiti del Regolamento di esecuzione (UE) 2025/2530, per quanto rilevante ai fini della qualificazione e del riconoscimento europeo.

TITOLO V — VIGILANZA E DISPOSIZIONI FINALI

Art. 30

(Evidenze specifiche per la vigilanza)

1. Nell'ambito delle attività di vigilanza disciplinate dal Regolamento quadro, il prestatore deve poter produrre le evidenze specifiche necessarie a verificare la conformità dei servizi FE-Q.

2. In relazione al servizio interessato, tali evidenze comprendono almeno:

a) versioni vigenti delle policy e dei practice statement;

b) profili dei certificati e configurazioni rilevanti;

c) registrazioni relative a emissione, sospensione e revoca;

d) evidenze di identificazione e dei controlli sulle RA;

e) registri delle operazioni critiche e delle cerimonie di chiave;

f) evidenze di certificazione dei dispositivi qualificati e di gestione dei dispositivi remoti;

g) rapporti e risultati dei servizi di convalida e dei controlli temporali, ove applicabili;

h) prove di continuità, ripristino e gestione delle compromissioni;

i) CAR, rapporti tecnici e risultanze delle valutazioni periodiche;

l) documentazione delle modifiche rilevanti e delle azioni correttive.

3. L'Autorità ICT-C tiene conto delle evidenze già prodotte al CAB o già nella propria disponibilità e ne evita la richiesta duplicata quando siano ancora valide e pertinenti.

Art. 31

(Atti europei e standard tecnici di riferimento)

1. Ai fini della qualificazione e del riconoscimento dei servizi disciplinati dal presente Regolamento nel quadro europeo, sono considerati, secondo il rispettivo ambito, gli atti di esecuzione adottati in attuazione del Regolamento eIDAS, inclusi:

a) Regolamento di esecuzione (UE) 2025/2530, relativo ai requisiti per i prestatori di servizi fiduciari qualificati;

b) Regolamento di esecuzione (UE) 2025/1943, relativo ai certificati qualificati per firme elettroniche e sigilli elettronici;

c) Regolamento di esecuzione (UE) 2025/1942, relativo ai servizi di convalida qualificati;

d) Regolamento di esecuzione (UE) 2025/1929, relativo ai servizi di validazione temporale qualificata;

e) Regolamento di esecuzione (UE) 2025/1566, relativo alla verifica dell'identità e degli attributi, applicabile dal 19 agosto 2027;

f) Regolamento di esecuzione (UE) 2025/1567, relativo alla gestione dei dispositivi qualificati a distanza, applicabile dal 19 agosto 2027;

g) Regolamento di esecuzione (UE) 2025/2162, relativo alla valutazione della conformità e ai CAR;

h) Regolamento di esecuzione (UE) 2025/1572, relativo alla notifica dell'intenzione e alle verifiche per l'avvio dei servizi fiduciari qualificati;

i) Regolamento di esecuzione (UE) 2025/1570, relativo alla notifica delle informazioni sui dispositivi qualificati certificati;

l) Decisione di esecuzione (UE) 2016/650, nella misura in cui resta vigente e pertinente alla valutazione di sicurezza dei dispositivi qualificati;

m) Regolamento di esecuzione (UE) 2026/248, per i profili di firma e sigillo e le finalità di interoperabilità cui esso si riferisce.

2. Gli standard ETSI e le specifiche tecniche richiamati dagli atti di cui al comma 1 costituiscono riferimento per la presunzione di conformità o per la valutazione tecnica esclusivamente nei termini, nelle versioni e con gli adattamenti previsti dai rispettivi atti.

3. Una versione successiva di uno standard non sostituisce automaticamente la versione richiamata da un atto europeo ai fini della presunzione di conformità. L'eventuale uso di versioni o soluzioni alternative deve essere gestito secondo quanto consentito dalla disciplina applicabile e deve essere supportato da evidenze idonee a dimostrare il soddisfacimento dei requisiti.

4. L'Autorità ICT-C può mantenere e pubblicare un elenco ricognitivo degli atti e degli standard applicabili, aggiornato all'evoluzione del quadro europeo, senza modificare con tale elenco la natura o gli effetti giuridici delle fonti richiamate.

Art. 32

(Coordinamento con la disciplina sammarinese preesistente)

1. Restano ferme le disposizioni della Legge 20 luglio 2005 n. 115 nei limiti e secondo il coordinamento previsto dal Decreto Delegato n. 173/2024.

2. Le disposizioni tecniche del Decreto 8 novembre 2005 n. 156 continuano a costituire riferimento per gli aspetti non diversamente disciplinati, purché compatibili con il Decreto Delegato n. 173/2024, con il Regolamento eIDAS come successivamente modificato e con gli atti europei considerati ai fini della qualificazione e del riconoscimento del servizio.

3. Quando una materia è disciplinata da requisiti europei più recenti espressamente richiamati ai fini della qualificazione, il prestatore struttura il servizio secondo tali requisiti, fermo restando il rispetto delle disposizioni sammarinesi non incompatibili e degli ulteriori obblighi di legge vigenti.

4. Il presente articolo ha funzione di coordinamento tecnico e non determina abrogazioni o modifiche di fonti di rango superiore.

Art. 33

(Entrata in vigore e aggiornamento)

1. Il presente Regolamento entra in vigore il 15 settembre 2026, fermo restando quanto stabilito dall'articolo 4 in relazione all'efficacia delle disposizioni sulla qualificazione.

2. L'Autorità ICT-C cura la pubblicazione del presente Regolamento sul proprio sito istituzionale.

3. Le modifiche degli atti europei e degli standard tecnici sono recepite o coordinate secondo le modalità previste dal Regolamento quadro e dalle competenze attribuite all'Autorità ICT-C, preservando per quanto possibile la continuità delle qualificazioni e la neutralità tecnologica.

4. Per quanto non espressamente disciplinato dal presente Regolamento si applicano il Decreto Delegato n. 173/2024, il Regolamento AICT-C n. 2026-01 e, ai fini della qualificazione e del riconoscimento nel quadro europeo, il Regolamento eIDAS e gli atti europei pertinenti.