AUTORITÀ ICT-C

Verbale n. 3/2026

Il giorno 11 settembre 2026, alle ore 19:30, si è riunita in via straordinaria l'Autorità ICT-C in videoconferenza.

Presenti: Stefano Salsano (Presidente), Matteo Botteghi, Corrado Giustozzi, Gherardo Marrapese e Laura Rovizzi.

1. Approvazione dei regolamenti in materia di servizi fiduciari.

Il Presidente illustra i regolamenti in materia di servizi fiduciari predisposti nell'ambito del Tavolo di confronto di cui all'art. 29 del Decreto Delegato 13 novembre 2024 n. 173, quali norme tecniche la cui redazione è affidata all'Autorità dal medesimo Decreto Delegato. Segue discussione.

L'Autorità approva all'unanimità dei presenti i seguenti regolamenti: Regolamento AICT-C n. 2026-01 – Regolamento quadro generale dei servizi fiduciari (Allegato A); Regolamento AICT-C n. 2026-02 – Regolamento tecnico per l'accreditamento e la qualificazione dei servizi di archiviazione elettronica (Allegato B); Regolamento AICT-C n. 2026-03 – Regolamento tecnico per la qualificazione dei servizi di firma elettronica, sigillo elettronico, validazione temporale e servizi fiduciari connessi (Allegato C). I regolamenti entrano in vigore il 15 settembre 2026.

L'Autorità dispone la pubblicazione dei regolamenti sul sito istituzionale e la loro trasmissione, tramite la Segreteria di Stato, al Congresso di Stato per la presa d'atto prevista dal Decreto Delegato n. 173/2024. Il Presidente è autorizzato a recepire, prima della pubblicazione, eventuali correzioni di meri errori materiali, senza alterazione del contenuto dei testi.

La riunione termina alle ore 20:15 dell'11 settembre 2026.

Il Presidente dell'Autorità ICT-C

Prof. Stefano Salsano

STEFANO
DOMENICO
SALSANO
14.09.2026
09:27:24
GMT+02:00

REPUBBLICA DI SAN MARINO
via 28 Luglio, 192 - 47893 Borgo Maggiore
T +378 (0549) 882 552
info@autoritaict.sm

ALLEGATO A

Regolamento AICT-C n. 2026-01

Regolamento quadro generale dei servizi fiduciari

REPUBBLICA DI SAN MARINO
via 28 Luglio, 192 - 47893 Borgo Maggiore
T +378 (0549) 882 552
info@autoritaict.sm

Regolamento AICT-C n. 2026-01

REGOLAMENTO QUADRO GENERALE DEI SERVIZI FIDUCIARI

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 disciplina i criteri, le modalità e i requisiti per l'accreditamento, l'iscrizione e la permanenza:

a) negli elenchi dei prestatori di servizi di pubblica utilità di cui all'articolo 22, comma 7, del Decreto Delegato 13 novembre 2024 n. 173;

b) negli elenchi di fiducia dei prestatori di servizi fiduciari qualificati di cui all'articolo 8, comma 1, lettera dd), del Decreto Delegato 20 novembre 2018 n. 146, come successivamente modificato e integrato.

2. Il regolamento definisce, inoltre, i criteri generali per la vigilanza e il controllo sui prestatori iscritti ai già menzionati elenchi da parte dell'Autorità ICT-C, nel rispetto delle competenze ad essa attribuite dal Decreto Delegato 20 novembre 2018 n. 146, come successivamente modificato e integrato.

Art. 2

(Riferimenti normativi)

1. Il presente regolamento si applica in attuazione e nel rispetto di:

a) il Regolamento (UE) n. 910/2014 (eIDAS), come recepito nell'ordinamento sammarinese dal Decreto Delegato 13 novembre 2024 n. 173;

b) il Decreto Delegato 20 novembre 2018 n. 146, come successivamente modificato e integrato, in particolare dal Decreto Delegato 20 novembre 2020 n. 204;

c) ogni ulteriore disposizione sammarinese vigente in materia di servizi fiduciari, sviluppo digitale e trattamento dei dati personali.

2. Per quanto non espressamente disciplinato dal presente regolamento, si applicano le disposizioni del Regolamento (UE) n. 910/2014, degli atti europei applicabili e, nei termini da essi previsti, degli standard tecnici pertinenti, nonché delle eventuali circolari tecniche adottate dall'Autorità ICT-C nell'esercizio delle competenze attribuite dal Decreto Delegato n. 173/2024 e dall'articolo 12, comma 1, lettere d) e h), del Decreto Delegato 20 novembre 2018 n. 146, come successivamente modificato e integrato.

Art. 3

(Definizioni)

1. Ai fini del presente regolamento si applicano le definizioni:

a) di cui all'articolo 3 del Regolamento (UE) n. 910/2014;

b) di cui all'articolo 2 del Decreto Delegato n. 173/2024;

c) di cui agli articoli 7 e 8 del Decreto Delegato 20 novembre 2018 n. 146, come successivamente modificato e integrato.

2. Per “prestatori di servizi fiduciari non qualificati” e “prestatori di servizi fiduciari qualificati” si intendono i soggetti definiti, rispettivamente, agli articoli 19 e 25 del Decreto Delegato n. 173/2024.

3. Ai fini del presente regolamento si intende inoltre per:

a) CAB (Conformity Assessment Body): organismo di valutazione della conformità accreditato da un organismo nazionale di accreditamento ai sensi del Regolamento (CE) n. 765/2008, secondo la disciplina prevista dal Regolamento di esecuzione (UE) 2025/2162, e il cui ambito di accreditamento comprende il prestatore e la tipologia di servizio fiduciario qualificato oggetto della valutazione;

b) CAR (Conformity Assessment Report): la relazione di valutazione della conformità rilasciata da un CAB, relativa al prestatore e ai servizi fiduciari qualificati oggetto della valutazione;

c) fascicolo unico del prestatore: modalità di gestione della documentazione comune al prestatore che consente il riuso, nei diversi procedimenti di accreditamento o qualificazione, dei documenti e delle evidenze già validamente acquisiti dall’Autorità ICT-C, quando risultino ancora validi, aggiornati e pertinenti, evitando duplicazioni non necessarie.

TITOLO II — REQUISITI COMUNI PER TUTTI I PRESTATORI

Art. 4

(Ambito soggettivo)

1. Le disposizioni del presente Titolo si applicano a tutti i prestatori di servizi fiduciari che richiedono l’iscrizione o risultano iscritti:

a) negli elenchi dei prestatori di servizi di pubblica utilità di cui all’articolo 22, comma 7, del Decreto Delegato n. 173/2024;

b) negli elenchi di fiducia dei prestatori di servizi fiduciari qualificati di cui all’articolo 8, comma 1, lettera dd), del Decreto Delegato n. 146/2018, come successivamente modificato e integrato.

2. Ulteriori requisiti specifici si applicano, per ciascuna tipologia di servizio, secondo quanto previsto nei successivi Titoli del presente regolamento.

Art. 5

(Requisiti societari e di autorizzazione all’esercizio)

1. Il prestatore deve essere un operatore economico di diritto sammarinese, regolarmente autorizzato all’esercizio dell’attività.

2. L’oggetto sociale o l’attività esercitata deve essere coerente con i servizi fiduciari e/o i servizi ICT per i quali è richiesta l’iscrizione negli elenchi.

Art. 6

(Requisiti finanziari minimi)

1. Il prestatore deve disporre di mezzi finanziari adeguati alla natura, al volume e al tipo di servizi fiduciari offerti, anche al fine di garantire l’adempimento delle responsabilità derivanti dall’erogazione dei servizi stessi.

2. Ai fini dell’iscrizione negli elenchi di fiducia dei prestatori di servizi fiduciari qualificati, il prestatore deve dimostrare:

a) un capitale sociale non inferiore a euro 500.000 (cinquecentomila);

b) di garanzie assicurative adeguate e proporzionate ai livelli dei servizi offerti.

Art. 7

(Requisiti organizzativi, funzioni minime e nomine esterne)

1. Il prestatore deve dotarsi di una struttura organizzativa adeguata, proporzionata alla complessità e al volume dei servizi fiduciari offerti, in grado di assicurare il rispetto dei requisiti previsti dalla normativa vigente e dagli standard tecnici applicabili.

2. Devono essere individuate e formalmente attribuite, anche cumulativamente alla medesima persona fisica o unità organizzativa, almeno le seguenti funzioni minime:

a) funzione di gestione del servizio, responsabile della pianificazione, dell'erogazione e del monitoraggio dei servizi fiduciari;

b) funzione di sicurezza delle informazioni, responsabile della definizione e dell'attuazione delle misure di sicurezza tecniche e organizzative, nonché della gestione degli incidenti;

c) funzione di controllo interno o audit interno;

d) per i servizi che lo richiedono, funzione di gestione delle chiavi crittografiche e dell'infrastruttura a chiave pubblica (PKI).

3. L'organo amministrativo del prestatore individua e nomina i responsabili delle funzioni di cui al precedente comma, potendo affidarne lo svolgimento, in tutto o in parte, a soggetti esterni all'organizzazione, nel rispetto dei seguenti principi:

a) la responsabilità ultima verso l'Autorità ICT-C e verso i terzi permane in capo all'organo amministrativo del prestatore;

b) i rapporti con i soggetti esterni devono essere regolati da contratti scritti che definiscono con chiarezza compiti, limiti, livelli di servizio, obblighi di riservatezza e modalità di collaborazione con l'Autorità ICT-C;

c) per le funzioni critiche esternalizzate, il prestatore assicura che il soggetto incaricato possieda competenze, affidabilità e requisiti adeguati alla funzione svolta, fermo restando quanto eventualmente previsto dalle norme tecniche relative al singolo servizio;

d) qualora il soggetto esterno eroghi direttamente un servizio fiduciario per il quale la normativa applicabile richiede lo status qualificato, esso deve possedere tale status;

e) il prestatore deve garantire in ogni momento la disponibilità effettiva delle funzioni esternalizzate e la possibilità per l'Autorità ICT-C di interloquire con i soggetti incaricati.

4. Il prestatore assicura che l'Autorità ICT-C disponga di interlocutori chiaramente individuati per ciascuna delle funzioni di cui al secondo comma, interni o esterni, comunicandone i riferimenti in sede di accreditamento e aggiornandoli in caso di variazione.

5. L'assetto delle funzioni, dei responsabili e delle eventuali esternalizzazioni è descritto in apposita documentazione interna, inclusa o richiamata nella documentazione di servizio e messo a disposizione dell'Autorità ICT-C su richiesta.

Art. 8

(Conformità a standard tecnici)

1. Il prestatore deve conformarsi agli standard tecnici internazionali applicabili ai servizi fiduciari erogati, con particolare riferimento agli standard ETSI della serie EN 319 relativi ai prestatori di servizi fiduciari e ai servizi qualificati ai sensi del Regolamento (UE) n. 910/2014, nei casi e nei termini in cui il loro rispetto è richiesto dalla normativa applicabile.

2. Negli altri casi, gli standard tecnici richiamati dalla normativa europea costituiscono riferimento ai fini della presunzione di conformità o della valutazione tecnica, secondo quanto previsto dalla disciplina applicabile.

3. L’Autorità ICT-C indica, con proprie norme tecniche, circolari tecniche o prassi, l’elenco degli standard tecnici applicabili e le relative versioni, tenuto conto dell’evoluzione del quadro europeo e delle migliori pratiche internazionali.

4. In sede di accreditamento e di vigilanza, il prestatore deve essere in grado di dimostrare la propria conformità ai requisiti applicabili, anche mediante il rispetto degli standard tecnici pertinenti, mediante idonea documentazione, certificazioni, rapporti di audit o altre evidenze oggettive.

Art. 9

(Oneri a carico dei prestatori)

1. Per l’iscrizione e il mantenimento negli elenchi dei prestatori di servizi di pubblica utilità si applicano le disposizioni di cui all’articolo 24 del Decreto Delegato 13 novembre 2024 n. 173.

2. In sede di prima applicazione e fino al 31 dicembre 2027, la tassa di iscrizione negli elenchi di fiducia è stabilita in euro 5.000 (cinquemila) per il primo servizio fiduciario qualificato e in euro 1.000 (mille) per ciascun ulteriore servizio fiduciario qualificato del medesimo prestatore.

3. La tassa è versata a seguito dell’accoglimento della domanda di qualificazione e prima dell’iscrizione del relativo servizio nell’elenco di fiducia. L’Autorità ICT-C rende pubbliche sul proprio sito istituzionale le modalità operative di pagamento.

4. Gli importi applicabili successivamente al 31 dicembre 2027 sono stabiliti dall’Autorità ICT-C con norma tecnica.

Art. 10

(Responsabilità del prestatore)

1. Il prestatore rende chiaramente riconoscibili nel contratto di fornitura all’utenza i limiti d’uso e gli ambiti di applicazione dei servizi erogati. Il prestatore di servizi fiduciari non qualificato rende altresì chiaramente riconoscibili i livelli minimi di fornitura del servizio (Service Level Agreement – SLA).

2. Per i prestatori di servizi fiduciari non qualificati, l’onere di dimostrare il dolo o la negligenza del prestatore ricade sulla persona fisica o giuridica che denuncia il danno.

3. Il prestatore di servizi fiduciari non qualificato non è responsabile per i danni causati dalla fruizione dei servizi al di fuori dei limiti d’uso o degli ambiti di applicazione di cui al primo comma.

4. Per i prestatori di servizi fiduciari qualificati si presume il dolo o la negligenza ai sensi dell’articolo 13 del Regolamento eIDAS, salvo che il prestatore dimostri che il danno non è originato da un mancato adempimento degli obblighi di legge ovvero che la fruizione del servizio è avvenuta al di fuori dei limiti d’uso o degli ambiti di applicazione indicati nel contratto.

5. Il prestatore garantisce il rispetto della Legge 21 dicembre 2018 n. 171 e successive modifiche in materia di protezione dei dati personali.

TITOLO III — ACCREDITAMENTO AGLI ELENCHI DI PUBBLICA UTILITÀ (NON QUALIFICATI)

Art. 11

(Ambito di applicazione del Titolo)

1. Il presente Titolo disciplina i requisiti e il procedimento per l’accreditamento, l’iscrizione e la permanenza negli elenchi dei prestatori di servizi di pubblica utilità di cui all’articolo 22, comma 7, del Decreto Delegato 13 novembre 2024 n. 173, ai quali sono equiparati i prestatori di servizi fiduciari non qualificati ai sensi dell’articolo 19 del medesimo decreto.

Art. 12

(Domanda di accreditamento)

1. L’operatore economico che intende essere iscritto negli elenchi dei prestatori di servizi di pubblica utilità presenta all’Autorità ICT-C apposita domanda di accreditamento, indicando le lettere dell’articolo 22, comma 7, del Decreto Delegato 13 novembre 2024 n.173 per le quali richiede l’iscrizione e specificando i servizi fiduciari che intende erogare.

2. La domanda deve consentire all’Autorità ICT-C di verificare la sussistenza dei requisiti soggettivi, organizzativi, tecnici e finanziari previsti dal presente regolamento.

3. Alla domanda sono allegati almeno i seguenti documenti:

a) copia dell’atto costitutivo e dello statuto vigenti, ove applicabili;

b) documentazione attestante la regolare autorizzazione all’esercizio dell’attività;

c) ultimi bilanci approvati, se disponibili, o documentazione equivalente per i soggetti di nuova costituzione, ai fini della verifica dei requisiti finanziari;

d) descrizione dei servizi fiduciari che si intendono erogare, con evidenza della loro riconducibilità alle lettere dell’articolo 22, comma 7, del Decreto Delegato n. 173/2024;

e) descrizione sintetica dell’assetto organizzativo e delle funzioni minime di cui all’articolo 7 del presente regolamento, con indicazione dei relativi responsabili e delle eventuali esternalizzazioni;

f) documentazione di servizio (ad esempio, Trust Service Practice Statement o documento equivalente) nella parte già disponibile alla data della domanda;

g) descrizione delle principali misure di sicurezza, dei presìdi di continuità operativa e delle coperture assicurative a supporto dei servizi per cui è richiesto l’accreditamento;

h) relazione tecnica indipendente, redatta da un soggetto terzo dotato di adeguate competenze rispetto al servizio oggetto della domanda, contenente una valutazione della conformità del servizio ai requisiti applicabili e le eventuali evidenze tecniche a supporto.

Art. 13

(Istruttoria e decisione sull’accreditamento)

1. L’Autorità ICT-C verifica la completezza della domanda e della documentazione allegata e può richiedere integrazioni, chiarimenti o ulteriori documenti ritenuti necessari ai fini dell’istruttoria, fermo restando il termine previsto dall’articolo 23 del Decreto Delegato 13 novembre 2024 n. 173.

2. L’istruttoria è svolta secondo principi di trasparenza, proporzionalità e non discriminazione e può includere verifiche tecniche e organizzative sui sistemi utilizzati per l’erogazione dei servizi fiduciari.

3. Nel corso dell’istruttoria l’Autorità ICT-C valuta la sussistenza dei requisiti comuni di cui al Titolo precedente e dei requisiti specifici eventualmente stabiliti con proprie norme tecniche, circolari tecniche o prassi per ciascuna tipologia di servizio ricompresa negli elenchi di pubblica utilità.

4. L’Autorità ICT-C conclude l’istruttoria e adotta il provvedimento motivato entro 30 giorni dalla presentazione della domanda. Qualora il provvedimento non sia adottato entro il termine previsto, il richiedente può ricorrere ai sensi dell’articolo 10, comma 2, della Legge n. 68/1989.

5. L’Autorità ICT-C può effettuare, direttamente o tramite soggetti da essa incaricati, verifiche documentali e, ove necessario, ispezioni presso il prestatore o i suoi fornitori rilevanti, al fine di accertare la concreta attuazione dei requisiti dichiarati.

6. All’esito dell’istruttoria, l’Autorità ICT-C adotta un provvedimento motivato di accoglimento o rigetto della domanda. In caso di accoglimento, il prestatore è iscritto negli elenchi dei prestatori di servizi di pubblica utilità, con indicazione puntuale delle lettere dell’articolo 22, comma 7, del Decreto Delegato n. 173/2024 per le quali è accreditato.

Art. 14

(Requisiti specifici per i servizi di pubblica utilità)

1. Per ciascuna lettera dell'articolo 22, comma 7, del Decreto Delegato n. 173/2024, l'Autorità ICT-C definisce, con proprie norme tecniche, circolari tecniche o prassi, i requisiti specifici aggiuntivi rispetto a quelli comuni previsti dal presente regolamento, tenendo conto:

a) della natura tecnica del servizio e dei relativi rischi;

b) delle disposizioni del Regolamento (UE) n. 910/2014 e degli atti europei applicabili;

c) degli standard tecnici indicati ai sensi dell'articolo 8 del presente regolamento;

d) delle migliori pratiche adottate a livello europeo per servizi analoghi.

2. I prestatori iscritti negli elenchi dei servizi di pubblica utilità devono conformarsi ai requisiti specifici stabiliti dall'Autorità ICT-C per ciascun servizio per il quale risultano accreditati e mantenere tale conformità per tutta la durata dell'iscrizione.

TITOLO IV — ACCREDITAMENTO AGLI ELENCHI DI FIDUCIA (QUALIFICATI)

Art. 15

(Ambito di applicazione del Titolo)

1. Le disposizioni del presente Titolo, nonché le altre disposizioni del presente regolamento riferite esclusivamente ai prestatori di servizi fiduciari qualificati e agli elenchi di fiducia, acquistano efficacia a decorrere dall'attivazione degli elenchi di fiducia ai sensi dell'articolo 28 del Decreto Delegato n. 173/2024. Fino a tale momento l'Autorità ICT-C rifiuta le domande di qualificazione.

2. Prima dell'attivazione degli elenchi di fiducia, gli operatori possono tuttavia trasmettere all'Autorità ICT-C documentazione e fascicoli preparatori relativi ai servizi per i quali intendono successivamente richiedere la qualificazione. L'Autorità ICT-C può svolgere verifiche preliminari e richiedere integrazioni ai fini della preparazione del successivo procedimento. Tali attività non costituiscono domanda di qualificazione, non determinano la decorrenza dei termini di cui all'articolo 25 del Decreto Delegato n. 173/2024, non attribuiscono alcuno status qualificato e non vincolano la successiva valutazione dell'Autorità ICT-C o del CAB.

3. La documentazione già acquisita può essere riutilizzata nel successivo procedimento di qualificazione quando ancora valida, aggiornata e pertinente.

Art. 16

(Domanda di qualificazione quale prestatore di servizi fiduciari qualificati)

1. L'operatore economico che intende ottenere la qualificazione quale prestatore di servizi fiduciari qualificati presenta all'Autorità ICT-C apposita domanda, indicando i servizi fiduciari per i quali richiede la qualificazione e la corrispondente riconducibilità alle categorie previste dal Regolamento (UE) n. 910/2014.

2. Alla domanda sono allegati almeno i seguenti documenti:

a) copia dell'atto costitutivo e dello statuto vigenti;

b) documentazione attestante la regolare autorizzazione all'esercizio dell'attività, in conformità all'articolo 5 del presente regolamento;

c) documentazione idonea a dimostrare il possesso dei requisiti finanziari e assicurativi di cui all'articolo 6;

d) descrizione dettagliata dei servizi fiduciari che si intendono erogare in forma qualificata, con evidenza della loro riconducibilità alle tipologie previste dal Regolamento (UE) n. 910/2014 e dal Decreto Delegato n. 173/2024;

e) descrizione dell'assetto organizzativo e delle funzioni minime di cui all'articolo 7, con indicazione dei relativi responsabili e delle eventuali esternalizzazioni, nonché delle modalità di coordinamento complessivo dei servizi fiduciari qualificati;

f) documentazione di servizio e ulteriori evidenze tecniche previste dai regolamenti tecnici applicabili ai singoli servizi fiduciari per i quali è richiesta la qualificazione;

g) descrizione delle principali misure di sicurezza, dei presìdi di gestione del rischio, di continuità operativa e disaster recovery, nonché delle coperture assicurative a supporto dei servizi per cui è richiesta la qualificazione;

h) CAR rilasciato da un CAB competente e accreditato per il perimetro dei servizi fiduciari qualificati oggetto della domanda.

3. Non devono essere nuovamente prodotti documenti o evidenze già validamente acquisiti dall'Autorità ICT-C, quando risultino ancora validi, aggiornati e pertinenti ai fini della qualificazione richiesta.

Art. 17

(Istruttoria e decisione sulla qualificazione ai fini dell'iscrizione negli elenchi di fiducia)

1. L'Autorità ICT-C verifica la completezza della domanda e della documentazione allegata e può richiedere integrazioni, chiarimenti o ulteriori documenti ritenuti necessari ai fini dell'istruttoria, anche con riferimento alla conformità ai requisiti del Regolamento (UE) n. 910/2014.

2. Nel corso dell'istruttoria l'Autorità ICT-C valuta la sussistenza dei requisiti comuni di cui al presente regolamento, dei requisiti specifici eventualmente stabiliti con proprie norme tecniche, circolari tecniche o prassi per ciascuna tipologia di servizio fiduciario qualificato, nonché la coerenza complessiva dell'assetto del prestatore con i requisiti di qualificazione previsti dal Regolamento (UE) n. 910/2014.

3. Il CAR costituisce elemento necessario dell'istruttoria. L'Autorità ICT-C può richiedere al prestatore o al CAB chiarimenti relativi agli esiti, al contenuto e al perimetro della valutazione di conformità, ferma restando l'autonoma verifica da parte dell'Autorità ICT-C della sussistenza dei requisiti necessari alla qualificazione.

4. L'Autorità ICT-C conclude l'istruttoria e adotta il provvedimento motivato entro novanta giorni dalla data di presentazione della domanda. Il termine può essere sospeso una sola volta, entro trenta giorni dalla presentazione, esclusivamente per la motivata richiesta di documenti integrativi o completivi non già nella disponibilità dell'Autorità ICT-C né acquisibili autonomamente; esso riprende a decorrere dalla ricezione della documentazione richiesta. Qualora il provvedimento non sia adottato entro il termine previsto, il richiedente può ricorrere ai sensi dell'articolo 10, comma 2, della Legge n. 68/1989.

5. L'Autorità ICT-C può effettuare, direttamente o tramite soggetti da essa incaricati, verifiche documentali e ispezioni presso il prestatore o i suoi fornitori rilevanti, al fine di accertare la concreta attuazione dei requisiti dichiarati e la capacità del prestatore di erogare in modo continuativo e sicuro i servizi fiduciari qualificati oggetto della domanda.

6. All'esito dell'istruttoria, l'Autorità ICT-C adotta un provvedimento motivato di accoglimento o rigetto della domanda. In caso di accoglimento, l'Autorità ICT-C dispone l'iscrizione del prestatore negli elenchi di fiducia, con indicazione dei servizi per i quali è riconosciuta la qualificazione.

Art. 18

(Pubblicazione e gestione degli elenchi di fiducia)

1. L'Autorità ICT-C pubblica e mantiene aggiornati gli elenchi di fiducia dei prestatori di servizi fiduciari qualificati accreditati ai sensi del presente regolamento.

2. Gli elenchi di fiducia indicano almeno i prestatori qualificati iscritti, i servizi fiduciari qualificati per i quali è stata riconosciuta la qualificazione e ogni altra informazione ritenuta necessaria ai fini della trasparenza e dell'interoperabilità con gli elenchi europei.

3. L'Autorità ICT-C assicura che la pubblicazione degli elenchi avvenga con modalità idonee a garantirne la consultazione pubblica, l'aggiornamento tempestivo e, ove applicabile, la compatibilità tecnica con i formati utilizzati a livello europeo per gli elenchi di fiducia.

Art. 19

(Requisiti specifici per i servizi fiduciari qualificati)

1. Per ciascuna tipologia di servizio fiduciario qualificato ai sensi del Regolamento (UE) n. 910/2014 e del Decreto Delegato n. 173/2024, l'Autorità ICT-C definisce, con proprie norme tecniche, circolari tecniche o prassi, i requisiti specifici aggiuntivi rispetto a quelli comuni previsti dal presente regolamento, tenendo conto:

a) delle disposizioni del Regolamento (UE) n. 910/2014 relative alla qualificazione dei prestatori e dei servizi;

b) degli standard tecnici indicati ai sensi dell'articolo 8;

c) dei livelli di garanzia richiesti per il reciproco riconoscimento europeo e per l'inclusione negli elenchi di fiducia europei;

d) delle migliori pratiche adottate a livello europeo per servizi analoghi.

2. I prestatori iscritti negli elenchi di fiducia devono conformarsi ai requisiti specifici stabiliti dall'Autorità ICT-C per ciascun servizio fiduciario qualificato per il quale risultano accreditati e mantenere tale conformità per tutta la durata dell'iscrizione, fermo restando quanto previsto dal Regolamento (UE) n. 910/2014 in materia di vigilanza e mantenimento della qualificazione.

Art. 20

(Periodo transitorio per i requisiti di competenza)

1. Per un periodo transitorio decorrente dall'entrata in vigore del presente regolamento, la dimostrazione dell'adeguatezza delle competenze del personale e dei responsabili delle funzioni minime coinvolte nell'erogazione dei servizi fiduciari qualificati può essere basata prioritariamente su esperienza professionale documentata, anche in assenza di specifiche certificazioni individuali.

2. Nel periodo transitorio, ai fini dell'accreditamento e del mantenimento dell'iscrizione negli elenchi di fiducia, il prestatore deve dimostrare che le persone chiave coinvolte nella gestione dei servizi fiduciari qualificati possiedono conoscenze e competenze pratiche adeguate, risultanti da attività svolte in ambito di sicurezza delle informazioni, gestione di infrastrutture critiche, servizi fiduciari o servizi ICT di analoga rilevanza.

3. Il prestatore predispone un piano di sviluppo delle competenze che individua, per ciascuna funzione rilevante, gli obiettivi formativi e, ove ritenuto opportuno, le certificazioni o qualifiche professionali che intende conseguire entro il termine del periodo transitorio, tenendo conto degli standard tecnici indicati dall'Autorità ICT-C e delle migliori pratiche di settore.

4. L'Autorità ICT-C definisce, con proprie norme tecniche, circolari tecniche o prassi, la durata del periodo transitorio, i criteri minimi per la valutazione dell'esperienza professionale e, se del caso, le principali qualifiche o certificazioni raccomandate per le funzioni maggiormente critiche, fermo

restando che la mancanza di una specifica certificazione individuale non comporta automaticamente l'impossibilità di ottenere o mantenere la qualificazione del prestatore.

5. Al termine del periodo transitorio, l'Autorità ICT-C può valutare l'opportunità di aggiornare o prorogare i criteri relativi alle competenze, anche alla luce dell'evoluzione del quadro europeo in materia di supervisione dei prestatori di servizi fiduciari qualificati.

TITOLO V — VIGILANZA, CONTROLLI E SANZIONI

Art. 21

(Principi generali di vigilanza)

1. L'Autorità ICT-C esercita la vigilanza sui prestatori iscritti negli elenchi dei servizi di pubblica utilità e negli elenchi di fiducia al fine di verificare, in modo proporzionato e continuo, il rispetto dei requisiti previsti dal presente regolamento, dai decreti delegati vigenti in materia di servizi fiduciari e dalle norme tecniche adottate dall'Autorità stessa.

2. La vigilanza è esercitata secondo principi di obiettività, trasparenza, proporzionalità e non discriminazione, tenendo conto della natura e della criticità dei servizi fiduciari erogati, nonché del loro eventuale rilievo ai fini del mutuo riconoscimento europeo.

Art. 22

(Poteri di richiesta di informazioni e verifiche)

1. I prestatori iscritti negli elenchi sono tenuti a fornire all'Autorità ICT-C, nei termini e con le modalità da essa indicate, tutte le informazioni e la documentazione necessarie per l'esercizio delle funzioni di vigilanza, comprese quelle relative ai soggetti esterni ai quali siano state affidate funzioni rilevanti ai sensi del presente regolamento.

2. L'Autorità ICT-C può effettuare verifiche documentali e, ove necessario, ispezioni presso le sedi dei prestatori e presso i luoghi in cui sono localizzati sistemi e infrastrutture critiche, anche avvalendosi del supporto di altri soggetti pubblici o privati competenti, nel rispetto delle attribuzioni previste dai decreti delegati vigenti.

3. I prestatori devono assicurare piena collaborazione alle attività di verifica e ispezione, garantendo l'accesso alle informazioni, ai sistemi e ai locali strettamente necessari allo svolgimento dei controlli.

Art. 23

(Obblighi di segnalazione di incidenti e variazioni rilevanti)

1. I prestatori sono tenuti a comunicare tempestivamente all'Autorità ICT-C il verificarsi di incidenti di sicurezza o malfunzionamenti che determinino disservizi, sospensioni o interruzioni significative dei servizi fiduciari erogati, nel rispetto degli obblighi e dei termini di notifica previsti dal Regolamento eIDAS per i prestatori qualificati e non qualificati.

2. I prestatori devono altresì comunicare senza ingiustificato ritardo ogni variazione rilevante rispetto alle condizioni in base alle quali è stato concesso l'accreditamento, incluse modifiche dell'assetto organizzativo, delle funzioni minime, delle infrastrutture critiche, delle coperture assicurative e della situazione finanziaria che possa incidere sulla continuità dei servizi.

Art. 24

(Mantenimento dei requisiti ed esiti della vigilanza)

1. I prestatori iscritti negli elenchi di servizi di pubblica utilità e negli elenchi di fiducia devono mantenere nel tempo i requisiti previsti per l'accreditamento e adeguarsi agli eventuali aggiornamenti delle norme tecniche e delle circolari tecniche adottate dall'Autorità ICT-C.

2. L'Autorità ICT-C, all'esito delle attività di vigilanza, può formulare rilievi e raccomandazioni, fissando termini per la rimozione delle carenze riscontrate. In caso di irregolarità o inadempienze non gravi, l'Autorità può limitarsi a richiedere misure correttive e a monitorarne l'attuazione.

Art. 25

(Schema sanzionatorio per i prestatori non qualificati)

1. Per i prestatori iscritti negli elenchi di servizi di pubblica utilità, il presente regolamento definisce lo schema sanzionatorio oggettivo previsto ai sensi dell'articolo 3, comma 9, del Decreto Delegato n. 173/2024. Le relative sanzioni amministrative sono irrogate dall'Autorità ICT-C secondo quanto stabilito dal decreto delegato adottato ai sensi dell'articolo 33 del medesimo decreto.

2. Lo schema prevede sanzioni pecuniarie di importo compreso tra euro 1.000 (mille) ed euro 10.000 (diecimila), nel rispetto dei limiti e delle linee guida di cui all'articolo 3, comma 9, del Decreto Delegato n. 173/2024, inclusa la non applicabilità di ammonimenti, diffide e sanzioni per i disservizi previsti o rientranti nei livelli minimi di fornitura (SLA) e per i casi di forza maggiore, nonché l'applicazione del solo ammonimento nei casi fortuiti.

3. Nella determinazione delle sanzioni amministrative l'Autorità ICT-C tiene conto della gravità e durata della violazione, del numero di utenti potenzialmente coinvolti, del comportamento collaborativo del prestatore e delle misure correttive adottate.

Art. 26

(Schema sanzionatorio per i prestatori qualificati)

1. Per i prestatori di servizi fiduciari qualificati iscritti negli elenchi di fiducia, il presente regolamento definisce lo schema sanzionatorio pecuniario previsto ai sensi dell'articolo 28, comma 2, lettera b), del Decreto Delegato n. 173/2024. Le relative sanzioni amministrative sono irrogate dall'Autorità ICT-C secondo quanto stabilito dal decreto delegato adottato ai sensi dell'articolo 33 del medesimo decreto.

2. Lo schema prevede, per i prestatori qualificati, sanzioni pecuniarie di importo compreso tra euro 10.000 (diecimila) ed euro 100.000 (centomila), proporzionati alla gravità, durata e impatto della violazione.

3. L'applicazione delle sanzioni pecuniarie tiene conto della gravità e reiterazione della violazione, del numero di utenti potenzialmente coinvolti, del comportamento collaborativo del prestatore e delle misure correttive adottate.

Art. 27

(Cancellazione dagli elenchi e revoca della qualificazione)

1. La perdita di uno dei requisiti previsti per l'iscrizione negli elenchi dei prestatori di servizi di pubblica utilità, certificata dall'attività di vigilanza, comporta la cancellazione dall'elenco secondo le modalità previste dall'articolo 21 del Decreto Delegato n. 173/2024. Il mancato pagamento della tassa di rinnovo produce gli effetti di cui all'articolo 24, comma 6, del medesimo decreto.

2. Per i prestatori di servizi fiduciari qualificati, a decorrere dall'attivazione degli elenchi di fiducia, si applicano le disposizioni del Regolamento eIDAS e delle norme tecniche adottate ai sensi dell'articolo 28 del Decreto Delegato n. 173/2024.

Art. 28

(Rapporti con le autorità estere e riconoscimento europeo)

1. Per i prestatori di servizi fiduciari qualificati, l'Autorità ICT-C esercita le funzioni di vigilanza tenendo conto delle disposizioni del Regolamento (UE) n. 910/2014 in materia di supervisione dei prestatori qualificati e delle eventuali intese o accordi di cooperazione con le autorità competenti degli Stati membri dell'Unione europea.

2. L'Autorità ICT-C può scambiare informazioni rilevanti con le autorità estere competenti, nel rispetto della normativa applicabile, al fine di favorire la cooperazione tra autorità di vigilanza e agevolare il riconoscimento e l'interoperabilità dei servizi fiduciari qualificati, nonché l'eventuale inclusione dei prestatori sammarinesi negli elenchi di fiducia europei.

Art. 29

(Cessazione volontaria dei prestatori)

1. Il prestatore di servizi fiduciari, qualificato o non qualificato, che intenda cessare l'attività da uno o più servizi per i quali è iscritto agli elenchi di fiducia o di pubblica utilità, notifica all'Autorità ICT-C con preavviso di almeno sessanta giorni, informando contestualmente la clientela e garantendo il recesso senza oneri aggiuntivi.

2. Il prestatore può indicare prestatori sostitutivi iscritti agli stessi elenchi, ai quali cedere entro trenta giorni la documentazione, la clientela e i registri dei certificati. Per i certificati in scadenza dopo la cessazione, non si procede alla revoca se trasferiti al sostitutivo; in mancanza, l'Autorità ICT-C acquisisce i registri e ne pubblica le revoche nelle liste di revoca (CRL).

3. L'Autorità ICT-C verifica l'adempimento e pubblica la data di cessazione negli elenchi rispettivi.

4. In caso di mancato adempimento, per i prestatori non qualificati si applicano le disposizioni e le sanzioni previste dall'articolo 21 del Decreto Delegato n. 173/2024 e dall'articolo 25 del presente regolamento. Per i prestatori qualificati, l'Autorità ICT-C intima l'adempimento entro il termine previsto dall'articolo 27 del Decreto Delegato n. 173/2024 e, in caso di persistente inadempimento, applica le sanzioni di cui all'articolo 26 del presente regolamento, secondo le modalità previste dalla normativa applicabile, fermo restando quanto previsto dall'articolo 27 del presente regolamento e dalle norme tecniche di settore per ciascun servizio.

TITOLO VI — DISPOSIZIONI TRANSITORIE E FINALI

Art. 30

(Applicazione)

1. Le disposizioni del presente regolamento si applicano a tutte le domande di accreditamento presentate a decorrere dalla sua entrata in vigore e ai prestatori che, a seguito di accoglimento della domanda, risultano iscritti negli elenchi dei servizi di pubblica utilità o negli elenchi di fiducia.

Art. 31

(Coordinamento con le norme tecniche dell'Autorità ICT-C)

1. L'Autorità ICT-C adegua e coordina le proprie norme tecniche, circolari tecniche e prassi in materia di servizi fiduciari con le disposizioni del presente regolamento, assicurandone la coerenza complessiva e tenendo conto dell'evoluzione del quadro normativo europeo e degli standard tecnici applicabili.

2. Le norme tecniche, le circolari tecniche e le prassi adottate dall'Autorità ICT-C ai sensi del Decreto Delegato n. 173/2024 e del Decreto Delegato n. 146/2018, come successivamente modificato e

integrato, specificano, per quanto di rispettiva competenza, i requisiti tecnici, organizzativi e procedurali di dettaglio, nonché le modalità di applicazione delle disposizioni del presente regolamento.

Art. 32

(Aggiornamento del regolamento)

1. L’Autorità ICT-C approva, con propria deliberazione, modifiche e integrazioni al presente regolamento, in particolare quando ciò risulti necessario:

a) per recepire aggiornamenti del Regolamento (UE) n. 910/2014 o di altri atti europei rilevanti;

b) per tenere conto dell’evoluzione degli standard tecnici e delle migliori pratiche internazionali;

c) per adeguare la disciplina dell’accreditamento e della vigilanza all’esperienza applicativa maturata e alle esigenze di sviluppo del mercato dei servizi fiduciari.

Art. 33

(Entrata in vigore e pubblicazione)

1. Il presente regolamento entra in vigore il 15 settembre 2026.

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

3. Resta fermo quanto previsto dall’articolo 15 in relazione all’efficacia delle disposizioni relative agli elenchi di fiducia.

ALLEGATO B

Regolamento AICT-C n. 2026-02

Regolamento tecnico per l’accreditamento e la qualificazione dei servizi di archiviazione elettronica

REPUBBLICA DI SAN MARINO
via 28 Luglio, 192 - 47893 Borgo Maggiore
T +378 (0549) 882 552
info@autoritaict.sm

Regolamento AICT-C n. 2026-02

REGOLAMENTO TECNICO PER L'ACCREDITAMENTO E LA QUALIFICAZIONE DEI SERVIZI DI ARCHIVIAZIONE ELETTRONICA

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 prestazione dei servizi di archiviazione elettronica da parte degli operatori economici di diritto sammarinese che intendono ottenere o mantenere:

a) l'iscrizione nell'elenco dei prestatori abilitati all'archiviazione elettronica di cui all'articolo 22, comma 7, lettera f), del Decreto Delegato 13 novembre 2024 n. 173, quali prestatori di servizi fiduciari non qualificati;

b) la qualificazione del servizio di archiviazione elettronica e la conseguente iscrizione negli elenchi di fiducia, secondo quanto previsto dagli articoli 25 e 28 del Decreto Delegato n. 173/2024.

2. 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 accreditamento e qualificazione, la vigilanza, le sanzioni, le garanzie economiche e assicurative, nonché gli altri obblighi non specificamente riferiti al servizio di archiviazione elettronica.

3. Quando il medesimo prestatore richiede l'accreditamento o la qualificazione per più servizi fiduciari, la documentazione comune già acquisita dall'Autorità ICT-C è gestita secondo il principio del fascicolo unico del prestatore previsto dal Regolamento quadro. Il presente Regolamento disciplina esclusivamente le informazioni e le evidenze specifiche relative al servizio di archiviazione elettronica.

4. Il Regolamento persegue un modello tecnologicamente neutrale e basato sui risultati, evitando di imporre specifiche soluzioni software, 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 n. 173/2024 e del Regolamento (UE) n. 910/2014 e successive modifiche.

2. In particolare, per archiviazione elettronica si intende il servizio che assicura la ricezione, la memorizzazione, il reperimento e la cancellazione di dati elettronici e documenti elettronici, al fine di garantirne la durabilità e la leggibilità e di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione.

3. Ai fini del presente Regolamento si intende inoltre per:

a) servizio AE: il servizio di archiviazione elettronica;

b) servizio AE-NQ: il servizio di archiviazione elettronica prestato da un prestatore iscritto nell'elenco di cui all'articolo 22, comma 7, lettera f), del Decreto Delegato n. 173/2024, privo dello status di servizio fiduciario qualificato;

c) servizio AE-Q: il servizio di archiviazione elettronica qualificato ai sensi del Regolamento (UE) n. 910/2014;

d) oggetto di archiviazione: il dato elettronico, il documento elettronico o l'aggregazione di dati o documenti affidati al servizio;

e) soggetto produttore o produttore: il soggetto che versa o fa versare gli oggetti di archiviazione nel sistema e che risponde delle informazioni e dei documenti affidati al servizio nei limiti definiti dal contratto;

f) periodo di conservazione: l'intervallo temporale durante il quale l'oggetto deve essere mantenuto dal servizio, individuato sulla base della legge, del contratto o delle indicazioni del titolare;

g) evidenza di archiviazione: l'insieme delle informazioni idonee a documentare le operazioni compiute sull'oggetto e a verificarne nel tempo integrità, provenienza e storia;

h) migrazione o riversamento: il trasferimento dell'oggetto o delle relative informazioni verso supporti, sistemi o formati differenti, effettuato senza perdita delle caratteristiche che devono essere preservate;

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

Art. 3

(Perimetro del servizio e responsabilità)

1. Il prestatore definisce in modo chiaro il perimetro del servizio di archiviazione elettronica e le attività delle quali assume la responsabilità.

2. Il servizio deve distinguere almeno:

a) le attività svolte dal soggetto produttore prima del versamento;

b) la fase di ricezione e presa in carico;

c) il periodo di archiviazione;

d) l'accesso, la ricerca e il reperimento degli oggetti;

e) l'eventuale migrazione o trasformazione;

f) la restituzione, il trasferimento o la cancellazione al termine del periodo previsto.

3. Salvo che il contratto attribuisca espressamente al prestatore ulteriori funzioni, il soggetto produttore resta responsabile del contenuto, della completezza e della correttezza dei dati e dei documenti trasmessi e della loro corrispondenza agli eventuali originali dai quali derivano.

4. L'identificazione dell'utente, del sistema o del soggetto che effettua il versamento deve essere assicurata con modalità adeguate al livello di rischio e deve consentire di ricostruire la provenienza dell'operazione.

5. Le responsabilità delle parti sono descritte in modo comprensibile nel contratto, nelle condizioni del servizio o nella documentazione tecnica concordata con il cliente.

TITOLO II — REQUISITI SPECIFICI DEL SERVIZIO DI ARCHIVIAZIONE ELETTRONICA

Art. 4

(Documentazione del servizio)

1. Il prestatore mantiene una documentazione aggiornata che descrive il funzionamento del servizio, le responsabilità, le procedure operative, le misure di sicurezza e le modalità con cui sono soddisfatti i requisiti del presente Regolamento.

2. Le informazioni possono essere contenute in uno o più documenti, quali manuale del servizio, policy, practice statement, 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 del servizio;

b) i ruoli e le responsabilità;

c) le modalità di versamento, presa in carico e rifiuto;

d) i formati e i metadati gestiti;

e) le modalità di protezione dell'integrità e della provenienza;

f) le modalità di accesso, ricerca e reperimento;

g) le procedure di migrazione e gestione dell'obsolescenza;

h) le misure di sicurezza e continuità;

i) le regole di cessazione, trasferimento e cancellazione.

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

Art. 5

(Versamento e presa in carico)

1. Il prestatore adotta procedure documentate per la ricezione degli oggetti di archiviazione.

2. Il processo deve consentire di associare in modo verificabile il versamento:

a) al soggetto produttore;

b) all'utente o al sistema autorizzato che ha effettuato l'operazione;

c) agli oggetti ricevuti;

d) ai metadati ad essi associati;

e) alla data e all'ora dell'operazione o agli altri riferimenti temporali utilizzati.

3. Prima della presa in carico sono effettuati controlli adeguati alla tipologia di oggetto e alle condizioni concordate con il cliente, comprendenti, ove applicabili, la verifica dell'integrità, dei formati, dei metadati, delle firme o dei sigilli elettronici e degli altri elementi richiesti.

4. L'esito positivo della presa in carico genera un'evidenza che consenta di identificare gli oggetti acquisiti e i controlli effettuati.

5. In caso di mancata accettazione, il servizio rende disponibile al soggetto produttore un esito comprensibile che identifichi le anomalie riscontrate.

6. Le modalità tecniche di trasmissione possono utilizzare servizi web, interfacce applicative, trasferimenti di file, portali o altre tecnologie idonee, purché siano garantiti i requisiti del presente articolo.

Art. 6

(Integrità, provenienza, durabilità e leggibilità)

1. Il sistema di archiviazione assicura, per tutto il periodo di conservazione previsto:

a) l'integrità degli oggetti archiviati;

b) la possibilità di verificarne la provenienza;

c) la durabilità delle informazioni;

d) la leggibilità e la possibilità di renderle nuovamente disponibili;

e) la reperibilità;

f) la riservatezza, ove richiesta dalla natura dei dati.

2. Il prestatore adotta misure idonee a rilevare alterazioni, perdite, danneggiamenti o indisponibilità degli oggetti e delle relative evidenze.

3. Le procedure utilizzate devono consentire di ricostruire gli eventi rilevanti intervenuti durante il periodo di archiviazione.

4. Le modifiche necessarie al supporto, al formato o alla rappresentazione tecnica dell'oggetto sono ammesse quando finalizzate a mantenerne la durabilità o la leggibilità e purché siano documentate e non compromettano le caratteristiche che devono essere preservate.

Art. 7

(Metadati, formati e gestione dell'obsolescenza)

1. Il servizio associa agli oggetti di archiviazione metadati sufficienti alla loro identificazione, gestione, ricerca e successivo reperimento.

2. Il prestatore definisce i formati accettati e le eventuali condizioni applicabili ai formati ulteriori richiesti dal cliente.

3. Non è imposto un elenco chiuso di formati quando il prestatore sia in grado di dimostrare che il formato utilizzato consente il mantenimento nel tempo delle caratteristiche richieste.

4. Il prestatore mantiene sotto controllo l'evoluzione tecnologica dei formati, dei supporti, dei sistemi e degli strumenti necessari alla lettura degli oggetti archiviati.

5. Quando emerge un rischio di obsolescenza, il prestatore pianifica e attua le misure necessarie, comprese ove opportuno la migrazione o il riversamento.

6. Ogni trasformazione significativa deve essere tracciata in modo da consentire di individuare l'oggetto di origine, la trasformazione effettuata, il momento in cui è avvenuta e il relativo esito.

Art. 8

(Accesso, ricerca, reperimento ed esibizione)

1. Gli oggetti archiviati devono poter essere ricercati e recuperati attraverso modalità coerenti con i metadati e con le regole di accesso definite per il servizio.

2. L'accesso è consentito esclusivamente ai soggetti autorizzati e deve essere protetto con misure di autenticazione adeguate al rischio e alla natura delle informazioni trattate.

3. Il servizio deve consentire al titolare o agli altri soggetti legittimati di ottenere gli oggetti archiviati insieme alle informazioni necessarie a verificarne l'integrità e la provenienza.

4. Il sistema mantiene evidenza degli accessi e delle operazioni rilevanti secondo criteri proporzionati al rischio.

5. L'esibizione può avvenire per via elettronica e non richiede la conversione su supporto cartaceo salvo che ciò sia espressamente previsto dalla legge o richiesto dall'avente diritto.

Art. 9

(Firme elettroniche, sigilli e riferimenti temporali)

1. Qualora gli oggetti ricevuti contengano firme elettroniche, sigilli elettronici, validazioni temporali o altre evidenze elettroniche, il prestatore adotta procedure adeguate a conservarne le informazioni necessarie alla successiva verifica.

2. Il sistema registra, ove rilevante, le informazioni disponibili sullo stato delle firme, dei sigilli, dei certificati e delle relative evidenze al momento della presa in carico o nelle successive operazioni di conservazione.

3. Le firme, i sigilli e le validazioni temporali utilizzati dal prestatore per produrre evidenze proprie del processo devono essere adeguati alla natura del servizio e al valore che tali evidenze devono assumere.

4. Per il servizio AE-Q si applicano inoltre le disposizioni specifiche del Titolo IV.

Art. 10

(Sicurezza, riservatezza e continuità)

1. Il prestatore protegge il servizio da accessi non autorizzati, perdita, alterazione, distruzione e indisponibilità delle informazioni.

2. Le misure di sicurezza sono determinate sulla base dei rischi e sono coordinate con il sistema generale di gestione della sicurezza del prestatore disciplinato dal Regolamento quadro.

3. Devono essere previste misure adeguate per:

a) il controllo degli accessi;

b) la separazione dei ruoli e dei privilegi;

c) la protezione delle comunicazioni;

d) la protezione delle copie e delle repliche;

e) il backup e il ripristino;

f) la continuità operativa e il disaster recovery;

g) il monitoraggio degli eventi di sicurezza;

h) la gestione degli incidenti;

i) la protezione dei registri e delle evidenze.

4. Il prestatore verifica periodicamente l'effettiva capacità di ripristinare il servizio e gli oggetti archiviati.

5. Le informazioni riservate e i dati personali sono trattati nel rispetto della Legge 21 dicembre 2018 n. 171 e delle altre disposizioni applicabili.

Art. 11

(Registrazioni, controlli e verifiche periodiche)

1. Il prestatore conserva registrazioni sufficienti a ricostruire le operazioni rilevanti effettuate sugli oggetti archiviati e sul servizio.

2. Le registrazioni devono essere protette contro cancellazioni o alterazioni non autorizzate.

3. Il prestatore effettua verifiche periodiche sull'integrità, sulla leggibilità, sulla reperibilità e sulla disponibilità degli oggetti archiviati.

4. La periodicità e l'estensione delle verifiche sono stabilite sulla base del rischio, della durata prevista della conservazione, delle tecnologie utilizzate e dell'evoluzione dei formati e dei supporti.

5. Le anomalie rilevate, le azioni correttive e i relativi esiti sono documentati.

6. Il prestatore mantiene evidenze delle prove di continuità, ripristino, migrazione e recupero eseguite sul sistema.

Art. 12

(Periodo di conservazione e cancellazione)

1. Per ciascuna tipologia documentale o insieme omogeneo di oggetti deve essere determinabile il periodo di conservazione applicabile.

2. Il periodo può derivare dalla legge, dal contratto, dalle istruzioni del titolare o da una combinazione di tali fonti.

3. Il prestatore non procede alla cancellazione di oggetti prima del termine previsto, salvo ordine legittimo dell'avente diritto o altra causa prevista dalla legge.

4. Prima della cancellazione definitiva, il prestatore assicura che siano rispettate le procedure concordate con il cliente e gli eventuali obblighi di proroga, trasferimento o conservazione ulteriore.

5. La cancellazione deve essere effettuata con modalità coerenti con la natura delle informazioni e deve essere tracciabile.

6. L'eventuale prosecuzione della conservazione oltre il termine originariamente previsto deve poter avvenire senza compromettere la continuità delle evidenze già prodotte.

Art. 13

(Fornitori tecnologici e affidamento a terzi)

1. Il prestatore può avvalersi di fornitori tecnologici, infrastrutturali o di altri soggetti terzi nello svolgimento del servizio.

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

3. Il prestatore identifica le funzioni affidate a terzi e mantiene evidenza dei relativi accordi, dei livelli di servizio, delle misure di sicurezza e delle responsabilità.

4. Per le funzioni rilevanti ai fini della sicurezza, integrità, disponibilità o continuità, il prestatore deve poter ottenere dal fornitore le informazioni e le evidenze necessarie alla propria attività di controllo e alla dimostrazione della conformità.

5. Non è richiesto che il fornitore tecnologico possieda autonomamente lo status di prestatore fiduciario qualificato, salvo che eroghi un servizio per il quale tale status sia espressamente richiesto dalla normativa applicabile.

6. Per i servizi AE-Q si applicano inoltre i requisiti in materia di terze parti e subfornitura previsti dal quadro europeo applicabile ai prestatori qualificati.

Art. 14

(Portabilità, trasferimento e cessazione del servizio)

1. Il servizio è progettato in modo da consentire la restituzione o il trasferimento degli oggetti archiviati senza perdita delle informazioni necessarie alla loro identificazione, comprensione e verifica.

2. In caso di trasferimento devono essere resi disponibili, in relazione al perimetro interessato:

a) gli oggetti archiviati;

b) i metadati;

c) le evidenze di archiviazione;

d) le informazioni necessarie a ricostruire le operazioni rilevanti;

e) le informazioni tecniche indispensabili alla corretta acquisizione da parte del destinatario.

3. I formati e le modalità di esportazione devono essere documentati e consentire una ragionevole interoperabilità con altri sistemi di archiviazione.

4. Il trasferimento verso altro prestatore deve essere gestito in modo da evitare interruzioni o lacune non documentate nella catena di custodia.

5. Restano ferme le disposizioni del Regolamento quadro e del Decreto Delegato n. 173/2024 relative alla cessazione dell'attività del prestatore.

TITOLO III — ACCREDITAMENTO DEL SERVIZIO DI ARCHIVIAZIONE ELETTRONICA NON QUALIFICATO

Art. 15

(Domanda di iscrizione)

1. L'operatore che richiede l'iscrizione nell'elenco di cui all'articolo 22, comma 7, lettera f), del Decreto Delegato n. 173/2024 presenta la domanda secondo il procedimento stabilito dal Regolamento quadro.

2. Non devono essere nuovamente prodotti documenti comuni al prestatore già validamente acquisiti dall'Autorità ICT-C.

3. Alla domanda è associato un fascicolo tecnico del servizio AE-NQ contenente le informazioni necessarie a dimostrare il rispetto del presente Regolamento.

Art. 16

(Fascicolo tecnico del servizio AE-NQ)

1. Il fascicolo tecnico consente all'Autorità ICT-C di comprendere il servizio e di verificarne concretamente i requisiti.

2. Esso contiene o richiama almeno:

a) descrizione del servizio e del relativo perimetro;

b) architettura logica e principali flussi informativi;

c) documentazione di cui all'articolo 4;

d) ruoli del prestatore, del produttore e degli eventuali soggetti terzi;

e) modalità di identificazione e autorizzazione dei soggetti o sistemi che effettuano il versamento;

f) procedure di ricezione, controllo, accettazione e rifiuto;

g) gestione di formati, metadati e identificativi;

h) modalità di protezione dell'integrità, della provenienza e della leggibilità;

i) modalità di ricerca, accesso, recupero ed esibizione;

j) procedure relative a firme, sigilli e riferimenti temporali;

k) misure specifiche di sicurezza, backup, ripristino e continuità;

l) procedure di monitoraggio, verifica dell'integrità e gestione dell'obsolescenza;

m) regole relative al periodo di conservazione e alla cancellazione;

n) fornitori tecnologici e funzioni affidate a terzi rilevanti per il servizio;

o) modalità di esportazione, trasferimento e cessazione;

p) condizioni contrattuali e livelli di servizio applicabili;

q) evidenze di test, collaudi, audit, certificazioni o valutazioni tecniche disponibili.

3. La documentazione può fare riferimento a procedure, certificazioni o sistemi già utilizzati dal prestatore, purché sia chiaramente individuato il loro rapporto con il servizio sottoposto ad accreditamento.

4. L'Autorità ICT-C evita la richiesta di documentazione duplicata quando il medesimo requisito risulti già adeguatamente dimostrato.

Art. 17

(Verifica del servizio e iscrizione)

1. Nell'ambito dell'istruttoria prevista dal Regolamento quadro, l'Autorità ICT-C verifica la coerenza tra la documentazione presentata e il funzionamento effettivo del servizio.

2. Quando utile alla verifica, l'Autorità ICT-C può richiedere una dimostrazione del servizio, l'esecuzione di operazioni di prova o la produzione di evidenze generate dal sistema.

3. Certificazioni, audit indipendenti e valutazioni di conformità possedute dal prestatore sono considerate quali evidenze utili nella misura in cui siano pertinenti al requisito esaminato, senza determinare automatica equivalenza con l'accreditamento.

4. In caso di accoglimento, il prestatore è iscritto nell'elenco di cui all'articolo 22, comma 7, lettera f), del Decreto Delegato n. 173/2024 per il servizio di archiviazione elettronica.

Art. 18

(Percorso preparatorio alla qualificazione)

1. Il richiedente o il prestatore già iscritto può dichiarare, secondo il Regolamento quadro, l'obiettivo di conseguire successivamente la qualificazione europea del servizio di archiviazione elettronica.

2. La dichiarazione è facoltativa, non attribuisce lo status di prestatore o servizio qualificato e non consente l'utilizzo di denominazioni o segni che possano indurre gli utenti a ritenere il servizio già qualificato.

3. Nell'ambito del percorso preparatorio il prestatore può strutturare sin dall'origine il servizio AE-NQ secondo i requisiti previsti per il servizio AE-Q e presentare all'Autorità ICT-C le relative evidenze.

4. L'Autorità ICT-C può utilizzare la fase preparatoria per verificare il grado di allineamento del servizio rispetto:

a) agli articoli 45 decies e 45 undecies del Regolamento (UE) n. 910/2014;

b) al Regolamento di esecuzione (UE) 2025/2532;

c) agli ulteriori requisiti generali applicabili ai prestatori qualificati;

d) agli standard e alle specifiche tecniche richiamati dal quadro europeo;

e) al perimetro della futura valutazione da parte del CAB.

5. La fase preparatoria ha la finalità di ridurre le attività da ripetere al momento della successiva qualificazione, senza anticiparne gli effetti giuridici, senza costituire una pre-certificazione e senza anticipare o vincolare la valutazione del CAB.

TITOLO IV — QUALIFICAZIONE DEL SERVIZIO DI ARCHIVIAZIONE ELETTRONICA

Art. 19

(Efficacia delle disposizioni sulla qualificazione)

1. Le disposizioni del presente Titolo 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 restano consentite esclusivamente le attività preparatorie che non producono effetti di qualificazione.

3. La qualificazione nazionale e l'eventuale inserimento del servizio sammarinese nel sistema europeo delle Trusted List restano distinti e sono subordinati alle condizioni e agli accordi di riconoscimento previsti dal Decreto Delegato n. 173/2024.

Art. 20

(Requisiti del servizio AE-Q)

1. Il servizio AE-Q soddisfa i requisiti del Regolamento (UE) n. 910/2014, in particolare degli articoli 24, 45 decies e 45 undecies, nonché degli atti europei di esecuzione e delle specifiche tecniche rilevanti ai fini della qualificazione e del riconoscimento del servizio nel quadro europeo.

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) 2025/2532 e, quale riferimento tecnico per la presunzione di conformità, dalla CEN/TS 18170:2025, con gli adattamenti e i riferimenti normativi previsti dal medesimo Regolamento di esecuzione.

3. Il servizio deve, in particolare:

a) essere prestato da un prestatore fiduciario qualificato;

b) assicurare durabilità e leggibilità oltre il periodo di validità tecnologica e almeno per l'intero periodo di conservazione previsto dalla legge o dal contratto;

c) mantenere l'integrità degli oggetti e l'accuratezza della loro origine;

d) proteggere gli oggetti da perdita e alterazione, fatte salve le modifiche del supporto o del formato necessarie alla loro conservazione;

e) mantenere evidenze sufficienti a verificare il processo per tutta la durata prevista;

f) consentire ai soggetti autorizzati di ottenere in modo automatizzato il rapporto previsto dall'articolo 45 undecies del Regolamento (UE) n. 910/2014.

4. Il rapporto di cui al comma 3, lettera f), deve essere prodotto in modo affidabile ed efficiente e recare la firma elettronica qualificata o il sigillo elettronico qualificato del prestatore del servizio AE-Q.

5. La conformità agli standard, alle specifiche e alle procedure individuati dal Regolamento di esecuzione (UE) 2025/2532 determina la presunzione di conformità prevista dall'articolo 45 undecies del Regolamento eIDAS. L'utilizzo di prassi differenti è ammesso esclusivamente nei casi consentiti dalla disciplina europea e purché la conformità ai requisiti applicabili sia adeguatamente dimostrata nel procedimento di valutazione.

Art. 21

(Archiviazione di documenti sottoscritti o sigillati)

1. Quando gli oggetti affidati al servizio AE-Q contengono firme elettroniche qualificate o sigilli elettronici qualificati, il prestatore utilizza procedure e tecnologie idonee a mantenere l'affidabilità di tali firme o sigilli anche oltre il loro periodo di validità tecnologica e almeno fino alla conclusione del periodo legale o contrattuale di conservazione.

2. Devono essere preservate l'integrità e l'accuratezza dell'origine delle firme e dei sigilli interessati.

3. A tale scopo il prestatore può avvalersi, quando opportuno, di un servizio qualificato di conservazione delle firme elettroniche qualificate o dei sigilli elettronici qualificati.

4. Quando il prestatore utilizza firme elettroniche, sigilli elettronici o validazioni temporali per produrre evidenze del processo di archiviazione qualificata o per stabilire l'origine dei dati, tali strumenti devono possedere il livello di qualificazione richiesto dalla disciplina europea applicabile. Il prestatore può utilizzare servizi fiduciari qualificati erogati da altri prestatori, senza che ciò richieda che egli sia direttamente qualificato per ciascuno dei servizi fiduciari utilizzati.

Art. 22

(Valutazione del CAB e rapporto di conformità)

1. La domanda di qualificazione del servizio AE-Q è supportata da una relazione di valutazione della conformità rilasciata da un CAB accreditato per la valutazione dei prestatori di servizi fiduciari qualificati e con un ambito di accreditamento idoneo a comprendere i servizi qualificati di archiviazione elettronica.

2. La valutazione è effettuata secondo il Regolamento di esecuzione (UE) 2025/2162 e gli ulteriori atti applicabili.

3. Il perimetro della valutazione deve corrispondere al servizio effettivamente sottoposto a qualificazione e deve comprendere le componenti, i siti, le infrastrutture e i soggetti terzi rilevanti per il rispetto dei requisiti, nei limiti previsti dallo schema di valutazione applicabile.

4. Modifiche intervenute successivamente alla valutazione che possano incidere sulla conformità devono essere gestite secondo le procedure di change management previste dal quadro europeo.

5. La presenza di certificazioni ulteriori, comprese certificazioni dei sistemi di gestione della sicurezza o di qualità, costituisce evidenza utile ma non sostituisce il rapporto di valutazione della conformità previsto per il servizio qualificato.

Art. 23

(Notifica, qualificazione e iscrizione negli elenchi di fiducia)

1. La notifica dell'intenzione di avviare il servizio AE-Q e la relativa istruttoria sono effettuate secondo il Regolamento quadro e, per quanto applicabile, il Regolamento di esecuzione (UE) 2025/1572.

2. La documentazione individua senza ambiguità il servizio per il quale è richiesta la qualificazione e comprende gli elementi necessari alla sua successiva rappresentazione nell'elenco di fiducia.

3. L'Autorità ICT-C verifica il prestatore, il servizio e il rapporto del CAB secondo le modalità previste dalla normativa applicabile.

4. Il prestatore non presenta al pubblico il servizio come qualificato prima dell'attribuzione dello status qualificato e della relativa registrazione nell'elenco di fiducia applicabile.

5. L'inserimento nel sistema europeo delle Trusted List è subordinato al perfezionamento delle condizioni previste dall'articolo 28 del Decreto Delegato n. 173/2024 e non discende automaticamente dalla sola qualificazione nazionale.

Art. 24

(Riuso della documentazione e delle evidenze)

1. Nel passaggio dal servizio AE-NQ al servizio AE-Q, l'Autorità ICT-C non richiede nuovamente documenti o evidenze già acquisiti quando risultino ancora validi, aggiornati, pertinenti, non modificati e idonei anche ai fini della qualificazione.

2. Il prestatore può pertanto presentare un fascicolo integrativo contenente principalmente:

a) le modifiche intervenute rispetto al servizio già accreditato;

b) i requisiti aggiuntivi propri della qualificazione;

c) le evidenze aggiornate richieste dal CAB;

d) il rapporto di valutazione della conformità;

e) le informazioni specifiche necessarie alla qualificazione e all'iscrizione nell'elenco di fiducia.

3. Il principio di riuso si applica anche alla documentazione comune del prestatore già acquisita per altri servizi fiduciari, purché permangano le condizioni di cui al comma 1.

4. Il riuso documentale non limita la verifica completa richiesta per la qualificazione, non sostituisce la valutazione del CAB e non comporta automatica estensione al servizio AE-Q di certificazioni o valutazioni riferite a servizi differenti.

Art. 25

(Continuità degli archivi nel passaggio da AE-NQ ad AE-Q)

1. Il conseguimento della qualificazione non determina, per il solo mutamento dello status del servizio, l'obbligo di migrare, duplicare o riversare nuovamente il contenuto degli oggetti già validamente acquisiti e conservati secondo la disciplina applicabile. Restano ferme le eventuali operazioni tecniche e documentali necessarie per la presa in carico degli oggetti nel perimetro del servizio qualificato e per la produzione delle evidenze richieste dalla disciplina applicabile.

2. Restano fermi gli effetti e la validità già acquisiti dagli oggetti e dalle relative evidenze nel periodo precedente alla qualificazione, secondo quanto previsto dall'articolo 10, comma 3, del Decreto Delegato n. 173/2024 e dalle altre disposizioni applicabili.

3. La qualificazione produce gli effetti propri del servizio AE-Q a decorrere dal momento in cui il servizio consegue validamente lo status qualificato secondo la normativa applicabile.

4. Quando il medesimo archivio prosegue senza soluzione di continuità dal regime AE-NQ al regime AE-Q, il prestatore mantiene la catena delle evidenze e rende tecnicamente individuabile il momento dal quale il servizio opera con status qualificato.

5. Per gli oggetti già presenti nel sistema al momento della qualificazione, il prestatore adotta, ove necessario, una procedura documentata di transizione nel perimetro qualificato, idonea a verificare la continuità delle evidenze, l'integrità e la provenienza degli oggetti e a determinare il momento dal quale sono prodotti gli effetti e le evidenze propri del servizio AE-Q. Tale procedura non comporta necessariamente la migrazione o la duplicazione degli oggetti conservati.

6. Il passaggio di status non deve comportare interruzioni della custodia, perdita di metadati o perdita delle evidenze già prodotte.

7. La qualificazione non attribuisce retroattivamente al periodo precedente al conseguimento dello status qualificato gli effetti giuridici propri del servizio AE-Q. Restano ferme eventuali disposizioni normative che stabiliscano specifici regimi transitori.

8. Quando necessario a una corretta interpretazione delle evidenze, le informazioni rilasciate dal servizio distinguono il periodo precedente alla qualificazione dal periodo successivo.

Art. 26

(Modifiche rilevanti e cessazione del servizio AE-Q)

1. Il prestatore dispone di una procedura per identificare e valutare preventivamente le modifiche che possono incidere sulla conformità del servizio AE-Q.

2. Le modifiche rilevanti relative, in particolare, ad architettura, infrastruttura, hosting, tecnologie crittografiche, procedure fondamentali, organizzazione, fornitori critici o perimetro del servizio sono comunicate al CAB e all'Autorità ICT-C nei casi e nei termini previsti dalla disciplina europea applicabile e dal Regolamento quadro.

3. Il prestatore mantiene un piano di cessazione aggiornato che assicuri il trasferimento o la restituzione ordinata degli oggetti, dei metadati e delle evidenze necessarie.

4. Per il servizio AE-Q sono rispettati i termini di preavviso specifici previsti dal quadro europeo per le modifiche significative e per la cessazione programmata, quando più ampi rispetto ai termini generali previsti dalla normativa sammarinese.

5. La cessazione non deve compromettere la possibilità di verificare gli oggetti già archiviati né determinare la perdita delle evidenze necessarie alla loro successiva utilizzazione.

TITOLO V — VIGILANZA E DISPOSIZIONI FINALI

Art. 27

(Vigilanza sul servizio)

1. La vigilanza sul prestatore e sul servizio è esercitata secondo il Regolamento quadro.

2. Per il servizio di archiviazione elettronica, l'Autorità ICT-C può richiedere le evidenze necessarie a verificare, in particolare:

a) operazioni di versamento e presa in carico;

b) esiti dei controlli e dei rifiuti;

c) verifiche di integrità e leggibilità;

d) procedure di ripristino e continuità;

e) migrazioni e trasformazioni effettuate;

f) accessi e recuperi;

g) cancellazioni;

h) trasferimenti verso altri sistemi;

i) attività affidate a terzi;

j) gestione degli incidenti e delle modifiche rilevanti.

3. L'Autorità ICT-C privilegia, ove possibile, l'utilizzo di evidenze già prodotte nell'ambito di audit, certificazioni, valutazioni del CAB o controlli precedenti, evitando duplicazioni non necessarie.

Art. 28

(Sistemi e documentazione preesistenti)

1. I sistemi, le procedure, i manuali, le certificazioni e le evidenze già esistenti alla data di entrata in vigore del presente Regolamento possono essere utilizzati per dimostrare i requisiti in esso previsti nella misura in cui risultino ancora validi, pertinenti e tecnicamente adeguati.

2. L'Autorità ICT-C può richiedere una matrice di corrispondenza tra la documentazione preesistente e i requisiti del presente Regolamento, anziché la riscrittura integrale della documentazione.

3. La conformità a precedenti discipline nazionali, alle Linee guida italiane sulla conservazione o ad altri schemi di certificazione costituisce evidenza utilizzabile ma non determina, da sola, la conformità ai requisiti europei del servizio AE-Q.

4. Restano validi gli oggetti già conservati secondo la disciplina applicabile al momento del loro ingresso nel sistema, nei termini previsti dal Decreto Delegato n. 173/2024.

Art. 29

(Normativa europea e standard tecnici)

1. Per il servizio AE-Q costituiscono riferimenti, nel testo vigente e secondo le modalità stabilite dal Regolamento quadro:

a) il Regolamento (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183;

b) il Regolamento di esecuzione (UE) 2025/2532;

c) il Regolamento di esecuzione (UE) 2025/1572;

d) il Regolamento di esecuzione (UE) 2025/2162;

e) gli atti europei relativi ai requisiti generali dei prestatori fiduciari qualificati e alla gestione delle Trusted List;

f) gli standard e le specifiche tecniche espressamente richiamati dagli atti di cui alle lettere precedenti.

2. Quando un atto europeo individua una specifica versione di uno standard ai fini della presunzione di conformità, si utilizza la versione indicata dall'atto medesimo.

3. L'Autorità ICT-C può aggiornare mediante circolare tecnica, con funzione ricognitiva e di coordinamento, l'elenco dei riferimenti applicabili quando intervengono nuovi atti europei, nuove versioni formalmente riconosciute o modifiche rilevanti del quadro tecnico. La circolare non introduce autonomamente nuovi requisiti sostanziali non previsti dalle fonti applicabili e non impone al prestatore standard non ancora applicabili al servizio.

Art. 30

(Entrata in vigore e applicazione)

1. Il presente Regolamento entra in vigore il 15 settembre 2026.

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

3. Dalla data di entrata in vigore si applicano le disposizioni relative al servizio AE-NQ.

4. Le disposizioni del Titolo IV relative al servizio AE-Q acquistano efficacia esclusivamente alle condizioni previste dall'articolo 19.

5. Per quanto non espressamente disciplinato dal presente Regolamento si applicano il Regolamento quadro generale dei servizi fiduciari e le altre disposizioni vigenti.

ALLEGATO C

Regolamento AICT-C n. 2026-03

Regolamento tecnico per la qualificazione dei servizi di firma elettronica, sigillo elettronico, validazione temporale e servizi fiduciari connessi

REPUBBLICA DI SAN MARINO
via 28 Luglio, 192 - 47893 Borgo Maggiore
T +378 (0549) 882 552
info@autoritaict.sm

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.