Actalis S.p.A.

Practice Statement – Manuale Operativo Servizio di firma remota e gestione dei QSCD

Versione: 1.0
Data di aggiornamento: 03/03/2026
Approvato da: Andrea Sassetti
Classificazione del documento: Pubblico

VERSIONE	DATA	MODIFICA
V 1.0	03/03/2026	Prima versione

Sassetti
Andrea
30.03.2026
17:30:27
UTC

SOMMARIO

1 INTRODUZIONE E AMMINISTRAZIONE DEL DOCUMENTO

1.1 Quadro generale

Actalis S.p.A. è prestatore di servizi fiduciari qualificato, accreditato presso AgID dal 2002, che fornisce servizi di certificazione qualificata di chiavi pubbliche, ovvero servizi di Certification Authority (CA), nonché servizi relativi alla gestione sicura e all'esercizio di dispositivi qualificati per la creazione di una firma elettronica a distanza (QSCD), oltre agli altri servizi fiduciari qualificati di cui si rimanda sito web https://www.actalis.com .

Un certificato digitale di firma remota associa una chiave pubblica ad un Titolare, persona fisica o giuridica. Il Titolare del certificato possiede e utilizza in via esclusiva la corrispondente chiave privata. Il certificato è emesso e rilasciato al Titolare da una terza parte fidata e accreditata, denominata Certification Authority (CA), ed è firmato digitalmente dalla CA.

Il presente documento descrive il servizio di **Servizio di firma remota e gestione dei QSCD** per la creazione della firma elettronica (Remote QSCD) per conto dei titolari, inclusi i processi di generazione, attivazione, sospensione, revoca e distruzione delle chiavi crittografiche dei Titolari, in conformità alla normativa vigente ed in particolare al Regolamento (UE) n. 910/2014 così come modificato dal Regolamento (UE) 2024/1183.

Per ulteriori informazioni sul servizio di firma digitale, si rimanda al documento "*Certificati Qualificati – Manuale Operativo / Certification Practice Statement e Certificate Policy*" pubblicato all'indirizzo https://www.actalis.com/it/legal-repository .

1.2 Practice Statement

1.2.1 Nome identificativo del documento e uso dei certificati

Il presente documento costituisce il Manuale Operativo del **Servizio di firma remota e gestione dei QSCD** di Actalis S.p.A., identificato dall'Object Identifier (OID) 1.3.159.

Il documento descrive le modalità con cui Actalis S.p.A. soddisfa i requisiti della policy EUSPv2 definita nello standard ETSI TS 119 431-1.

Gli Object Identifier (OID) utilizzati nei certificati qualificati emessi da Actalis sono definiti nella sezione 1.4 del CPS, alla quale si rimanda per l'elenco completo e la relativa descrizione.

In aggiunta agli OID di policy già definiti nel CPS, i certificati qualificati emessi nell'ambito del servizio di firma remota qualificata includono l'OID della policy EUSPv2.

> ***EUSPv2**, EU SSAS Policy - itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE policies(19431) ops(1) policy-identifiers(1) eu-remote-qscd-v2(4).*

I certificati qualificati che includono l'OID della policy EUSPv2 sono disciplinati dal presente Manuale Operativo.

1.2.2 Amministrazione del Practice Statement

La versione del presente Manuale Operativo / Practice Statement (PS) è indicata nella pagina iniziale. Il documento è redatto, pubblicato e aggiornato dalla Certification Auhtority Actalis S.p.A..

Il responsabile del Servizio di Actalis è:

Andrea Sassetti
Direttore dei Servizi di Certificazione
Actalis S.p.A.

Il presente Manuale Operativo / Practice Statament è oggetto di revisione periodica, con cadenza almeno annuale.

Ogni nuova versione del presente documento è immediatamente pubblicata sul sito web di Actalis S.p.A. (https://www.actalis.com/legal-repository) in formato PDF firmato, al fine di garantirne l'origine e l'integrità.

Il repository online è normalmente disponibile in modo continuativo (24 ore al giorno, 7 giorni su 7).

1.2.3 Soggetti approvatori

Il presente documento è approvato dalla Direzione di Actalis S.p.A., a seguito della verifica da parte delle strutture aziendali coinvolte e tenuto conto delle disposizioni previste dallo standard *ETSI TS 119 431 v1.3.1* e dai paragrafi 6.1 e 6.2 dello standard *ETSI EN 319 401*.

1.3 Definizioni e acronimi

I termini utilizzati nel presente documento sono definiti come segue:

AgID	Agenzia per l'Italia Digitale.
CA	Certification Authority.
CPS	Certificate Practice Statement dell'Autorità di Certificazione Actalis, disponibile all'indirizzo https://www.actalis.com/legal-repository
DTBS/R	Rappresentazione dei documenti informatici in corso di sottoscrizione.
HSM	Hardware Secure Module.
eID	Identificazione elettronica.
eID mean	Unità materiale e/o immateriale contenente i dati e gli attributi necessari per l'identificazione di un soggetto ed utilizzata per l'autenticazione online a un servizio informatico.
EUSPv2	EU SSAS Policy così come descritta nello standard ETSI 119 431-1, cfr. allegato A.2 *itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4) .*
IDS	IDentification Service - Il servizio Actalis S.p.A. per la verifica dell'identità e degli attribute dei Richiedenti.
QSCD	Dispositivo per la creazione di una firma elettronica qualificata, come definito nel Regolamento eIDAS.
OTP	One Time Password
Provisioner	Servizio informatico che orchestra le interazioni con il SAM/HSM ed il servizio di Certification Authority.
PS	Practice Statament o Manuale Operativo – il presente documento.
SAD	Signature Activation Data.
SAM	Signature Activation Module.
SAP	Signature Activation Protocol.
SIC	Interaction Component del Titolare.

Soggetto	La persona fisica o giuridica identificata nell'attributo "Soggetto" del certificato.
Sottoscrittore	Persona fisica o giuridica a cui è rilasciato il certificato.
TSMP	Trust Service Management Platform – Servizio di Actalis che gestisce i servizi fiduciari.

2 SERVIZIO DI FIRMA REMOTA E GESTIONE DEI QSCD

Il Servizio di Firma Remota e Gestione QSCD fornito da Actalis S.p.A. consente la creazione di firme elettroniche qualificate attraverso un'infrastruttura sicur lato-server gestita sotto la responsabilità della Certification Authority Actalis S.p.A. e in via esclusiva da parte del Titolare.

I dati per la creazione della firma del Titolare sono generati e conservati all'interno di *un dispositivo qualificato per la creazione di una firma elettronica a distanza* (QSCD) in un ambiente remoto protetto e per conto del Titolare. La chiave privata non è esportabile e tutte le operazioni di firma sono eseguite all'interno del QSCD.

Il servizio garantisce l'identificazione certa e l'autenticazione forte del Titolare, l'attivazione controllata delle chiavi di firma e la generazione della firma sul documento informatico, in conformità al Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024, che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo per l'identità digitale, nonché agli standard tecnici applicabili, quali *ETSI TS 119 461*.

3 GESTIONE DEL CICLO DI VITA DELLA CHIAVE DI FIRMA

3.1 Inizializzazione

3.1.1 Dispositivi di creazione della firma

Le chiavi private dei Titolari vengono inizializzate e utilizzate all'interno del dispositivo QSCD sotto riportato, pienamente conforme alle normative europee e registrato come dispositivo qualificato per la creazione di firme (QSCD):

Applicant	Entrust EU S.L
Name	Entrust Signature Activation Module, version 1.1.1
Certificazione QSCD	https://www.a-sit.at/downloads/2403
Certificazione Common Criteria	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0368256-CR-1.0.pdf
Security Target	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0368256-ST-1.1.pdf

In aggiunta, Actalis S.p.A. gestisce ulteriori dispositivi QSCD certificati e conformi alle normative europee applicabili, sebbene attualmente siano in uno stato *legacy* e soggetti a migrazione tecnologica verso nuove soluzioni. Tali dispositivi *legacy* sono inclusi nell'ambito di applicazione della presente Practice Statement, in quanto dispositive qualificati e certificati "QSCD" dall'Autorità Nazionale competente ed in gestione da parte della Certification Authority.

Applicant	Thales e-Security Ltd
Nome	nShield Connect v11.72.02 Family
Certificazione QSCD	https://www.acn.gov.it/portale/documents/20119/915264/ac_rda_eidas_nshield_v1.0.pdf
Certificazione Common Criteria	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0368256-CR-1.0.pdf
Obiettivo di sicurezza	https://www.commoncriteriaportal.org/files/epfiles/st_thales_nshield_v1.0_public.pdf

Applicant	nChipher Security Limited
Nome	nShield Connect v11.72.03 Family
Certificato QSCD	https://www.acn.gov.it/portale/documents/20119/914698/ac_rda_eidas_nshield_2019_v1.0.pdf
Certificazione Common Criteria	https://www.acn.gov.it/portale/documents/20119/914698/rc_ncipher_nshield_v1.0.pdf/0a43da48-e80f-771e-799e-fee6355657fc?t=1749546055059
Security Target	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/st_ncipher_nshield_v1.1_public.pdf

3.1.2 Suite crittografiche

Actalis seleziona gli algoritmi crittografici e i relativi parametri utilizzati nell'ambito del servizio di firma remota in conformità allo standard ETSI TS 119 312 e alla normativa nazionale applicabile, tenendo conto del livello di sicurezza richiesto, del periodo di validità previsto dei certificati qualificati remoti e del quadro normativo di riferimento.

Alla data del presente documento, Actalis adotta le seguenti suite crittografiche per la generazione e l'utilizzo dei dati di creazione della firma nell'ambito del servizio di firma remota:

Algoritmo	Lunghezza chiave	Funzione di hash
RSA	2048 bit[1]	SHA-256
RSA	3072 bit	SHA-256
ECC	P-256 o superiore	SHA-256

Tutte le suite crittografiche adottate sono allineate alle caratteristiche tecniche e di sicurezza dei dispositivi QSCD. In particolare, gli algoritmi selezionati e le lunghezze delle chiavi sono supportati dai dispositivi QSCD e risultano coerenti con il relativo Security Target valutato e con i relativi vincoli di configurazione.

3.1.3 Generazione della chiave di firma

Nel contesto del servizio di Firma Remota, la chiave privata del Titolare è generata direttamente all'interno del QSCD e non esportabile dal perimetro crittografico sicuro del dispositivo.

Le coppie di chiavi crittografiche sono di solito generate all'interno del QSCD prima della richiesta e della loro successiva assegnazione ad uno specifico Titolare. Le chiavi crittografiche, chiamate anche *parked keys,* sono successivamente assegnate e associate logicamente ai singoli Titolari e ai relativi certificati di chiave pubblica così come descritto nei paragrafi seguenti.

L'orchestrazione dei processi di assegnazione è effettuata dai servizi TSMP e Provisioner di Actalis .

3.1.4 Identificazione e collegamento dell'identità

La verifica dell'identità del Richiedente è effettuata tramite l'applicativo IDS di Actalis S.p.A., che gestisce le modalità di identificazione dei Richiedenti previste e descritte nel CPS del servizio di firma elettronica qualificata. Per ulteriori dettagli si rimanda al CPS.

Il servizio TSMP stabilisce un collegamento univoco tra le evidenze di identificazione prodotte e raccolte dal servizio IDS, e successivamente trasmesse a TSMP, la sessione univoca di richiesta del certiticato ed il certificato qualificato che sarà emesso nelle fasi successive.

Tale associazione univoca è garantita anche nei casi in cui le attività di identificazione siano delegate a terze parti (Identity Provider) e/o i sistemi QSCD siano gestiti da organizzazioni esterne sotto la responsabilità della Certification Authority così come previsto dall'Art. 3 del Decreto del Presidente del Consiglio dei Ministri (DPCM) del 22 febbraio 2013.

3.1.5 Linking del certificato

Il collegamento del certificato viene eseguito a seguito della verifica dell'identità e degli attribute del Titolare, persona fisica o giuridica, e dell'emissione del certificato stesso.

[1] La suite crittografica RSA a 2048bit viene attualmente mantenuta per garantire l'interoperabilità e la retrocompatibilità con i sistemi informatici *legacy* e alcune parti terze. In linea con le attuali *best practices* di sicurezza e con gli standard applicabili, la suite RSA 2048bit è in corso di sostituzione con suite crittografiche più robuste.

A seguito della convalida dell'identità e degli attributi, il Provisioner di Actalis richiede l'assegnazione di una coppia di chiavi crittografiche tra le *parked keys* pregenerate all'interno del dispositivo QSCD. In base ai dati e agli attribute verificati dal servizio IDS, e resi disponibili dal sistema TSMP, il Provisioner richiede al servizio di Certification Authority l'emissione di un certificato qualificato contenente le raccolte e verificate del Titolare, tale fase è chiamata anche *Certificate Signing Request.*

Una volta che il certificato è stato generato dal servizio CA, questo viene trasmesso al QSCD dal Provisioner e successivamente all'HSM e quindi associato logicamente alla corrispondente chiave privata del Titolare. Questo processo garantisce un vincolo univoco tra l'identità del Titolare verificatada IDS, il certificato emesso dalla CA e le chiavi di firma all'interno dell'HSM.

Nel caso di *dispositivi legacy* che non implementano un SAM, il Provisioner si interfaccia direttamente con la componente crittografica dell'HSM al fine di associare il certificato alla chiave privata del Titolare.

3.1.6 Consegna dei mezzi di autenticazione

La consegna dei mezzi di autenticazione è effettuata dai sistemi di Actalis S.p.A. durante le fasi di registrazione.

A seguito della registrazione dell'utenza da parte del servizio TSMP:

- viene inviato un link di attivazione all'indirizzo e-mail dichiarata dal Richiedente durante la fase di registrazione;
- viene inviato un codice OTP via SMS al numero di cellulare dichiarato dal Richiedente durante la fase di registrazione.

Tramite il link di attivazione e l'OTP, il Richidente è definisce una password personale secondo definite policy aziendali. Tale password è logicamente associata all'account del Titolare e successivamente verificata dal servizio *Front-End* durante le procedure di autenticazione.

Il secondo fattore di autenticazione viene attivato tramite il servizio *StrongAuth*, tramite la scansione di un QR-code o l'inserimento di un codice di attivazione all'interno dell'applicazione mobile dedicate della Certification Authority. In alternativa, ove èpssibile, può essere consegnato un token hardware OTP all'indirizzo postale dichiarato dal Richiedente durante la fase di registrazione su TSMP.

Tale vincolo garantisce che le credenziali di autenticazione utilizzate all'interno del servizio di Firma Remota siano sotto il controllo esclusivo del Titolare, garantendo la completa tracciabilità e sicurezza delle credenziali di autenticazione.

3.2 Attivazione della firma

Il processo di attivazione della firma viene avviato quando il Titolare accede al Servizio di Firma Remota tramite un'applicazione client PEC di Actalis (ad es. ArubaSign, Aruba Trusted Platform...) ed esegue un'autenticazione a due fattori. Durante questa fase, il Titolare invia anche il DTBS/R per l'apposizione della firma sui documenti informatici caricati.

Il Titolare si autentica al servizio di Firma Remota utilizzando meccanismi di autenticazione a più fattori. La credenziale statica (password) viene verificata dal *Servizio Front-End*, mentre la One-Time Password (OTP) viene convalidata dal servizio *StrongAuth*, che funge da *Authorization Server*. Una volta completata con successo l'autenticazione, l'Authorization Server genera una corrispondente asserzione di avvenuta autenticazione.

A seguito dell'avvenuta autenticazione e dell'autorizzazione concessa dall'Authorization Server, viene generata una asserzione SAD. Tale asserzione include almeno:

- il DTBS/R specificato o un insieme di DTBS/R da firmare;
- i dati che identificano il Titolare correttamente autenticato;
- la chiave di firma predefinita o esplicitamente dichiarata dal Titolare.

Il SAD viene quindi trasmesso tramite il protocollo SAP al QSCD, che ne verifica la validità e l'autenticità in conformità con i documenti tecnici applicabili. Una volta completata con successo tale verifica, il QSCD attiva la chiave privata del Titolare all'interno dell'HSM ed esegue l'operazione di sottoscrizione dei documenti informatici.

I documenti firmati vengono quindi restituiti al Titolare per tramte del client di Actalis .

Actalis gestisce inoltre servizi *di firma remota automatica*, come disciplinato dal Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013. In tale ambito, e ove consentito dalla normativa nazionale applicabile, il Titolare autorizza il processo di firma automatica tramite un'unica attivazione e autorizzazione, esercitando il controllo esclusivo delle chiavi a *livello di batch* sulla base di regole di autorizzazione predefinite e di una configurazione preventiva. Tali modalità sono implementate nel rispetto di adeguate misure di sicurezza contrattuali, organizzative e tecniche, garantendo l'attribuzione della firma al Titolare e la conformità ai requisiti normativi nazionali applicabili.

Nel caso di *sistemi legacy* che non implementano un modulo SAM, il processo di autenticazione a due fattori viene verificato attraverso i database dei servizi *StrongAuth* e *Front-End*. Una volta validati con successo i fattori di autenticazione, questi componenti interagiscono direttamente con il componente crittografico del QSCD al fine di autorizzare l'operazione di firma, in conformità con la documentazione tecnica applicabile.

Infine, modalità di autenticazione semplificate, nonché meccanismi di autenticazione delegati a fornitori terzi, possono essere implementati laddove consentito dalla legislazione nazionale applicabile. In particolare, ai sensi dell'articolo 35, comma 5, del Decreto Legislativo n. 82/2005, tali modalità sono soggette a una specifica valutazione e all'autorizzazione preventiva da parte dell'Autorità Nazionale competente AgID.

3.3 Cancellazione della chiave di firma

La cancellazione della chiave crittografica di firma del Titolare viene effettuata:

- a seguito della revoca del corrispondente certificato qualificato da parte del Titolare (cfr. anche par. 4.9 del CPS); oppure

- a seguito di una richiesta di revoca da parte del Terzo Interessato; oppure
- su richiesta di un'Autorità competente o di un terzo di fiducia che agisca in conformità alle leggi e ai regolamenti applicabili (ad esempio, Polizia o Autorità Giudiziarie ecc…)
- a seguito all'attivazione del Piano di Cessazione che interessi il Servizio di Firma Qualificata e/o il Servizio di firma remota e gestione dei QSCD della Certification Authority Actalis .

Previa verifica della validità e dell'autenticità della richiesta di revoca, Actalis procede alla cancellazione dell'account associato al Titolare (nome utente) e alla revoca del corrispondente certificato qualificato all'interno del servizio di Certification Authority.

Tali azioni garantiscono che la chiave privata del Titolare non possa più essere utilizzata in alcun caso. Successivamente, lo stato del certificato viene aggiornato e pubblicato nella Lista di Revoca dei Certificati (CRL).

Per ulteriori informazioni, si rimanda al paragrafo 4.9 del CPS.

3.4 Backup e ripristino delle chiavi di firma

Il backup delle chiavi di firma viene eseguito all'interno di sistemi crittografici sicuri che forniscono un livello di protezione equivalente a quello dell'ambiente QSCD primario. Tali sistemi assicurano le stesse garanzie di sicurezza in termini di riservatezza, integrità, non estraibilità e resistenza contro l'accesso non autorizzato.

Le procedure di backup sono eseguite esclusivamente da personale autorizzato e dai *Trusted Roles*, in conformità con politiche di sicurezza e meccanismi di controllo degli accessi formalmente approvati.

4 MISURE DI SICUREZZA

4.1 Prescrizioni generali

Actalis implementa controlli relativi alle infrastrutture, alla gestione e alle operazioni al fine di proteggere i sistemi e gli asset a supporto dell'erogazione del servizio di firma remota e dei servizi di gestione dei QSCD, in conformità alla norma ETSI EN 319 401, paragrafo 7.6.

Sono adottate misure di sicurezza fisica e ambientale volte a prevenire accessi non autorizzati, danni o interferenze alle strutture e alle infrastrutture critiche. Le procedure operative sono documentate, attuate e mantenute al fine di garantire un'erogazione del servizio sicura e affidabile. I ruoli e le responsabilità sono chiaramente definiti e le attività sono svolte nel rispetto del principio di segregazione dei compiti.

I processi operativi includono il monitoraggio dei sistemi, la gestione degli incidenti, la registrazione degli eventi (logging) e la protezione degli asset informativi, al fine di garantire la riservatezza, l'integrità e la disponibilità del servizio fiduciario durante tutto il suo ciclo operativo.

Per ulteriori informazioni si rimanda anche al paragrafo 5 del CPS.

4.2 Controlli di sicurezza fisica

Actalis utilizza i servizi di gestione del data center (certificati ISO/IEC 27001) forniti dalla capogruppo Aruba S.p.A., responsabile dell'hosting, della connettività Internet e della sicurezza fisica dei sistemi di elaborazione utilizzati a supporto del Servizio di firma remota e Gestione dei QSCD.

La capogruppo Aruba S.p.A. garantisce ad Actalis :

- il controllo degli accessi fisici;
- la continuità dell'alimentazione elettrica;
- sistemi antincendio e antiallagamento;
- ventilazione e climatizzazione ottimali;
- connettività Internet ridondante e almeno il doppio della capacità minima richiesta;
- un Centro Operativo della Struttura (FOC) e un Centro Operativo di Sicurezza del Sito (SiSOC), presidiati 24 ore su 24, 7 giorni su 7, 365 giorni all'anno da personale qualificato, che garantisce il monitoraggio costante dell'infrastruttura e un intervento tempestivo in caso di necessità.

Per ulteriori informazioni, si prega di consultare il CPS par. 5.1.

4.3 Controlli procedurali

Actalis definisce e gestisce account dedicati per le attività amministrative relative all'installazione, alla configurazione, alla gestione e alla manutenzione dei sistemi a supporto del Servizio di firma remota e gestione dei QSCD, si veda anche il par. 5.1. Tali account sono creati specificatamente per scopi amministrativi e sono separati dagli account standard degli utenti.

Gli account privilegiati sono assegnati secondo il principio del *least privilege* e sono utilizzati solo laddove siano strettamente necessari per svolgere una specifica attività autorizzata. L'assegnazione, l'uso e la revoca dell'accesso privilegiato sono regolati da specifiche procedure formali di controllo degli accessi.

Tutto il personale che opera in ruoli amministrativi o privilegiati è identificabile in modo univoco e responsabile delle proprie azioni. Le attività amministrative sono registrate e tracciabili fino ai singoli utenti, garantendo la responsabilità e supportando i requisiti di audit e conformità.

4.4 Controlli sul personale

Actalis garantisce che i membri del personale assegnati al servizio di Certification Authority siano adeguatamente qualificati per i compiti a loro assegnati, sulla base di istruzione, formazione, addestramento, abilità ed esperienza adeguati, e privi di conflitti di interesse che possano compromettere la necessaria imparzialità e il rispetto delle procedure.

Nel caso di nuove assunzioni, Actalis si riserva sempre il diritto di valutare quale tipo di formazione sia necessaria in relazione ai compiti da assegnare, alle qualifiche e all'esperienza esistenti e, ove necessario, provvede all'inserimento della persona in un piano di formazione.

4.5 Audit logging

Actalis implementa meccanismi di registrazione dei dati che coprono gli eventi operativi e rilevanti per la sicurezza associati al Servizio di firma remota e gestione dei QSCD e all'infrastruttura di supporto.

Gli eventi di audit sono registrati in conformità con i requisiti stabiliti dalle norme ETSI EN 319 401, ETSI TS 119 431 e UNI EN 419241 e dalla legislazione nazionale applicabile. L'ambito degli eventi registrati comprende tutte le categorie richieste dalle norme e dal quadro normativo sopra citati, nella misura in cui siano applicabili al servizio fornito.

Gli *audit log* sono opportunamente protetti per garantirne l'integrità e la riservatezza dei dati.

Vengono implementate misure tecniche e organizzative adeguate per impedire l'accesso non autorizzato, la modifica o la cancellazione dei registri di audit. L'accesso ai registri di audit è limitato al personale autorizzato con ruoli di fiducia definiti.

4.6 Archiviazione delle registrazioni

I registri di audit – *audit log* - vengono conservati per un periodo di 20 anni in conformità con la legislazione nazionale applicabile.

I sistemi di archiviazione WORM su cui vengono registrati i registri di audit sono replicati in due data center geograficamente separati, garantendo l'integrità, la durata e la disponibilità dei registri conservati.

4.7 Rinnovo del certificato

Per il rinnovo del certificato si rimanda al paragrafo 4.6 del CPS.

4.8 Compromissione e disaster recovery

Il Sistema di Gestione della Sicurezza delle Informazioni (ISMS) di Actalis S.p.A., conforme allo standard ISO/IEC 27001, prevede procedure di gestione degli incidenti e delle violazioni.

La gestione di un incidente di sicurezza informatica avviene attraverso una procedura articolata in più fasi, ciascuna delle quali ha uno scopo specifico, coordinata da un comitato interno (Comitato per la sicurezza e la gestione delle crisi, di seguito "Comitato") composto da persone con diverse responsabilità e da membri della Direzione. Di seguito sono descritte le fasi in cui è organizzato il processo:

- Rilevamento: fase in cui chiunque (dipendente, collaboratore o qualsiasi parte interessata) che rilevi un possibile incidente lo comunichi al Comitato. Il Comitato si assicura che la segnalazione sia il più dettagliata possibile e che chi ha riscontrato il problema non intraprenda alcuna azione in modo autonomo.
- Identificazione e analisi: il Comitato accoglie la segnalazione e valuta se si tratti effettivamente di un incidente di sicurezza. In caso affermativo, ne valuta la gravità e procede con le fasi successive. In caso contrario, chiude semplicemente l'incidente.

- Contenimento: in questa fase, per quanto possibile, gli effetti dannosi causati dall'incidente vengono limitati al fine di impedire che si diffondano ad altre aree dell'organizzazione.
- Raccolta delle evidenze: fase in cui si ricercano e raccolgono le evidenze da allegare alla documentazione dell'incidente in caso di possibili conseguenze legali o qualora fosse necessario procedere con indagini più approfondite. Tutte le prove vengono raccolte seguendo linee guida volte a garantirne una raccolta corretta e affidabile.
- Rimozione e ripristino: fase in cui viene risolta e/o rimossa la causa del danno e, attraverso le procedure di ripristino, vengono riattivati i sistemi coinvolti nell'incidente, consentendo ai sistemi e agli utenti di tornare al lavoro.
- Chiusura e notifica dell'incidente: una volta terminata la fase di ripristino, l'incidente è considerato chiuso. In questa fase, la chiusura viene notificata ai vari responsabili coinvolti

Per ulteriori informazioni si rimanda al CPS.

4.9 Cessazione del servizio

Actalis può decidere, in qualsiasi momento e per qualsiasi motivo, di cessare il proprio Servizio di Firma Remota e gestione dei QSCD.

Actalis mantiene un *Piano di Cessazione* formalmente documentato e aggiornato che disciplina la cessazione ordinata e controllata del servizio, progettato per ridurre al minimo qualsiasi tipo di impatto negativo e garantire la piena conformità ai requisiti legali e normativi applicabili. Tale piano deve:

- almeno 90 giorni prima della data di cessazione prevista, garantire una notifica tempestiva e appropriata ai Titolari, nonché all'Organismo di Vigilanza nazionali (AgID) e al *conformity assessment body* (CAB);

- garantire che qualsiasi interruzione derivante dalla cessazione del servizio di firma remota e gestione dei QSCD sia ridotta al minimo e gestita in modo controllato;

- garantire la conservazione e la salvaguardia delle evidenze, dei registri, dei log e dei dati a valore legale relativi al servizio per il periodo di tempo prescritto dalla legge, compreso, ove applicabile, il loro trasferimento sicuro e controllato a una terza parte affidabile al fine di garantire la continuità della disponibilità e il rispetto degli obblighi normativi;

- garantire che i servizi di informazione sullo stato dei certificati (compresi i servizi OCSP e CRL) continuino ad essere forniti e mantenuti per il periodo normativo applicabile successivo alla cessazione, compreso, ove necessario, il trasferimento ordinato di tali servizi ad un altro fornitore di servizi fiduciari qualificato;

- garantire la distruzione sicura, al momento della cessazione ed in conformità con le politiche e gli standard di sicurezza applicabili, di qualsiasi chiave privata sotto il controllo di Actalis utilizzata per operazioni di firma remota;

Tutte le attività di cessazione devono essere condotte in conformità con il quadro normativo UE e italiano applicabile.

La cessazione del Servizio di Firma Remota e Gestione QSCD non comporta automaticamente la cessazione dei servizi di Autorità di Certificazione di Actalis S.p.A. Per la cessazione delle attività di Certification Authority si rimanda al par. 5.8 del CPS.

5 SICUREZZA ORGANIZZATIVA E TECNICA

5.1 Gestione dei sistemi e della sicurezza

Actalis ha istituito e mantiene una struttura organizzativa per la gestione dei sistemi informatici e della sicurezza in conformità con ETSI EN 319 401, ETSI EN 319 411-1 e la legislazione applicabile.

I ruoli di fiducia, *Trusted Roles*, e le responsabilità per la sicurezza sono formalmente definiti, documentati e assegnati dalla Direzione tramite nomine formali.

I requisiti di idoneità, competenza e indipendenza associati a ciascun ruolo vengono rivisti almeno una volta all'anno e ogni volta che si verificano cambiamenti organizzativi o strutturali significativi. I titolari dei ruoli possono essere supportati da personale qualificato, a condizione che tale delega rimanga soggetta ad autorizzazione formale e conforme alle politiche di sicurezza interne.

Le responsabilità e i compiti operativi sono strutturati in modo da garantire un'efficace *segregation of duties*, in particolare per quanto riguarda i dispositive e le infrastrutture critiche per l'erogazione dei servizi fiduciari. L'assegnazione delle funzioni impedisce a qualsiasi individuo di scavalcare o aggirare in modo indipendente i controlli di sicurezza stabiliti a protezione dei sistemi e delle risorse correlate.
I Trusted Roles o il personale addetto a operazioni critiche dal punto di vista della sicurezza sono tenuti ad operare in assenza di conflitti di interesse che potrebbero compromettere l'integrità, l'imparzialità o la sicurezza dei servizi forniti.

Actalis ha definito e implementato specici Ruoli di Fiducia e specifiche responsabilità di sicurezza come parte del proprio quadro di governance dei sistemi e della sicurezza:

- **Security Officer**: responsabile nel complesso per l'implementazione e la gestione delle procedure di sicurezza;
- **System Administrator**: responsabile per l'installazione, la configurazione e il mantenimento dei sistemi del servizio di Firma Remota e gestione dei QSCD. Tra i System Administrator è ricompresa la figura del "*Responsabile della Conduzione Tecnica dei Sistemi*" in conformità con le normative vigenti;
- **System Operator:** responsabile per l'operatività quotidiana dei sistemi del Servizio di firma remota e gestione dei QSCD;
- **System Auditor**: responsabile della verifica degli archivi e dei log di audit dei sistemi.

In conformità alla normativa nazionale vigente, in particolare all'art. 38 del Decreto del Presidente del Consiglio dei Ministri (DPCM) del 22 febbraio 2013, Actalis ha inoltre formalmente definito:

- *Responsabile dei servizi tecnici e logistici;*
- *Responsabile delle verifiche e delle ispezioni (auditing);*
- *Responsabile della sicurezza.*

5.2 Sicurezza operativa

Actalis gestisce l'infrastruttura del servizio di firma remota e gestione dei QSCD in conformità tramite procedure di sicurezza operativa formalmente definite, al fine di garantire il corretto e sicuro funzionamento dei dispositivi QSCD e dei relativi servizi informatici e componenti.

Prima di essere messo in servizio, ogni dispositivo QSCD viene sottoposto a procedure di verifica volte a confermarne l'integrità, la corretta installazione e la corretta configurazione. Tali controlli includono la convalida dei meccanismi *anti-tampering*, la verifica dello stato del dispositivo e la conferma della sua conformità ai parametri operativi previsti. I dispositivi vengono attivati solo dopo il completamento con esito positivo dei suddetti controlli preventivi.

I dispositivi QSCD sono configurati e gestiti in stretta conformità con le condizioni definite nella loro documentazione di certificazione e nelle specifiche tecniche applicabili. Actalis garantisce che i dispositivi rimangano nell'ambito della configurazione certificata e siano utilizzati esclusivamente nelle modalità operative descritte nella relativa documentazione tecnica e nelle politiche di sicurezza.

Vengono inoltre implementate misure di protezione adeguate per salvaguardare i sistemi da modifiche non autorizzate o software dannosi garantendo così l'integrità dei processi crittografici e delle informazioni.

5.3 Sicurezza dei sistemi

Actalis applica controlli di sicurezza del ciclo di vita a tutti i sistemi che supportano il servizio di firma remota e gestione dei QSCD, garantendo che i requisiti di sicurezza siano implementati e mantenuti durante le fasi di sviluppo, implementazione, funzionamento e manutenzione.

Le modifiche ai sistemi sono gestite attraverso procedure formali di *change-management*, che includono la valutazione dell'impatto sulla sicurezza, l'approvazione, la tracciabilità e il rilascio controllato negli ambienti di produzione.

Il servizio di firma remota e gestione dei QSCD implementa inoltre meccanismi di monitoraggio in grado di rilevare eventi anomali che potrebbero impattare sul servizio erogato. Tali eventi generano avvisi tempestivi e attivano notifiche al personale amministrativo e di sicurezza designato per garantire un'analisi della possibile problematica e una risposta rapida ed efficace.

Per ulteriori informazioni si rimanda al paragrafo 6.5 del CPS.

5.4 Sicurezza del ciclo di vita

Actalis garantisce che i controlli di sicurezza siano applicati durante l'intero ciclo di vita dei servizi e dei sistemi a supporto dei propri servizi fiduciari, incluso il servizio di firma remota e gestione dei QSCD.

Le attività di sviluppo del software vengono svolte in conformità con il Sistema di Gestione della Qualità (SGQ) dell'azienda, conforme alla norma UNI EN ISO 9001. Inoltre, Actalis gestisce un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) allineato alla norma ISO/IEC 27001, che copre tutte le aree organizzative coinvolte nello sviluppo e nella fornitura dei servizi di fiducia.

Le attività relative al ciclo di vita dei sistemi, comprese le modifiche e gli aggiornamenti, sono regolate da procedure aziendali di *change management* consolidate e formali, al fine di garantire un'evoluzione controllata e sicura dell'infrastruttura e dei sistemi.

Per ulteriori informazioni si rimanda al paragrafo 6.6 del CPS.

5.5 Sicurezza di rete

L'accesso agli host on-line della CA è protetto da firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni. Prima dei firewall, una batteria di router che implementano opportune ACL (Access Control List) costituisce un'ulteriore barriera di protezione. Sui server del servizio di CA, tutte le porte di comunicazione non necessarie sono disattivate. Sono attivi esclusivamente quegli agenti che supportano i protocolli e le funzioni necessarie per il funzionamento del servizio.

Per irrobustire il filtraggio delle comunicazioni tutto il sistema di certificazione è suddiviso in un'area esterna, una interna ed una DMZ.

Actalis commissiona almeno trimestralmente un Vulnerability Assessment (VA) per verificare l'eventuale presenza di vulnerabilità, avvalendosi di specialisti indipendenti.

Per ulteriori informazioni, si prega di consultare il CPS par. 6.7.

6 AUDIT DI CONFORMITÀ E ALTRE VALUTAZIONI

La conformità al Regolamento eIDAS e alle norme ETSI applicabili del Servizio di firma remota e gestione dei QSCD di Actalis S.p.A. descritta nel presente Practice Statament viene verificata su base annuale da un Organismo di Valutazione accreditato (*Conformity Assessment Body, CAB*).

Inoltre, sempre su base annuale, viene eseguito un audit interno sui servizi di Certification Authority che tiene conto anche degli aspetti relativi alla sicurezza delle informazioni, alle leggi applicabili in materia di protezione dei dati e alle politiche e procedure interne.

Per ulteriori informazioni, si rimanda al capitolo 8 del CPS.

7 CONDIZIONI GENERALI

7.1 Tariffe del servizio

Per ulteriori informazioni, si rimanda al paragrafo 9.1 del CPS.

7.2 Copertura assicurativa

Actalis ha stipulato una polizza assicurativa specifica con una compagnia assicurativa di prim'ordine a copertura dei rischi derivanti dalla fornitura del Servizio di firma remota e gestione dei QSCD. In particolare, l'assicurazione prevede un massimale di indennizzo per sinistro e per periodo assicurativo pari a € 1.500.000.

7.3 Riservatezza delle informazioni

Per ulteriori informazioni si rimanda al paragrafo 9.3 del CPS.

7.4 Programma sulla privacy

Actalis è il titolare del trattamento dei dati personali raccolti in sede di identificazione e registrazione degli utenti richiedenti certificati ed è pertanto tenuta a trattare tali dati con la massima riservatezza e in conformità alle disposizioni del D.Lgs. 196/03 e del Regolamento (UE) 2016/679.

Per ulteriori informazioni, visitare il sito web di Actalis https://www.actalis.com .

7.5 Diritti di proprietà intellettuale

7.6 Dichiarazioni e garanzie

Per ulteriori informazioni si rimanda al paragrafo 9.6 del CPS.

7.7 Limitazione di responsabilità

Gli obblighi e le responsabilità di Actalis sono esclusivamente quelli definiti nel presente documento e nel Contratto di fornitura del Servizio. La Certification Authority è responsabile dei danni causati, dolosamente o per negligenza, a qualsiasi persona fisica o giuridica in caso di inadempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente nei casi e nei limiti stabiliti dall'art. 13 del Regolamento.

Fermo restando quanto sopra, salvo circostanze soggette a una disposizione di legge vincolante, in nessun altro caso, a nessun titolo e/o per nessun motivo Actalis potrà essere ritenuta responsabile nei confronti del Cliente, o di qualsiasi altro soggetto direttamente o indirettamente collegato o connesso al Cliente, per danni diretti o indiretti, perdita di dati, violazioni di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, verificatisi in relazione alla Prestazione del Servizio o connessi direttamente o indirettamente a, o derivanti da:

- casi di forza maggiore, cause di forza maggiore, eventi catastrofici (ad esempio, ma non solo: incendio, esplosione, sciopero, sommosse ecc.); e/o
- manomissioni o interventi che interessino il Servizio o le apparecchiature da parte del Cliente e/o di terzi non autorizzati da Actalis.

Actalis non sarà in alcun caso responsabile per l'utilizzo del Servizio in relazione a situazioni critiche, inclusi, ad esempio, rischi specifici per la sicurezza delle persone, danni all'ambiente, rischi specifici in relazione ai servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e ai dispositivi medici; in tali circostanze, Actalis si renderà disponibile a valutare e negoziare con il Cliente, nell'ambito dei rispettivi "SLA", un accordo specifico "mission critical".

Actalis non offre alcuna garanzia in merito alla validità e agli effetti, ivi compresi quelli probatori, del Servizio o di qualsiasi dato, informazione, messaggio, atto o documento ad esso associato o, in ogni caso, emesso, comunicato, trasferito, conservato o in qualsiasi modo trattato tramite tale Servizio:

- qualora il Cliente intenda utilizzarli o fare affidamento su di essi in paesi diversi dall'Italia, ad eccezione dei Certificati emessi sulla base del presente documento per i paesi all'interno dell'Unione Europea;
- per la loro riservatezza e/o integrità (nel senso che eventuali violazioni di quest'ultima possono normalmente essere identificate dall'Utente o dal destinatario tramite l'apposita procedura di verifica).

In nessun caso Actalis si assumerà alcuna responsabilità per le informazioni, i dati o i contenuti diffusi o trasmessi e, in ogni caso, trattati dal Cliente tramite il Servizio, né, in generale, per l'utilizzo da parte del Cliente del suddetto Servizio, e si riserva il diritto di adottare qualsiasi misura e azione volta a tutelare i propri diritti e interessi, ivi compresa la comunicazione alle persone coinvolte di informazioni che possano contribuire all'identificazione del Cliente.

7.8 Indennizzi

7.8.1 Indennizzo ai contraenti

Actalis ha stipulato una specifica polizza assicurativa a copertura dei rischi di attività e di eventuali danni derivanti dalla prestazione del servizio di certificazione (cfr. sezione 7.2).

Nel caso in cui i certificati rilasciati da Actalis prevedano limitazioni d'uso – incluse limitazioni sul valore delle transazioni per le quali il certificato è valido, o limitazioni sulle finalità per le quali il certificato può essere utilizzato – Actalis non sarà responsabile per i danni derivanti da un uso improprio.

In ogni caso, il risarcimento dei danni a terzi non potrà superare l'importo massimo annuo complessivo di 1.250.000 € (un milione e duecentocinquantamila euro), comprese le spese di liquidazione del sinistro.

In caso di danno derivante dalle attività oggetto del Contratto, la Parte contraente è tenuta, a pena di decadenza:

- presentare reclamo ad Actalis entro 24 ore dal verificarsi del fatto, o dal momento in cui ne venga a conoscenza (fornendo conferma successivamente tramite lettera raccomandata con avviso di ricevimento, o tramite PEC entro le successive 24 ore);

- entro sei mesi dalla presentazione del reclamo di cui al punto precedente, quantificare l'eventuale danno subito e presentare la relativa richiesta di risarcimento.

7.8.2 Risarcimento ad Actalis

Fatte salve le Condizioni Generali di Fornitura, le Parti contraenti sono tenute a risarcire eventuali danni subiti da Actalis nei seguenti casi:

- falsa dichiarazione (ad es. circa l'identità del Richiedente) nella richiesta del certificato;
- omessa informazione su atti o fatti essenziali, sia per negligenza che intenzionale;
- omessa custodia dei dati di attivazione (es. PIN) della propria chiave privata;
- utilizzo di nomi in violazione dei diritti di proprietà intellettuale di altri soggetti.

7.9 Durata e risoluzione del contratto

7.9.1 Durata del Contratto

Il Contratto ha inizio alla data della sua accettazione da parte della Parte contraente e termina alla data di scadenza del certificato rilasciato da Actalis ; in caso di rinnovo del certificato stesso, il periodo di validità del Contratto è prorogato fino alla data di scadenza del certificato rinnovato. In ogni caso, la validità del Contratto cessa in conseguenza della revoca del certificato, a qualsiasi titolo.

7.9.2 Risoluzione del Contratto

Si rimanda alle Condizioni Generali pubblicate sul sito web della Certification Authority.

7.9.3 Effetti della risoluzione

In caso di risoluzione del contratto, il certificato del Titolare viene revocato dalla Certification Authority.

7.10 Avvisi individuali e comunicazioni con i partecipanti

Per ulteriori informazioni si rimanda al paragrafo 1.5.1 del CPS.

7.11 Modifiche del documento

Actalis si riserva il diritto di apportare modifiche al presente documento in qualsiasi momento, senza preavviso, per esigenze tecniche o organizzative o a seguito di modifiche legislative.
Ogni nuova versione del Practice Statement / Manuale Operativo annulla e sostituisce le versioni precedenti.

Modifiche significative al documento, ad esempio quelle che incidono sulle procedure operative, sul profilo dei certificati, ecc., vengono concordate con l'organismo di valutazione della conformità (CAB) e l'Autorità di Vigilanza nazionale (AgID) prima della loro pubblicazione.

Inoltre, il presente Practice Statament viene rivisto da Actalis e, se necessario, aggiornato almeno una volta all'anno anche in assenza di modifiche al Quadro normativo.

Le nuove versioni sono pubblicate su https://www.actalis.com/it/legal-repository.

7.12 Foro competente

Il Foro di Arezzo è competente in via esclusiva per la risoluzione di tutte le controversie legali in cui Actalis S.p.A. sia attrice o convenuta e relative all'utilizzo del servizio di certificazione, alle procedure operative e all'applicazione delle disposizioni del presente documento.

7.13 Legge applicabile

Il contratto è soggetto al diritto italiano ed europeo e come tale deve essere interpretato ed eseguito. Per quanto non espressamente previsto nel contratto, il servizio CA è regolato dalle leggi vigenti.

7.14 Conformità alla normativa applicabile

Il principale quadro normativo applicabile è riportato di seguito:

I. Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo per l'identità digitale (eIDAS 2).

II. Regolamento di esecuzione (UE) 2025/1567 del 29 luglio 2025 che stabilisce le norme di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda la gestione dei dispositivi di creazione di firma elettronica qualificata a distanza e dei dispositivi di creazione di sigillo elettronico qualificato a distanza come servizi di fiducia qualificati.

III. Decreto Legislativo n. 82 del 7 marzo 2005: "Codice della Pubblica Amministrazione Digitale", G.U. n. 112 del 16 maggio 2005, e successive integrazioni e modifiche.

IV. Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013: "Norme tecniche per la generazione, l'applicazione e la verifica delle firme elettroniche avanzate, qualificate e digitali...", G.U. n. 117 del 21 maggio 2013.

V. Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali", G.U. n. 174 del 29 luglio 2003, e successive integrazioni e modifiche.

VI. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

VII. Direttiva UE 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno ecc., Gazzetta ufficiale dell'Unione europea L 337 del 23 dicembre 2015.

VIII. Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione relative all'autenticazione forte del cliente e agli standard di comunicazione aperti, comuni e sicuri.

7.15 Informazioni di contatto

Per qualsiasi domanda o dubbio riguardante i presenti Termini o l'utilizzo del Servizio di firma remota e gestione dei QSCD è possibile contattare Actalis attraverso:

- Il call center tramite i canali indicati su https://assistenza.aruba.it
- Comunicazione mail all'indirizzo CPS-requests@ca.arubapec.it

7.16 Trasparenza

Nella fornitura del Servizio, Actalis S.p.A. opera in conformità con i principi di trasparenza, non discriminazione e parità di trattamento dei richiedenti.

Il Servizio è messo a disposizione di qualsiasi richiedente che accetti di rispettare i termini e le condizioni applicabili, inclusi gli obblighi definiti nel presente Practice Statament e nella relativa documentazione contrattuale.
Actalis mantiene un'adeguata capacità finanziaria e, ove richiesto dalla legislazione applicabile, un'adeguata copertura assicurativa per far fronte a potenziali responsabilità derivanti dalla fornitura del servizio. L'organizzazione garantisce la stabilità finanziaria e le risorse operative necessarie per mantenere la conformità continua ai requisiti legali, normativi e tecnici applicabili.

Laddove la fornitura del Servizio coinvolga subappaltatori, componenti esternalizzati o altri accordi con terze parti, Actalis garantisce che siano in essere accordi formali. Tali accordi definiscono ruoli, responsabilità e obblighi di sicurezza e assicurano che il Fornitore di Servizi Fiduciari mantenga la piena responsabilità per la conformità ai requisiti applicabili.

Sono inoltre stabilite procedure documentate per la gestione e la risoluzione di reclami, richieste di risarcimento e controversie presentate dagli Abbonati o dalle parti che fanno affidamento sul servizio in relazione alla fornitura dello stesso.

7.17 Test aggiuntivi

Nessuna previsione.

7.18 Disabilità

Nessuna previsione.

7.19 Termini e condizioni

I termini e le condizioni per i richiedenti e I titolari del servizio sono disponibili all'indirizzo https://www.actalis.com/it/legal-repository.