Allegato Tecnico

Certificati di sottoscrizione qualificati e di autenticazione su dispositivo o CNS, Certificati e servizi di firma e sigillo qualificati remoti

1. RIFERIMENTI ESTERNI

Documentazione	Link di dettaglio
CP e CPS (Manuale Operativo) per emissione certificati qualificati	https://qtsp.infocert.it/pdf/ICERT_INDI_MO.pdf
CP e CPS (Manuale operativo) per emissione certificati di Autenticazione	https://qtsp.infocert.it/pdf/ICERT_INDI_MOCA.pdf
SP e PS (Manuale Operativo) per servizi di firma e sigillo remoti qualificati	ICERT INDI SSAS
SP e PS (Manuale Operativo) del Servizio di Verifica dell'Identità	https://qtsp.infocert.it/pdf/ICERT-INDI-IPSPS-ITA.pdf
CP per certificati di autenticazione CNS	https://qtsp.infocert.it/pdf/ICERT_INDI_CPCA_CNS.pdf
PDS (PKI Disclosure Statement) per i certificati qualificati	https://qtsp.infocert.it/pdf/ICERT_INDI_PDS.pdf
Link di supporto (FAQ, Video, Guide)	https://help.infocert.it/cerca? = searchText Firma%20Digitale&idProdotto=33

2. DESCRIZIONE DEL SERVIZIO – INTRODUZIONE

Tinexta Infocert S.p.A. (di seguito, "Infocert"), nel contesto del presente documento, opera in qualità di prestatore di servizi fiduciari qualificati (di seguito, "QTSP" – Qualified Trust Service Provider), ai sensi del Regolamento (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183 (di seguito, il "Regolamento eIDAS"), per l'erogazione dei servizi di:

- emissione di certificati qualificati di firma elettronica e sigillo elettronico, su dispositivo fisico o in modalità remota;
- emissione di certificati di autenticazione, inclusi quelli su dispositivi CNS (Carta Nazionale dei Servizi);

- erogazione di servizi di firma e sigillo elettronico qualificati in modalità remota.

Tali servizi (di seguito, congiuntamente, il "Servizio") sono erogati in conformità ai rispettivi Manuali Operativi (di seguito anche "CPS" – Certificate Practice Statement o "PS" – Practice Statement) e, ove applicabile, al PKI Disclosure Statement (PDS) di Infocert.
Per i Servizi sopra indicati, Infocert ha ottenuto una valutazione di conformità da parte dell'organismo di valutazione della conformità CSQA Certificazioni S.r.l., ai sensi del Regolamento eIDAS e delle norme ETSI applicabili, tra cui ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 ed ETSI TS 119 431, secondo lo schema di valutazione eIDAS definito da ACCREDIA, in conformità alle norme ETSI EN 319 403 e UNI CEI EN ISO/IEC 17065:2012.
Infocert è inoltre accreditata presso l'Agenzia per l'Italia Digitale (AgID) ed è inclusa nella Trusted List europea dei prestatori di servizi fiduciari qualificati (Trusted Service List – TSL), pubblicata dalla Commissione Europea.
Nell'ambito dei Servizi oggetto del presente Allegato Tecnico:

- Infocert opera in qualità di Certification Authority (CA) per le attività di identificazione dei soggetti, emissione e gestione dei certificati qualificati e di autenticazione;
- Infocert opera altresì in qualità di Server Signature Application Service Provider ("SSASP") per i servizi di firma e sigillo elettronico qualificati in modalità remota, inclusa la gestione dei dispositivi remoti di creazione della firma o del sigillo.

I certificati qualificati e i servizi di firma e sigillo elettronico qualificati consentono la sottoscrizione di documenti informatici con effetti giuridici ai sensi del Regolamento eIDAS. In particolare, la firma elettronica qualificata produce gli effetti giuridici equivalenti a quelli della firma autografa.
I certificati di autenticazione consentono invece l'identificazione informatica del titolare e l'accesso sicuro a sistemi e servizi digitali, garantendo l'associazione univoca tra il soggetto e le credenziali utilizzate.
Il Servizio si basa su meccanismi crittografici a chiave pubblica, che garantiscono l'autenticità dell'origine, l'integrità dei dati e il non ripudio delle operazioni effettuate. A tal fine, a ciascun soggetto è associata una coppia di chiavi crittografiche (pubblica e privata), collegata a un certificato digitale (di seguito, il "Certificato") contenente i dati identificativi del titolare.
Le chiavi crittografiche sono generate, custodite e utilizzate mediante dispositivi sicuri per la creazione della firma o del sigillo (Qualified Signature/Seal Creation Device – QSCD), che possono consistere in:

- dispositivi fisici nella disponibilità del titolare (es. smart card, token USB);
- dispositivi remoti gestiti da InfoCert all'interno di infrastrutture ad alta sicurezza

I certificati e i servizi associati sono identificati tramite specifici Object Identifier (OID), che definiscono il prestatore, la tipologia di utilizzo e le policy applicabili. La descrizione dettagliata degli OID è contenuta nei rispettivi Manuali Operativi.

Il presente Allegato Tecnico costituisce parte integrante e sostanziale del contratto di acquisto dei servizi (di seguito, l"Accordo"), stipulato con il Cliente.
Ai soggetti che attivano, utilizzano o fanno affidamento sul Servizio si applicano le Condizioni Generali di Attivazione (di seguito, "CGA"), di cui il presente Allegato Tecnico costituisce parte integrante, fermo restando che, nei rapporti con il Cliente, trovano applicazione anche le disposizioni dell'Accordo.

2.1 Definizione Delle Parti

Cliente
Persona fisica o giuridica che ha stipulato il contratto di acquisto dei Servizi ("Accordo"), assumendone i relativi oneri economici. Il Cliente può coincidere con il Richiedente.

Soggetto / Titolare
Persona fisica o giuridica a cui è intestato il Certificato.
Nel caso di certificati intestati a persona fisica, il Soggetto/Titolare è la persona cui sono associati i dati contenuti nel Certificato e che utilizza il Certificato nell'ambito del Servizio.
Nel caso di certificati intestati a persona giuridica, il Soggetto/Titolare è l'organizzazione cui il Certificato è riferito

Richiedente
Persona fisica o giuridica che richiede a Infocert il rilascio dei Certificati e/o l'attivazione del Servizio. Il Richiedente può coincidere con il Soggetto, nel caso in cui richieda un Certificato per sé stesso, oppure può essere un soggetto terzo che richiede il Servizio per conto di uno o più Soggetti.

In particolare, il Richiedente può:

- richiedere certificati per sé stesso, in qualità di persona fisica e coincidere con il Soggetto;
- richiedere certificati riferiti a una persona giuridica, agendo in qualità di rappresentante o delegato della stessa;
- essere un'organizzazione che richiede il Servizio per soggetti ad essa collegati, nell'ambito di rapporti ad esempio commerciali (es. clienti) o di una struttura organizzativa (es. dipendenti o collaboratori).

Utente / Relying Party
Soggetto che fa affidamento su un certificato, una firma elettronica, un sigillo elettronico o un processo di autenticazione basato su certificato, ai fini della verifica dell'identità del Soggetto, dell'origine del documento o dell'integrità dei dati.

Ente Emettitore
Soggetto responsabile del rilascio di dispositivi fisici (quali smart card o token) destinati a contenere certificati di autenticazione CNS (Carta Nazionale dei Servizi). L'Ente Emettitore è responsabile del processo di emissione e della gestione del ciclo di vita del dispositivo CNS.

Terzo Interessato
Persona fisica o giuridica interessata alle informazioni contenute nel Certificato relative al ruolo e/o all'organizzazione del Soggetto, nonché legittimata, nei casi previsti, a richiederne la modifica, sospensione o revoca. Può coincidere con il Richiedente.

3. SPECIFICHE TECNICO-NORMATIVE

3.1 Rilascio e Utilizzo del Servizio

Il Servizio è erogato da Infocert in favore del Soggetto, nel rispetto del presente Allegato Tecnico, delle Condizioni Generali di Attivazione (CGA), della normativa applicabile e dei Manuali Operativi di riferimento.
Il rilascio dei certificati e l'attivazione del Servizio sono subordinati alla presentazione di una richiesta di attivazione predisposta da Infocert (di seguito, la "Richiesta di Attivazione"). Tale richiesta consiste in un modulo, anche in formato elettronico, che richiama espressamente il presente Allegato Tecnico, le CGA e la Privacy Policy come condizioni contrattuali del Servizio.
Nel caso di certificati intestati a una persona fisica, la Richiesta di Attivazione è accettata o firmata dal Soggetto.
Nel caso di certificati intestati a una persona giuridica, la Richiesta di Attivazione è accettata o firmata dal Richiedente, in qualità di rappresentante o soggetto delegato, secondo quanto previsto nei Manuali Operativi.
L'attivazione del Certificato da parte di Infocert è subordinata al completamento con esito positivo della procedura di identificazione del Soggetto, svolta secondo le modalità descritte nei Manuali Operativi. In caso di esito negativo della procedura di identificazione, non è possibile fruire del Certificato.
Il Servizio si considera attivato a seguito della accettazione della Richiesta di Attivazione e della conseguente emissione del Certificato, unitamente alla generazione della coppia di chiavi crittografiche, effettuata su dispositivo fisico o, nel caso di Servizi remoti, su infrastrutture gestite da Infocert in qualità di SSASP.
Il Certificato può essere utilizzato dal Soggetto per la sottoscrizione di documenti informatici o per l'autenticazione ai servizi digitali, mediante strumenti nella sua disponibilità o messi a disposizione da Infocert o dal Richiedente, secondo le modalità previste dal Servizio.
Infocert, in qualità di Certification Authority e, ove applicabile, di Server Signature Application Service Provider (SSASP), conserva le informazioni relative all'identità del Soggetto, al Certificato, alle chiavi crittografiche e ai log di servizio per un periodo non inferiore a venti (20) anni dalla scadenza del Certificato e comunque non superiore a ventitré (23) anni dalla sua data di emissione, secondo quanto previsto dalla normativa applicabile e dai Manuali Operativi.
In caso di cessazione dell'attività, Infocert provvede al trasferimento delle informazioni di cui sopra a un soggetto terzo che garantisca il rispetto delle medesime condizioni di sicurezza e conservazione, secondo quanto previsto dalla normativa applicabile e dai Manuali Operativi.
Le CGA, il presente Allegato Tecnico, i relativi Manuali Operativi e la documentazione informativa applicabile sono resi disponibili da Infocert sul proprio sito istituzionale e possono essere consultati dal Soggetto, dal Richiedente e dalle parti facenti affidamento prima dell'attivazione e durante l'utilizzo del Servizio

3.1.1 Certificato Digitale e chiavi crittografiche

Il Certificato digitale è un documento elettronico, emesso e firmato da Infocert in qualità di Certification Authority, che attesta l'associazione tra l'identità del Soggetto e una coppia di chiavi crittografiche (chiave pubblica e chiave privata), utilizzate per la firma elettronica, il sigillo elettronico o per l'autenticazione.
La chiave privata è utilizzata dal Soggetto per effettuare le operazioni di firma, sigillo o autenticazione, mentre la chiave pubblica è resa disponibile tramite il Certificato ai fini della

verifica delle stesse.
Le chiavi crittografiche sono generate e utilizzate mediante dispositivi crittografici sicuri, in conformità alla normativa applicabile e ai Manuali Operativi di riferimento.
Infocert garantisce la corretta associazione tra il Soggetto, il Certificato e le chiavi crittografiche, secondo quanto previsto dalla normativa applicabile e dai Manuali Operativi.
Il Certificato può contenere limitazioni d'uso e/o di valore. Le eventuali limitazioni d'uso del Certificato sono indicate nel Certificato stesso e/o nei Manuali Operativi.

3.1.2 Processo di verifica di identità

L'identificazione del Soggetto è un'attività svolta da Infocert in qualità di Certification Authority (CA) o da un soggetto delegato operante come Registration Authority (RA).
Le modalità di identificazione sono definite nel Manuale Operativo IPSPS e sono conformi alla normativa applicabile.

A) Persona fisica

L'identificazione del Soggetto avviene mediante una delle modalità previste e si basa sulla verifica dell'identità attraverso documenti di riconoscimento e/o strumenti di identificazione elettronica, nonché sulla raccolta delle informazioni necessarie all'emissione del Certificato.

B) Persona giuridica

Nel caso di rilascio di certificati o sigilli intestati a una persona giuridica, il soggetto che richiede il certificato (rappresentante legale o delegato) è identificato secondo le modalità previste per le persone fisiche.
Infocert procede inoltre alla verifica dei poteri di rappresentanza del soggetto richiedente e dei dati relativi alla persona giuridica, ai fini del rilascio del certificato e della corretta associazione dello stesso.

3.1.3 Processo di Autenticazione

L'utilizzo della chiave privata associata a un certificato è subordinato all'autenticazione del Soggetto, al fine di garantire il controllo esclusivo sull'uso dei dati per la creazione della firma o del sigillo elettronico.
L'autenticazione del Soggetto avviene mediante l'utilizzo di credenziali e/o dispositivi a lui associati, secondo le modalità previste dal Servizio e dai Manuali Operativi.
Nel caso di dispositivi di firma e/o autenticazione (quali smart card, token o CNS), l'autenticazione avviene mediante l'utilizzo di un codice personale o altro meccanismo equivalente previsto dal dispositivo.
Nel caso di servizi di firma o sigillo remoti, l'autenticazione è gestita da Infocert, in qualità di SSASP, o da un soggetto delegato, mediante i meccanismi previsti dal Servizio.
Il processo di autenticazione e attivazione garantisce che l'utilizzo della chiave privata avvenga sotto il controllo esclusivo del Soggetto e che ogni operazione sia a lui riconducibile.

3.1.4 Rinnovo del Servizio e riemissione del certificato con nuova chiave

Il rinnovo del Servizio consiste nella prosecuzione dello stesso oltre la sua scadenza, ove prevista, e, nel caso dei certificati, comporta l'emissione di un nuovo Certificato e la generazione di una nuova coppia di chiavi crittografiche.
Il rinnovo può essere richiesto prima della scadenza del Certificato o del Servizio, secondo le

modalità previste nei Manuali Operativi.
Il rinnovo non è ammesso nei casi previsti dal Manuale Operativo e in ogni caso, qualora sia intervenuta la scadenza, revoca o sospensione del Certificato o del Servizio e qualora i dati e le informazioni associati al Soggetto non risultino più validi o aggiornati. In tali casi è necessaria una nuova attivazione. La procedura prevista per la riemissione del certificato è descritta nel manuale operativo di riferimento.

3.1.5 Sospensione o Revoca del Servizio

Il Certificato o il Servizio possono essere sospesi o revocati, secondo le modalità previste nei Manuali Operativi.
La sospensione o la revoca possono avvenire su richiesta del Soggetto o del Richiedente, ove previsto, ovvero su iniziativa di Infocert nei casi stabiliti dalla normativa applicabile o dai Manuali Operativi.
La sospensione comporta l'interruzione temporanea della validità del Certificato o dell'utilizzo del Servizio, mentre la revoca ne determina la cessazione definitiva.
A seguito della sospensione o della revoca, non è più consentito l'utilizzo del Certificato o del Servizio.
Nel caso di servizi di firma o sigillo remoti, la sospensione comporta l'inibizione dell'utilizzo delle chiavi crittografiche, mentre la revoca ne determina la distruzione, secondo quanto previsto nei Manuali Operativi.

3.1.6 Affidamento sul Servizio

Al fine di poter fare affidamento sul documento informatico sottoscritto o su un processo di autenticazione basato su Certificati, l'Utente / Relying Party è tenuto a verificare la validità del risultato del Servizio e l'idoneità dello stesso all'uso che ne vuole fare,
A tal fine, deve verificare la validità del Certificato, l'esito della firma, del sigillo elettronico o del processo di autenticazione, l'eventuale presenza di limitazione d'uso o di valore, nonché che il Certificato sia stato emesso da un prestatore di servizi fiduciari conforme alla normativa applicabile, anche mediante strumenti messi a disposizione da Infocert, validatori pubblici dell'Unione Europea o eventuali strumenti di terze parti, per i quali Infocert non presta alcuna garanzia.

3.2 Prodotti e Servizi

3.2.1 Certificati di firma qualificata e autenticazione su Dispositivo

I dispositivi in possesso del Titolare, che contengono le chiavi crittografiche del Certificato, possono contenere, oltre ai Certificati di firma qualificata, anche "Certificati di autenticazione" o "Certificati di autenticazione – CNS".
I Certificati sono identificati dagli Object Identifiers (OID), ossia un codice che identifica il QTSP, l'uso del Certificato e la policy a cui esso è conforme.
Gli OID relativi ai certificati di firma qualificata su dispositivo fisico sono descritti al paragrafo 1.2 del Manuale Operativo ICERT-INDI-MO.
Gli OID relativi ai certificati di autenticazione su dispositivo fisico sono descritti al paragrafo 1.2 del

Manuale Operativo ICERT-INDI-MOCA.
Gli OID relativi ai certificati di autenticazione CNS sono descritti al paragrafo 2.1 del Manuale Operativo ICERT-INDI-CPCA-CNS.

I dispositivi configurabili, tutti dotati di un chip crittografico al loro interno, sono i seguenti:

- Il token USB o wireless (di seguito anche *"business key")* è un dispositivo utilizzabile su qualsiasi PC dotato di porta USB o connessione wireless.
  Per utilizzare la business key è sufficiente collegarla alla porta USB o alla connessione wireless del computer, installare i driver e il software forniti (se necessario) e avviare il software di firma per selezionare i documenti da firmare o accedere ai servizi digitali online inserendo il PIN associato al dispositivo.

- La *smart card* è una tessera elettronica che richiede un lettore di smart card dedicato per poter essere utilizzata. Per utilizzare la smart card, è necessario collegare il lettore di smart card al computer tramite cavo USB, inserire la carta nel lettore, verificare il riconoscimento tramite i driver specifici e utilizzare un software compatibile per apporre firme digitali o accedere ai servizi online tramite autenticazione.

Questi dispositivi possono essere utilizzati per firmare digitalmente con il Certificato di firma qualificata o per autenticarsi a determinati servizi online tramite il Certificato di autenticazione o autenticazione CNS. Qualora venga trovata una falla di sicurezza che ne pregiudica un conforme utilizzo, il dispositivo potrebbe diventare non più utilizzabile e dovrà essere sostituito quanto prima per non invalidare le firme emesse.
I certificati possono contenere ulteriori limiti d'uso come meglio descritti nel Manuale Operativo di riferimento

3.2.1.1 Certificati di Firma Qualificata su dispositivo

Questi Certificati, vengono rilasciati su dispositivi fisici sicuri quali smart card, o business key. Il Titolare è tenuto a custodire con cura il dispositivo di firma e le relative credenziali d'accesso, adottando misure organizzative e tecniche adeguate a prevenire danni a terzi e garantire l'uso esclusivamente personale e sicuro del dispositivo e delle credenziali.
Il Certificato di Firma Qualificata ha validità di tre anni a partire dalla sua data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente alla data di scadenza.

3.2.1.2 Certificato di Autenticazione su dispositivo

Il Certificato di Autenticazione rilasciato da Tinexta Infocert funge da strumento digitale per l'autenticazione del Titolare. Il Certificato di autenticazione è utilizzato per l'identificazione informatica del Titolare e per l'accesso sicuro a servizi digitali. Le modalità di emissione, gestione e utilizzo sono definite nel Manuale Operativo ICERT-INDI-MOCA. È utilizzabile per una varietà di servizi digitali che richiedono sicurezza elevata, quali autenticazione sicura, accesso a sistemi informatici e transazioni crittografate. Il processo di emissione, gestione e uso del Certificato è strettamente regolato dal Manuale Operativo ICERT-INDI-MOCA.
Il Certificato di Autenticazione ha validità di tre anni a partire dalla sua data di emissione, ovvero

fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente alla data di scadenza.

3.2.1.3 Certificato di Autenticazione CNS – Carta Nazionale dei Servizi

Il Certificato di Autenticazione CNS è rilasciato da un "Ente Emettitore", e funge da strumento digitale per l'autenticazione del Titolare per l'accesso ai servizi online dedicati. L'Ente Emettitore conferisce a Tinexta InfoCert mandato non esclusivo a espletare la funzione di Certification Authority (CA) per il rilascio di CNS. L'Ente Emettitore autorizza Tinexta InfoCert, in qualità di CA, a delegare l'attività di richiesta e rilascio di CNS a soggetti terzi delegati da InfoCert in qualità di Ufficio di Registrazione.

Questo certificato è essenziale per garantire l'integrità e l'autenticità delle comunicazioni digitali del Titolare, associando inequivocabilmente la sua identità alla chiave pubblica registrata. Il processo di emissione, gestione e uso del Certificato è regolato dalla policy InfoCert ICERT-INDI-CPCA-CNS reperibile sul sito del Certificatore e dal manuale operativo dell'Ente Emettitore reperibile sul sito di quest'ultimo.

Le procedure operative adottate dall'Ente Emettitore e dal Certificatore stesso per l'erogazione dei servizi di certificazione digitale sono riportate nel Manuale Operativo CNS redatto e reso disponibile dall'Ente Emettitore stesso.

Il Certificato di Autenticazione CNS ha validità di tre anni a partire dalla data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data. Il Certificato e il dispositivo possono essere rinnovati una sola volta. Dopo il primo rinnovo, si dovrà procedere ad una nuova emissione del Certificato e del dispositivo

3.2.2 Certificati qualificati per Firma/Sigillo Remoti e Servizio di firma e sigillo Remoti

Nel contesto dei Servizi remoti descritti in questo paragrafo Tinexta Infocert opera come Certification Authority, con riferimento alle attività di identificazione del soggetto ed emissione del certificato qualificato, mentre opera come SSASP con riferimento alla attività di attivazione e gestione remota delle chiavi per l'utilizzo della firma qualificata associata a quello specifico certificato.

Gli OID specifici riferiti ai certificati qualificati di firma e sigillo remoti sono descritti al paragrafo 1.2 del Manuale Operativo ICERT-INDI-MO.

Gli OID specifici relativi al servizio di firma e sigillo remoti sono descritti al paragrafo 1.2 del Manuale Operativo ICERT-INDI-SSAS.

3.2.2.1 Firma Remota

In caso di richiesta di un Certificato di sottoscrizione per procedura remota, il Servizio ha ad oggetto la generazione di una coppia di chiavi crittografiche e l'emissione di un Certificato Qualificato di firma elettronica remota con durata triennale. La firma remota consente al Titolare di apporre firme digitali senza la necessità di utilizzare dispositivi fisici personali, come token USB o smart card.

I Certificati di sottoscrizione per procedure di firma remota rilasciati da Tinexta Infocert sono utilizzati mediante apposite procedure informatiche che si collegano in maniera sicura al servizio di Firma Remota erogato da Infocert in qualità di SSASP. Tale servizio viene erogato tramite, tramite l'utilizzo di un dispositivo crittografico sicuro (**QSCD**) gestito dal QTSP.

Il Servizio prevede che al Titolare sia messa a disposizione, una procedura informatica, implementata sui sistemi di Infocert o del Richiedente, se diverso dal Titolare, mediante la quale il medesimo Titolare può gestire il proprio Certificato di sottoscrizione e le proprie chiavi.
I Certificati di Firma Remota possono essere rilasciati nel dominio messo a disposizione dal Richiedente diverso dal Titolare. Qualora il Richiedente chieda il rilascio, per i Titolari, di certificati il cui utilizzo è limitato esclusivamente al dominio informatico per il quale è stato emesso, tale certificato sarà utilizzabile esclusivamente nel/i dominio/i definiti dal Richiedente stesso. Tali Certificati sono definiti Long Term e possono contenere uno dei limiti d'uso previsti dal Manuale Operativo.
Le chiavi crittografiche necessarie per la firma sono custodite in un QSCD, gestito da Infocert. Il Titolare mantiene il controllo esclusivo sull'apposizione della firma mediante un processo di autenticazione, che prevede a titolo esemplificativo l'utilizzo combinato di PIN e OTP. Ogni sessione di firma richiede una nuova autenticazione per garantire la sicurezza del processo, e le operazioni possono essere eseguite sia su desktop che su smartphone, e possono essere gestite dal SSASP o da un suo delegato.
La firma remota può essere utilizzata tramite applicativi di firma messi a disposizione da Infocert oppure può essere integrata via API dall'applicazione messa a disposizione dal Richiedente.
La firma remota prevede la configurazione di un user e una password ed è attivabile o direttamente dal processo TOP (*Trust Onboarding Platform*) o dal portale di Tinexta Infocert MySign secondo le istruzioni inviate per mail, a cui il Titolare può accedere tramite le suddette credenziali e gestire il certificato in termini di modalità di autenticazione utilizzo e revoca, oppure dalle modalità previste dall'applicazione del Richiedente.
L'utilizzo della chiave privata avviene a seguito di una specifica richiesta di firma o sigillo riferibile al Soggetto, previa autenticazione e secondo i meccanismi di sicurezza previsti dal Servizio. Il processo di attivazione della firma o del sigillo è strutturato in modo da garantire la manifestazione di volontà del Soggetto in relazione alla singola operazione e il suo controllo esclusivo sull'utilizzo della chiave privata custodita nel QSCD remoto.

3.2.2.2 Firma remota automatica

La firma automatica è una modalità di firma remota nella quale il Titolare utilizza una coppia di chiavi destinata specificamente a tale scopo, diversa da tutte le altre in suo possesso, in conformità a quanto previsto dall'art. 35, comma 3, del CAD.
Il Servizio, in aggiunta a quanto previsto dal paragrafo 3.2.2.1 del presente Allegato Tecnico, consente la generazione automatica delle firme su documenti inviati attraverso procedure informatiche automatizzate. In tal caso non è richiesta una conferma puntuale per ogni singola operazione, in quanto la volontà del Titolare è espressa nell'ambito della procedura automatizzata previamente autorizzata. La gestione del servizio di firma automatica comprende l'autenticazione del Titolare mediante strumenti specifici e la gestione remota del Certificato digitale. Il processo prevede pertanto il rilascio di un Certificato di firma automatica contenente il seguente limite d'uso: *"Il presente certificato è valido solo per firme apposte con procedura automatica"*.
La firma automatica dei documenti viene effettuata dal sistema solo dopo che il Titolare ha attivato il Certificato, senza ulteriori interventi umani a meno che il Titolare stesso non richieda una sospensione temporanea del Certificato o dell'utilizzo dello stesso nella procedura automatica. L'accesso iniziale al sistema avviene tramite un meccanismo di autenticazione prestabilito, richiesto soltanto alla prima sessione, dopodiché i documenti vengono firmati automaticamente

al momento del caricamento, nel rispetto delle autorizzazioni concesse. La firma automatica di cui al presente paragrafo si avvale di un Certificato specifico, destinato unicamente a questa tipologia di utilizzo. Il Titolare è tenuto ad utilizzare Certificati diversi in procedure automatiche diverse, in modo da minimizzare i rischi di sicurezza legati ad un utilizzo improprio. A ciascun Certificato per procedura di firma automatica può essere associata una sola procedura informatica di trasmissione dei documenti.

3.2.2.3 Firma Remota One Shot

Il certificato di firma digitale One Shot (d'ora in avanti, "**OS**" o "**Servizio OS**") è un certificato di firma remota con una validità temporale limitata al tempo necessario per eseguire le firme. Qualora i Certificati OS abbiano una durata di 60 minuti, il periodo di validità è inferiore al tempo massimo per evadere una richiesta di revoca da parte del Richiedente o del Soggetto come specificato nel Manuale di riferimento. Una volta emesso il certificato e utilizzate le chiavi all'interno di una procedura di firma, il certificato emesso dal QTSP scade e le chiavi dovranno necessariamente essere distrutte. Il processo prevede pertanto il rilascio di un Certificato di firma OS contenente il seguente limite d'uso: *"Il presente certificato è utilizzabile esclusivamente nell'ambito della specifica sessione o procedura di firma per cui è stato emesso.*

Il Servizio OS consente al Titolare, previo riconoscimento della sua identità e di una conferma attraverso codice OTP, di autenticarsi e di utilizzare la Firma Remota collegata al Certificato. L'emissione del Certificato da parte di Infocert in favore del Titolare è subordinata all'esito positivo della necessaria procedura di identificazione e riconoscimento di quest'ultimo, nelle modalità rappresentate nel paragrafo 3.1.2. del presente Allegato Tecnico.

Qualora il Cliente abbia acquistato dall'e-commerce di Infocert o da un suo rivenditore un pacchetto di firme One Shot a consumo, le stesse dovranno essere consumate dal Soggetto entro un anno dall'acquisto del pacchetto.

3.2.2.4 Certificati qualificati di sigillo

Infocert, in qualità di Certification Authority, emette certificati qualificati di sigillo elettronico intestati a persone giuridiche, che consentono all'Organizzazione titolare di apporre sigilli elettronici sui documenti informatici, al fine di garantirne l'origine e l'integrità.

I certificati qualificati di sigillo possono essere rilasciati unitamente al servizio remoto di apposizione del sigillo erogato da Infocert. In tale modello, Infocert opera anche in qualità di SSASP e gestisce le chiavi di sigillo all'interno di dispositivi qualificati per la creazione del sigillo. Il sigillo apposto mediante tale servizio è qualificato.

Rientrano in questa categoria il servizio remoto standard di sigillo qualificato e il servizio remoto di sigillo qualificato per l'utilizzo in ambito EPREL. EPREL, European Product Registry for Energy Labelling, è la banca dati dell'Unione Europea relativa ai prodotti soggetti a etichettatura energetica, nella quale sono raccolte le informazioni necessarie a garantire trasparenza e conformità alla normativa europea di settore.

Infocert può inoltre emettere certificati qualificati di sigillo non associati al servizio remoto di apposizione del sigillo. In tali casi, le chiavi sono utilizzate su dispositivi o infrastrutture nella disponibilità del Richiedente o dell'Organizzazione. Qualora il dispositivo utilizzato non sia un dispositivo qualificato per la creazione del sigillo, il sigillo apposto non è qualificato, ma costituisce un sigillo elettronico avanzato basato su certificato qualificato.

Tra i certificati qualificati di sigillo non associati al servizio remoto rientrano anche i certificati con estensione PSD2, destinati a specifici ambiti regolamentati del settore dei servizi di pagamento.

La richiesta di rilascio del certificato qualificato di sigillo deve essere presentata da una persona fisica che agisce in nome e per conto dell'Organizzazione titolare del sigillo. Infocert verifica i poteri

di rappresentanza del richiedente e i dati relativi all'Organizzazione secondo quanto previsto dal paragrafo 3.1.2 del presente Allegato.

3.3 Obblighi e Responsabilità

3.3.1. Obblighi e Responsabilità del Soggetto.

Gli obblighi e le responsabilità del Soggetto, nell'attivazione e nell'utilizzo del Servizio, sono determinati dalla normativa applicabile, dal presente Allegato Tecnico, dalle CGA e dalla Privacy Policy vigenti alla data della Richiesta di Attivazione.

Il Soggetto è responsabile della veridicità e correttezza dei dati forniti nell'ambito del processo di identificazione e della Richiesta di Attivazione. Qualora fornisca informazioni non veritiere o adotti comportamenti idonei a compromettere il corretto processo di identificazione, il Soggetto risponde dei danni eventualmente derivanti a Infocert e/o a terzi, manlevando Infocert da eventuali pretese risarcitorie.

Il Soggetto è tenuto a utilizzare il Certificato e il Servizio esclusivamente per le finalità previste e nel rispetto delle eventuali limitazioni d'uso e/o di valore indicate nel Certificato e nei Manuali Operativi.

Nel caso di certificati su dispositivo fisico, il Soggetto è tenuto a custodire con diligenza il dispositivo e i relativi codici o credenziali di utilizzo, impedendone l'uso da parte di terzi.

Nel caso di servizi remoti, in cui le chiavi sono custodite da Infocert o da infrastrutture da essa gestite, il Soggetto è tenuto a proteggere gli strumenti di autenticazione e attivazione del Servizio, quali credenziali, codici, dispositivi o applicazioni di autenticazione, mantenendoli personali e riservati.

Il Soggetto è responsabile delle operazioni effettuate mediante il proprio Certificato e/o tramite il Servizio, nonché dei documenti sottoscritti, anche quando la procedura informatica o i documenti siano messi a disposizione dal Richiedente o da soggetti terzi.

Il Soggetto è tenuto a verificare il contenuto dei documenti prima della sottoscrizione e ad assicurarsi che gli stessi riflettano la propria volontà.

Il Soggetto deve richiedere tempestivamente la sospensione o la revoca del Certificato o del Servizio nei casi previsti dai Manuali Operativi, ed è responsabile dei danni derivanti da eventuali ritardi nell'attivazione di tali procedure.

Il Soggetto è inoltre tenuto a non utilizzare il Certificato o il Servizio dopo la relativa scadenza, sospensione o revoca.

Il Soggetto è altresì tenuto a comunicare senza indebito ritardo a Infocert qualsiasi sospetto di compromissione uso non autorizzato o perdita delle credenziali o degli strumenti di autenticazione.

3.3.2 Obblighi e Responsabilità del Richiedente

Gli obblighi di cui al presente paragrafo si applicano al Richiedente in relazione al ruolo concretamente svolto nell'ambito del Servizio.

Resta inteso che la Richiesta di Attivazione è sottoscritta dal Soggetto secondo quanto previsto al paragrafo 3.1. Qualora il Richiedente coincida con il Soggetto, si applicano in via principale gli obblighi previsti per il Soggetto al paragrafo 3.3.1, ferma restando l'applicazione dell'Accordo ove il medesimo soggetto coincida anche con il Cliente.

Il Richiedente è soggetto alle CGA, al presente Allegato Tecnico e alla Privacy Policy; qualora coincida con il Cliente, trovano altresì applicazione le disposizioni dell'Accordo.

Il Richiedente è tenuto a fornire a Infocert dati corretti, aggiornati e completi nell'ambito del processo di attivazione del Servizio, nonché, ove applicabile, le informazioni relative all'organizzazione, al ruolo o ai poteri rappresentativi da associare al Certificato.

Qualora il Richiedente agisca in nome e per conto di una persona giuridica, è responsabile della correttezza delle informazioni relative alla stessa e della sussistenza dei poteri necessari per richiedere l'attivazione del Servizio o il rilascio del Certificato riferito alla persona giuridica.

Qualora il Richiedente renda disponibile il Servizio a soggetti ad esso collegati, nell'ambito di rapporti commerciali o di una struttura organizzativa, è responsabile della gestione del Servizio all'interno dei propri processi, applicazioni o infrastrutture, nonché della corretta integrazione e interazione con i sistemi di Infocert.

In tali casi, il Richiedente è responsabile della correttezza e riferibilità dei documenti eventualmente messi a disposizione del Soggetto ai fini dell'utilizzo del Servizio, fermo restando che la manifestazione di volontà e l'utilizzo del Certificato restano in capo al Soggetto.

Qualora il Richiedente gestisca interfacce utente, applicazioni o componenti di front-end attraverso cui il Soggetto accede al Servizio, è tenuto a realizzarle e mantenerle in conformità alle indicazioni fornite da Infocert, garantendo coerenza con la normativa vigente e i requisiti di sicurezza previsti.

Qualora il Richiedente gestisca, anche indirettamente, componenti del processo di autenticazione o di attivazione del Servizio, è tenuto a garantire che tali componenti siano coerenti con le modalità e i livelli di sicurezza previsti per il Servizio.

Il Richiedente, ove renda disponibile il Servizio ai Soggetti, è tenuto ad assicurare che gli stessi possano prendere visione della documentazione contrattuale di Infocert relativa all'attivazione e all'utilizzo del Servizio.

Il Richiedente è tenuto ad adottare adeguate misure tecniche e organizzative per garantire la sicurezza dei sistemi, delle applicazioni e dei processi utilizzati per l'erogazione del Servizio e per l'interazione con i sistemi Infocert.

Il Richiedente è tenuto a non consentire l'utilizzo del Certificato o del Servizio dopo la relativa scadenza, sospensione o revoca e a cooperare con Infocert nei casi in cui sia necessario attivare le relative procedure.

Il Richiedente manleva Infocert da ogni responsabilità derivante da un utilizzo non conforme del Certificato o del Servizio nell'ambito dei propri processi, applicazioni o infrastrutture.

Il Richiedente è altresì responsabile degli eventuali utilizzi fraudolenti o non autorizzati del Certificato o del Servizio da parte di propri dipendenti, collaboratori o utenti autorizzati nell'ambito della propria organizzazione o infrastruttura.

Il Richiedente si impegna a cooperare con Infocert in caso di audit, verifiche o controlli richiesti dall'Autorità competente o derivanti dalla normativa applicabile, fornendo la documentazione e le informazioni ragionevolmente necessarie.

3.3.3 Obblighi e responsabilità di Infocert

Gli obblighi e le responsabilità di Infocert sono esclusivamente quelli previsti dalla normativa

applicabile, dal presente Allegato Tecnico, dalle Condizioni Generali di Attivazione (CGA), dall'Accordo ove applicabile e dai Manuali Operativi di riferimento.
Infocert, in qualità di prestatore di servizi fiduciari qualificati, eroga il Servizio in conformità ai requisiti previsti dal Regolamento eIDAS e dalle norme tecniche applicabili, secondo quanto descritto nei Manuali Operativi.
In particolare, Infocert è tenuta a:

- garantire l'erogazione del Servizio secondo le modalità e i livelli di servizio definiti nei Manuali Operativi;
- assicurare la corretta associazione tra il Soggetto e il Certificato sulla base delle procedure di identificazione adottate;
- gestire il ciclo di vita dei Certificati e, ove applicabile, delle chiavi crittografiche, secondo quanto previsto nei Manuali Operativi;
- conservare, in un apposito archivio digitale non modificabile, i Certificati emessi, le evidenze di identificazione e i log relativi al Servizio, in conformità alla normativa vigente e secondo le modalità previste nei Manuali Operativi.

Resta inteso che Infocert non assume obblighi ulteriori rispetto a quelli sopra indicati.
In particolare, Infocert non presta alcuna garanzia relativamente a:

- il corretto funzionamento e la sicurezza di sistemi, dispositivi hardware o software non forniti direttamente da Infocert, utilizzati dal Soggetto o dal Richiedente per l'accesso o l'utilizzo del Servizio;
- l'utilizzo del Certificato o del Servizio per finalità diverse da quelle previste o in violazione delle eventuali limitazioni d'uso e/o indicate nel Certificato o nei Manuali Operativi;
- il corretto funzionamento delle reti di comunicazione o dei sistemi di trasmissione dati non direttamente gestiti da Infocert;
- la validità, efficacia o rilevanza giuridica di firme, sigilli o processi di autenticazione in ordinamenti diversi da quello Italiano, salvo nei limiti in cui tali effetti siano espressamente riconosciuti e disciplinati dalla normativa europea applicabile;

Infocert non è responsabile del contenuto dei documenti sottoscritti né delle dichiarazioni o manifestazioni di volontà espresse dal Soggetto nell'utilizzo del Servizio.

3.3.4 Ruolo e Organizzazione

Conformemente al Manuale Operativo e alla normativa applicabile, tra cui l'articolo 28, comma 3, del Codice dell'Amministrazione Digitale (CAD) e la determinazione AgID n. 121/2019 e successive modifiche, il Soggetto o il Richiedente, ove previsto, possono richiedere l'inserimento nel Certificato di informazioni relative al ruolo del Soggetto.
Tali informazioni possono includere, a titolo esemplificativo:

- titoli e/o abilitazioni professionali;
- poteri di rappresentanza di persone fisiche o giuridiche;
- appartenenza a organizzazioni o enti;
- esercizio di funzioni pubbliche.

L'inserimento di tali informazioni avviene secondo le modalità previste nei Manuali Operativi ed è subordinato al consenso del Terzo Interessato, ove richiesto.

Il Terzo Interessato è il soggetto responsabile delle informazioni relative al ruolo o all'organizzazione indicate nel Certificato; esso può coincidere con il Richiedente, ma non necessariamente. Il Terzo Interessato è responsabile della correttezza e dell'aggiornamento di tali informazioni e può richiedere, nei casi previsti, la modifica, sospensione o revoca del Certificato.
Qualora il Certificato riporti l'appartenenza del Soggetto a un'organizzazione, è responsabilità del Terzo Interessato comunicare tempestivamente a Infocert eventuali variazioni relative a tale appartenenza.
Le richieste di certificati che includono riferimenti a organizzazioni sono accettate esclusivamente se relative a soggetti giuridici con forma identificabile e verificabile. Le informazioni relative all'organizzazione (quali denominazione o identificativi) sono inserite nel Certificato solo a seguito di autorizzazione espressa dell'organizzazione stessa, secondo quanto previsto nel Manuale Operativo pertinente.

4. SLA e KPI

In termini di erogazione, i valori di disponibilità mensile dei servizi sono rappresentati dettagliatamente nel Manuale Operativo pertinente.