**ALLEGATO TECNICO**

**Certificati qualificati e di autenticazione e servizi di firma qualificata.**

# Sommario



***

# 1. RIFERIMENTI ESTERNI

| Documentazione | Link di dettaglio |
|---|---|
| **CP e CPS (Manuale Operativo) per emissione certificati qualificati** | https://pki.infocert.it/pdf/ICERT_INDI_MO.pdf |
| **CP e CPS (Manuale operativo) per emissione certificati di Autenticazione** | https://pki.infocert.it/pdf/ICERT_INDI_MOCA.pdf |
| **per certificati di autenticazione CNS** | Ente Certificatore InfoCert Certificati di Autenticazione per la Carta Nazionale dei Servizi Certificate Policy |
| **PDS (PKI Disclosure Statement) per i certificati qualificati** | https://pki.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

InfoCert opera in qualità di prestatore di servizi fiduciari qualificati (d'ora in avanti, "**QTSP**" *Qualified Trust Service Provider*) per il servizio di emissione di Certificati Qualificati su dispositivo fisico o remoto, nel rispetto del proprio Manuale Operativo (d'ora in avanti anche "**CPS**" *Certificate Practice Statement)* e del proprio *PKI Disclosure Statement* (d'ora in avanti, "**PDS**").

Per tale servizio InfoCert ha ottenuto una valutazione di conformità effettuata dal *Conformity Assesment Body* CSQA Certificazioni S.r.l., ai sensi del Regolamento (UE) n. 910/2014 così come modificato dal Reg. (UE) 2024/1183 of the European Parliament and of the Council of April 2024.(d'ora in avanti, "**Regolamento eIDAS**") e delle norme ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319 403

e UNI CEIISO/IEC 17065:2012, nonché dal D.P.C.M. 22.02.2013, e dal Decreto Legislativo 7 marzo 2005, n. 82 (CAD) e successive modifiche (collettivamente, d'ora in avanti, la "**Normativa Applicabile**").
Per tale servizio InfoCert ha ottenuto accreditamento presso AgID ed è presente, come previsto dal regolamento eIDAS nella *Trusted Service List* Europea (https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls).
La firma elettronica qualificata o digitale o di sottoscrizione (d'ora in avanti, "**FD**" o "**Servizio FD**") consente di firmare i documenti direttamente da PC o smartphone mantenendo lo stesso valore legale della tradizionale firma autografa.
È il risultato di una trasformazione crittografica dei dati che garantisce l'autenticazione dell'origine, l'integrità e il non ripudio degli stessi da parte firmatario. Le chiavi crittografiche utilizzate per questa operazione sono conservate su un dispositivo fisico o remoto. Le chiavi sono associate ad un soggetto attraverso un Certificato digitale (d'ora in avanti, "**Certificato**"), che contiene i suoi dati identificativi.
Le chiavi di crittografia sono generate, conservate e utilizzate attraverso un dispositivo *sicuro Qualified Signature Creation Device* (d'ora in avanti anche "**QSCD**"), che può essere un dispositivo fisico consegnato al Soggetto oppure un dispositivo situato in un'area del data center ad alta sicurezza o HSTZ (*High Security Trusted Zone*).
Il tipo di Certificato è contraddistinto da un numero chiamato O.I.D. (*Object Identifier*), ossia un codice che identifica il Certificatore (InfoCert), l'uso del Certificato e la "*policy e procedure"* a cui esso è conforme. La definizione e descrizione completa degli O.I.D. si trova nel CPS.
I Certificati dettagliati nel presente allegato tecnico sono di due tipologie:
a) Certificati qualificati di sottoscrizione su dispositivo fisico o remoto;
b) Certificati di Autenticazione: fungono da strumento digitale per l'autenticazione del Titolare per l'accesso ai servizi online dedicati.

## 2.1 Definizione Delle Parti

**Soggetto/Titolare**: Il Soggetto, definito anche **Titolare**, si riferisce alla persona fisica titolare del Certificato Qualificato. Tale Soggetto è l'utilizzatore dei servizi offerti e ha i suoi dati identificativi fondamentali inseriti nel Certificato.

**Richiedente**: Il Richiedente è la persona fisica o giuridica che richiede il rilascio di Certificati digitali al QTSP per un Soggetto. **Il Richiedente può coincidere con il Soggetto/Titolare**, quando una persona fisica richiede un Certificato per sé stessa. In altre situazioni, il Richiedente può essere un ente o un'organizzazione, che agisce per conto di persone fisiche collegate da rapporti commerciali o nel quadro di una struttura organizzativa.

**Ente Emettitore**: Ente responsabile del rilascio di un dispositivo fisico (SmartCard o Token) opportunamente predisposto per ospitare un certificato di autenticazione CNS (Carta Nazionale Dei Servizi) come descritto nel paragrafo 3.2.1.3 del presente documento. È la Pubblica Amministrazione che emette la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della stessa.

**Terzo interessato**: persona fisica o giuridica interessata e/o responsabile dell'informazione inclusa nel Certificato relativa al Ruolo e/o all'Organizzazione.

# 3. SPECIFICHE TECNICO-NORMATIVE

## 3.1.1 Rilascio e Utilizzo del Servizio FD

Il Servizio FD è erogato da InfoCert in favore del Soggetto, in forza del presente Allegato Tecnico e delle Condizioni Generali di Contratto (d'ora in avanti, "**CGC**") stipulate con lo stesso.
Il Richiedente deve richiedere al QTSP la registrazione e l'emissione del Certificato seguendo le modalità stabilite nel Manuale Operativo pertinente, utilizzando l'apposita Richiesta di Attivazione fornita da InfoCert (d'ora in avanti "**Richiesta di Attivazione**").
Il rilascio del Certificato da parte di InfoCert in favore del Soggetto è subordinato all'esito positivo della preventiva e necessaria procedura di identificazione di quest'ultimo, come rappresentato nel par. 3.2.3 del CPS (*Certification Practice Statement*) e nel par. 3.1.3 del presente documento.
Pertanto, in caso di esito negativo dell'identificazione, il Certificato non sarà rilasciato dal QTSP; mentre in caso di esito positivo dell'identificazione, il Certificato verrà rilasciato al Soggetto ai sensi del CPS.
Il Certificato rilasciato può essere utilizzato per firmare documenti utilizzando strumenti messi a disposizione dal QTSP o dal Richiedente non Titolare, per sbloccare le chiavi di firma, e dopo aver svolto un processo di autenticazione tramite strumenti dedicati, il QTSP conserverà le informazioni relative alla reale identità della persona per almeno venti (20) anni dalla scadenza del Certificato stesso, fino a un massimo di 23 (ventitre) anni dalla data di emissione.
Nel caso in cui il QTSP termini la propria attività, provvederà al trasferimento di tali informazioni a terze parti, alle medesime condizioni ivi esposte, così come indicato nel Manuale Operativo pertinente.

## 3.1.2 Certificato Digitale

Un Certificato digitale è un documento elettronico, firmato da InfoCert, che certifica l'associazione tra il Soggetto e la sua coppia di chiavi crittografiche (pubblica e privata), utilizzate per la firma digitale o per l'autenticazione. Le chiavi vengono generate e gestite in un dispositivo crittografico sicuro sotto il controllo di InfoCert o del Soggetto stesso.
Il QTSP garantisce la corretta associazione delle chiavi con il Soggetto, emettendo il Certificato conformemente alla normativa applicabile e al Manuale Operativo pertinente.
I Certificati possono contenere delle limitazioni d'uso così come previste nel Manuale Operativo pertinente.

## 3.1.3 Processo di verifica di identità

Prima di procedere con il riconoscimento, il Titolare deve assicurarsi di essere in possesso dei documenti di identità in formato originale e di un codice fiscale.
Questi devono essere in originale, in buono stato e in corso di validità.
Sono accettabili esclusivamente i documenti elencati nel documento "CPS Addendum – Documenti di identità accettabili" presente sul sito InfoCert al seguente link: CPS_doc_identita.pdf.
Le modalità di identificazione di seguito elencate sono descritte nel dettaglio nel paragrafo 3.2.3 del CPS.

| Modalità di identificazione | Richiedenti che acquistano il servizio per se stessi | Richiedenti che acquistano per conto di altri Soggetti |
|---|---|---|

| | | |
|---|---|---|
| 1. LiveID | ☒ | ☒ |
| 2. AMLID | ☐ | ☒ |
| 3. SignID | ☒ | ☒ |
| 4. AutID | ☒ | ☒ |
| 5. VideoID | ☒ | ☒ |
| 6. eDocID | ☐ | ☒ |

### 3.1.4 Rinnovo del Certificato

Il Soggetto può rinnovare il Certificato, prima della sua scadenza, utilizzando gli strumenti messi a disposizione da InfoCert. La richiesta di rinnovo viene sottoscritta con la chiave privata, corrispondente alla chiave pubblica contenuta nel Certificato da rinnovare. L'esito del rinnovo è di fatto l'emissione di un nuovo Certificato.
Il rinnovo non è possibile se gli attributi indicati nel Certificato non sono più validi. Dopo la revoca o la scadenza del Certificato non è possibile eseguire il rinnovo del Certificato, diventando quindi necessaria una nuova identificazione.
In merito alla disposizione di cui al punto 7.2 delle CGC, nel caso in cui il Titolare dia la disdetta anticipata rispetto al rinnovo automatico annuale delle suddette Condizioni, la possibilità di utilizzare il Certificato verrà bloccata, e su richiesta del Titolare, lo stesso verrà revocato.

### 3.1.5 Sospensione o Revoca del Certificato

La revoca o sospensione del Certificato può avvenire su richiesta autenticata del Soggetto o del Richiedente non Titolare (Terzo Interessato nel caso in cui quest'ultimo abbia espresso il suo consenso per l'inserimento del Ruolo e/o il campo Organizzazione) ovvero su iniziativa del QTSP. Gli ulteriori dettagli in materia sono regolati nel Manuale Operativo pertinente.

## 3.2 SERVIZI

### 3.2.1 Certificati 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 dai seguenti Object Identifiers (OID), ossia un codice che identifica il QTSP, l'uso del Certificato e la policy a cui esso è conforme:

| Servizio | OID |
|---|---|
| Firma su Dispositivo | 1.3.76.36.1.1.1 e 1.3.76.36.1.1.61 |
| Autenticazione | 1.3.76.36.1.1.3 |
| Autenticazione CNS | 1.3.76.36.1.1.4 |

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.

3.2.1.1 Certificato 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 data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data.

3.2.1.2 Certificato di Autenticazione su dispositivo
Il Certificato di Autenticazione rilasciato da InfoCert funge da strumento digitale per l'autenticazione del Titolare. 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. È utilizzabile per una varietà di servizi digitali che richiedono sicurezza elevata, come firme elettroniche, transazioni crittografate e autenticazione sicura nei sistemi informatici. 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 data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data.

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 ad InfoCert mandato non esclusivo a espletare la funzione di Certification Authority (CA) per il rilascio di CNS. L'Ente Emettitore autorizza 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 Remota

I Certificati di firma remota di cui ai paragrafi successivi sono identificati dai seguenti Object Identifiers (OID):

| Servizio | OID |
|---|---|
| Emissione di certificati qualificati per Firma Remota | 1.3.76.36.1.1.22 e 1.3.76.36.1.1.63 |
| Emissione certificato qualificato per firma remota utilizzabile esclusivamente nel/i dominio/i definiti dal Richiedente | 1.3.76.36.1.1.35 e 1.3.76.36.1.1.65 |
| Emissione certificato qualificato per firma remota automatica | 1.3.76.36.1.1.2 e 1.3.76.36.1.1.62 |
| Emissione certificato qualificato per firma remota - Firma remota One Shot (OS) | 1.3.76.36.1.1.34 e 1.3.76.36.1.1.64 |

#### 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 InfoCert sono utilizzati mediante apposite procedure informatiche che si collegano in maniera sicura al servizio di Firma Remota erogato da InfoCert. Tale servizio garantisce il rispetto del Regolamento e di quanto previsto al dall'art. 35 del CAD, Codice dell'Amministrazione Digitale, tramite l'utilizzo di un dispositivo crittografico sicuro (**QSCD**).
Il Servizio prevede che al Titolare sia messa a disposizione, una procedura informatica, implementata sui sistemi di InfoCert o del Richiedente non Titolare, quando presente, mediante la quale il medesimo Titolare può gestire il proprio Certificato di sottoscrizione.
I Certificati di Firma Remota possono essere rilasciati nel dominio messo a disposizione dal Richiedente non 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 e nei rapporti tra Titolare e Richiedente.
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 di "livello elevato", che prevede 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.
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 non Titolare.
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 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 ottenimento codici OTP, oppure dalle modalità previste dall'applicazione del Richiedente.

3.2.2.2 Firma remota automatica
La Firma automatica è un tipo di firma remota che rispetta l'adempimento dei requisiti previsti dell'art. 35, comma 3 del Codice, il Titolare deve utilizzare una coppia di chiavi destinata a tale scopo, diversa da tutte le altre in suo possesso.
Il Servizio, in aggiunta a quanto previsto dal paragrafo 3.2.1 del presente Allegato Tecnico, consente la generazione automatica delle firme su documenti inviati attraverso procedure informatiche automatizzate. In tal caso non è necessario per il Titolare confermare la volontà di firmare perché è a conoscenza dei documenti che vengono generati dalla procedura informatica di cui sopra.
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 PIN e OTP, che sono richiesti 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 digitale per procedura di firma automatica può essere associata una sola procedura informatica di trasmissione dei documenti.

3.2.2.3 Firma Remota One Shot
La firma digitale One Shot (d'ora in avanti, "**OS**" o "**Servizio OS**") è una firma remota le cui chiavi, una volta generate, sono disponibili solo ed esclusivamente per la transazione di firma per la quale sono state generate. Immediatamente dopo il loro utilizzo la chiave privata viene distrutta.
I certificati afferenti a questa firma hanno una validità ridotta al tempo necessario per eseguire le firme. In questa categoria sono compresi anche certificati denominati "short-term" per i quali il periodo di validità è inferiore al tempo massimo per evadere una richiesta di revoca come specificato nel Manuale di riferimento.
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 3.1.3. del presente Allegato Tecnico.
In deroga a quanto stabilito all'articolo 10.4 delle CGC, poiché il Servizio OS, per sua natura, richiede l'esecuzione immediata, il Titolare accetta espressamente la perdita del diritto di recesso ai sensi dell'art. 59, lett. a), del Codice del Consumo.
Qualora il Certificato abbia la durata di 60 minuti, e in deroga a quanto previsto dal paragrafo 3.1.5 del presente documento, essendo la durata del certificato minore o uguale del tempo minimo (60 minuti) previsto per rendere pubblica l'informazione sulla subentrata invalidità dello stesso, per tali Certificati non è prevista la possibilità di revoca e sospensione.
Qualora il Certificato abbia la durata di 30/45/60 giorni, il contratto relativo al Servizio FD è sospensivamente condizionato al buon esito dell'identificazione che deve avvenire entro e non oltre i 30/45/60 giorni.

## 3.3 Obblighi e Responsabilità

### 3.3.1. Obblighi e Responsabilità di Soggetto e Richiedente non Titolare

Gli obblighi e le responsabilità del Soggetto e, quando applicabile, del Richiedente non Titolare sono determinati dalla normativa applicabile, dal presente Allegato Tecnico, dal Manuale Operativo pertinente e dalle CGC nella versione in vigore alla data della Richiesta di Attivazione. Se, al momento dell'identificazione, il Soggetto cela la sua reale identità o il Richiedente non Titolare o il Titolare stesso agiscono in modo da compromettere l'identificazione e le relative risultanze indicate nel Certificato, saranno considerati responsabili per tutti i danni derivanti al QTSP e/o a terzi dall'inesattezza delle informazioni contenute nel Certificato. Il Richiedente e/o Soggetto sono tenuti a garantire e manlevare il QTSP da eventuali richieste di risarcimento danni.
Sono anche responsabili per i danni derivanti al QTSP e/o a terzi in caso di ritardo nell'attivazione delle procedure di revoca o sospensione del Certificato, come previsto dal Manuale Operativo pertinente. Devono assicurarsi di rispettare i requisiti hardware e software necessari per il corretto utilizzo dei Certificati.
Il Soggetto e il Richiedente non Titolare sono gli unici responsabili dei documenti che attraverso le applicazioni InfoCert o del Richiedente stesso saranno trasmesse ai fini della firma, assumendo, pertanto, ogni e più ampia responsabilità in merito al funzionamento della stessa procedura informatica e al contenuto, validità e titolarità di detti documenti, sollevando il Certificatore da ogni e qualsiasi responsabilità in merito.

### 3.3.2. Obblighi Specifici del Soggetto

Gli strumenti di autenticazione (a titolo esemplificativo, il PIN, l'OTP o lo strumento che lo genera) per la procedura di attivazione del Certificato sono strettamente personali. Pertanto, il Titolare è tenuto a proteggere la segretezza di detti strumenti, omettendo di comunicarli o divulgarli a terzi, anche solo in parte, conservandoli in un luogo sicuro.
Il Soggetto, consapevole che l'utilizzo di un Certificato di firma comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona, è obbligato ad osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione messi a disposizione dal QTSP o dal Richiedente non Titolare.
Deve esercitare la massima diligenza nell'uso del Certificato di firma, verificando il contenuto dei documenti da firmare e assicurandosi che riflettano la sua volontà.
È inoltre tenuto a non utilizzare il Certificato dopo la sua scadenza, revoca o sospensione.

È responsabile per la veridicità dei dati comunicati durante l'identificazione e nella Richiesta di Attivazione.

### 3.3.3 Obblighi del Richiedente non Titolare

Il Richiedente non Titolare è responsabile della richiesta del Certificato al Certificatore ed è responsabile della sua gestione, conformemente al PDS e al Manuale Operativo. Deve adottare misure adeguate a prevenire danni derivanti dall'uso del sistema di chiavi asimmetriche o del Certificato. Se gestisce il processo di autenticazione, deve garantire una autenticazione con un livello elevato di sicurezza come previsto da Regolamento di Esecuzione (UE) 2015/1502 e secondo le modalità concordate con InfoCert. È inoltre tenuto a ricordare che l'uso del Certificato, dopo la sua scadenza, revoca o sospensione, determina l'apposizione di una firma non valida e, pertanto, è obbligato a manlevare InfoCert da qualsivoglia responsabilità per uso improprio del Certificato medesimo.

### 3.3.4 Obblighi del QTSP

Gli obblighi del QTSP sono esclusivamente quelli indicati dalla normativa applicabile, dal presente Allegato Tecnico, dei Manuali Operativi e dall'Accordo.
In particolare, il QTSP si obbliga a conservare in un apposito archivio digitale non modificabile per almeno venti (20) anni dalla scadenza del certificato, fino a un massimo di 23 (ventitré) anni dalla data di emissione, tutti i certificati emessi, i *log* di attivazione degli stessi e le evidenze di riconoscimento, nelle modalità previste dal Manuale Operativo.
In particolare, il QTSP non presta alcuna garanzia relativamente a:

- il corretto funzionamento e la sicurezza dei macchinari *hardware* e dei *software* utilizzati dal Titolare;
- usi diversi della chiave privata, del dispositivo sicuro di firma e/o di autenticazione e del Certificato rispetto a quelli previsti dalle norme italiane vigenti e dal Manuale Operativo pertinente;
- il regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali;
- la validità e rilevanza, anche probatoria, – della firma nei confronti di soggetti e per atti e documenti sottoposti a legislazioni differenti da quella italiana;
- la segretezza di qualsiasi messaggio, atto o documento firmato (quindi, eventuali violazioni di quest'ultima sono, di norma, rilevabili dal Titolare o dal destinatario attraverso l'apposita procedura di verifica).

Il QTSP garantisce unicamente il funzionamento del Prodotto, secondo i livelli di servizio indicati al Titolare nel Manuale Operativo pertinente.

### 3.3.5 Ruolo e Organizzazione

Conformemente al Manuale Operativo e alle normative vigenti delineate nell'articolo 28, comma 3, del Codice dell'Amministrazione Digitale (CAD) e nella determinazione dell'Agenzia per l'Italia Digitale (AgID) n. 121/2019 e successivi emendamenti, il Richiedente non Titolare o il Titolare stesso possono richiedere l'inserimento nel Certificato di specifiche informazioni relative al Ruolo del Titolare. Queste informazioni possono includere:

- titoli e/o abilitazioni professionali;
- poteri di rappresentanza di persone fisiche o di enti di diritto privato o pubblico;
- appartenenza a tali enti;

- esercizio di funzioni pubbliche.

Questo inserimento deve avvenire secondo le modalità delineate nel Manuale Operativo di riferimento. Per richiedere l'inserimento del Ruolo, è necessario il consenso del **Terzo Interessato**, che può coincidere con il Richiedente, e che può altresì richiedere la revoca o la sospensione del Certificato in qualunque momento. Se il Richiedente non Titolare vuole che il Certificato rifletta l'appartenenza del Soggetto stesso alla propria organizzazione, è responsabilità del Richiedente non Titolare, in qualità di Terzo Interessato, comunicare ad InfoCert eventuali cambiamenti relativi alla appartenenza del soggetto all'organizzazione.
Le richieste di certificati che indicano l'appartenenza all'organizzazione, sono accettate solo se provenienti da entità con una forma giuridica definita e verificabile presso il Registro delle Imprese. La ragione sociale, la denominazione e il codice identificativo dell'Organizzazione saranno inclusi nel Certificato solo se l'organizzazione ha espressamente autorizzato il rilascio del Certificato, anche senza una specifica indicazione di Ruolo, come da Manuale Operativo.

# 4. SLA

## 4.1 SLA di servizio

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