

**ALLEGATO B – TECNICO**  
**Certificato di Firma Digitale One-Shot - PMI**

**Indice:**

1. **Riferimenti Esterni**
2. **Descrizione del servizio**
3. **Specifiche tecnico-normative**
4. **Specifiche tecniche d'uso**
5. **SLA e KPI**

\*\*\*

**1. RIFERIMENTI ESTERNI:**

Documentazione	Link di dettaglio
Manuale Operativo	<a href="https://pki.infocert.it/pdf/ICERT_INDI_MO.pdf">https://pki.infocert.it/pdf/ICERT_INDI_MO.pdf</a>
Manuale Utente	N.D.
Documentazione API	<a href="https://developers.infocert.digital/e-signature-and-e-sealing/">https://developers.infocert.digital/e-signature-and-e-sealing/</a>
Link di supporto (FAQ, Video, Guide)	<a href="https://help.infocert.it/cerca?searchText=Firma%20Digitale&amp;idProdotto=33">https://help.infocert.it/cerca?searchText=Firma%20Digitale&amp;idProdotto=33</a>

**2. DESCRIZIONE DEL SERVIZIO**

InfoCert opera in qualità di prestatore di servizi fiduciari qualificati (d’ora in avanti, “**TSP**”), nel rispetto del proprio Manuale Operativo ICERT-INDI-MO (d’ora in avanti, “**CPS**”) e sulla base di una valutazione di conformità effettuata dal Conformity Assesment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento (UE) 910/2014 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. La firma digitale One Shot (d’ora in avanti, “**OS**” o “**Servizio OS**”) è una firma elettronica qualificata rilasciata mediante l’emissione di un certificato qualificato (d’ora in avanti, “**Certificato**”) da associare alla firma digitale del soggetto a cui è rilasciato il certificato digitale e i cui dati sono valorizzati all’interno dello stesso (d’ora in avanti, il “**Titolare**”), creata tramite un dispositivo sicuro, in conformità a quanto previsto nel C.A.D., nelle regole tecniche ivi richiamate (e successive modifiche ed integrazioni), nel PKI Disclosure Statement (d’ora in avanti, “**PDS**”) e nel CPS.

Il Servizio OS consente al Titolare, previo riconoscimento della sua identità e autenticazione dello stesso a mezzo di appositi strumenti, l’utilizzo in forma remota del Certificato, nel termine di durata di validità dello stesso, pari a 60 minuti oppure 30 giorni, ai fini della sottoscrizione dei documenti informatici.

**3. SPECIFICHE TECNICO-NORMATIVE**

**3.1 Utilizzo del Servizio OS**

Il Servizio OS è erogato da InfoCert in favore del Titolare, in forza delle CGC stipulate con lo stesso, oppure tra InfoCert ed il Cliente, affinché gli Utenti di quest’ultimo possano sottoscrivere documenti elettronici. Pertanto, attraverso l’utilizzo del Servizio OS, il Titolare può concludere contratti e, più in generale, assumere impegni e rilasciare dichiarazioni ad ogni effetto poiché la firma digitale apposta sui documenti informatici per legge è equiparata alla firma autografa.

Il Titolare deve richiedere al TSP la registrazione e l’emissione del Certificato nelle modalità stabilite nel PDS e dettagliate nel Manuale Operativo, utilizzando l’apposito modulo di adesione messo a sua disposizione in modalità telematica (d’ora in avanti “**Modulo di Adesione**”).

L’emissione del Certificato da parte di InfoCert in favore del Titolare è subordinata all’esito positivo della preventiva e necessaria procedura di identificazione e riconoscimento di quest’ultimo (d’ora in avanti,

l'”Identificazione”), nelle modalità di seguito rappresentate.

Le modalità di Identificazione al fine del rilascio del Certificato per il Servizio OS sono descritte nel CPS e potranno rispettare una delle due sequenze temporali sotto riportate:

- **Ex Ante:** l'Identificazione del Titolare viene effettuata prima del rilascio del Certificato e questo ha validità di 60 minuti. La procedura di rilascio e sottoscrizione deve concludersi positivamente entro 60 minuti dall'invio della richiesta. Diversamente, il Titolare deve procedere con una nuova richiesta.
- **Ex Post:** l'Identificazione del Titolare viene effettuata entro un termine non superiore a 30 (trenta) giorni dal rilascio del Certificato. I documenti informatici sottoscritti con tale Certificato sono sospensivamente condizionati all'esito positivo del riconoscimento del Titolare e, fino a tale momento, sono, pertanto, privi di efficacia giuridica.

Le chiavi di firma, una volta generate, sono disponibili solo ed esclusivamente per la transazione di firma per la quale sono state emesse. Immediatamente dopo l'utilizzo del Certificato, la chiave privata viene distrutta e il Certificato stesso non potrà più essere utilizzato.

In caso di esito positivo dell'Identificazione, il Certificato è emesso dal TSP, pubblicato nell'apposito registro e rilasciato al Titolare ai sensi del CPS.

In caso di esito negativo dell'Identificazione, il Certificato non sarà emesso dal TSP o, se emesso, si considererà privo di efficacia sin dal momento della sua emissione e l'Accordo si intenderà risolto di diritto. Il Titolare prende atto del fatto che il TSP registri e mantenga per 20 (venti) anni le informazioni raccolte con la registrazione, quelle concernenti gli strumenti forniti, la revoca, l'identità e gli attributi inseriti nel Certificato e altresì acconsente al trasferimento di tali informazioni a terze parti, alle medesime condizioni, nel caso in cui il TSP termini la propria attività, così come indicato nel Manuale Operativo.

Il Titolare, per l'erogazione di tale Servizio, non sosterrà alcun onere economico, il quale rimarrà in capo al Cliente.

### **3.2 Modalità di rilascio del Certificato:**

Il Certificato relativo al Servizio OS potrà essere rilasciato esclusivamente in modalità remota.

### **3.3 Responsabilità e Obblighi del Titolare:**

Il Titolare è responsabile della veridicità dei dati comunicati in fase di Identificazione e nel Modulo di Adesione sottoscritto dal Titolare stesso.

Qualora il Titolare abbia, in fase di Identificazione, celato ad InfoCert la propria reale identità o dichiarato falsamente di essere altro soggetto, anche attraverso l'utilizzo di documenti personali non veri, o abbia agito in modo tale da compromettere l'Identificazione e le relative risultanze, sarà considerato responsabile di tutti i danni causati al TSP e/o a terzi in forza delle errate informazioni rappresentate, oltre all'obbligo di e manlevare il TSP per eventuali richieste di risarcimento dei danni.

Il Titolare deve indicare, assumendo ogni responsabilità in merito, la tipologia di sistema OTP (One Time Password) prescelta al fine di attivare la procedura di firma One Shot.

Gli obblighi del Titolare sono quelli indicati dalla normativa vigente, dal PDS e dal CPS. Ai sensi dell'art. 32 del C.A.D., il Titolare è obbligato ad adottare tutte le misure idonee ad evitare che dall'utilizzo della firma digitale derivi danno ad altri.

In considerazione della circostanza che l'utilizzo di una firma digitale comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona, il Titolare è obbligato ad osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione messi a disposizione dal TSP, tra cui i codici OTP ricevuti sul numero di cellulare indicato.

Gli strumenti di autenticazione per l'attivazione della procedura di firma remota sono strettamente personali. Pertanto, il Titolare è tenuto a proteggere la segretezza di detti strumenti non comunicandoli o divulgandoli a terzi, neanche in parte, e conservandoli in un luogo sicuro. Il Titolare è, inoltre, tenuto a provvedere

all'adeguamento dei suoi sistemi hardware e software alle misure di sicurezza previste dalla legislazione vigente.

È responsabilità del Titolare verificare attentamente il contenuto dei documenti che il medesimo intende sottoscrivere con il Certificato.

#### **4. SPECIFICHE TECNICHE D'USO**

Il Servizio OS viene emesso in conformità a quanto previsto nel Codice dell'Amministrazione Digitale (d'ora in avanti, "C.A.D."), nelle regole tecniche ivi richiamate (e successive modifiche ed integrazioni) e nel CPS.

Il Certificato emesso da InfoCert, ai sensi della normativa applicabile, è contraddistinto da un O.I.D. (Object Identifier), ossia un codice che identifica il TSP, l'uso del Certificato e la policy a cui esso è conforme. L'O.I.D. del Servizio in oggetto è 1.3.76.36.1.1.34 e 1.3.76.36.1.1.64 e riporta i limiti d'uso e gli O.I.D. previsti dalle singole modalità di identificazione e indicati nel CPS.

L'attività di certificazione propedeutica al rilascio del Certificato consiste nella procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale InfoCert garantisce la corrispondenza biunivoca tra la chiave pubblica e il Titolare cui essa appartiene, identifica quest'ultimo e attesta il periodo di validità della già menzionata chiave ed il termine di scadenza del relativo Certificato, secondo le modalità indicate nel Manuale Operativo.

Le chiavi di firma, una volta generate, sono disponibili solo ed esclusivamente per la transazione di firma per la quale sono state emesse.

Immediatamente dopo l'utilizzo del Certificato, la chiave privata viene distrutta e il certificato stesso non potrà più essere utilizzato.

Il Certificato relativo al Servizio OS rilasciato dal TSP può essere utilizzato mediante apposite procedure informatiche tali da garantire il rispetto di quanto previsto dall'art. 35, c. 3, del C.A.D.

#### **5. SLA e KPI**

##### ***SLA di Assistenza***

Il supporto erogato da InfoCert è finalizzato a garantire continuità nella fruizione del servizio per le componenti fornite da InfoCert.

Il supporto, così inteso, è erogato dal Customer Care InfoCert attraverso l'utilizzo di uno o più sistemi di ticketing web.

Il servizio di assistenza, per i prodotti/servizi erogati in **SaaS**, si sviluppa come segue:

##### **Canale MASS**

Secondo le indicazioni pubblicate su <https://help.infocert.it/contatti>

Nelle modalità:

- Ticket: servizio disponibile h24 7x7 (presidio operatore lunedì – venerdì dalle 8.30 alle 18.30 - festivi esclusi)
- Chat: lunedì – venerdì dalle 8.30 alle 18.30 (escluso festivi)
- Telefono: lunedì – venerdì dalle 8.30 alle 18.30 (escluso festivi)

È disponibile inoltre, a pagamento, un'Assistenza Telefonica Specialistica che prevede il supporto tecnico da parte di personale qualificato, nella soluzione di situazioni particolari. Il servizio è erogato su prenotazione.

##### ***SLA di servizio***

##### **Disponibilità**

Misura la disponibilità dei servizi informatici erogati da InfoCert nel proprio perimetro di competenza, viene misurata su base mensile.

La figura sottostante offre uno schema esemplificativo del dialogo tra il Cliente ed il servizio / prodotto InfoCert utilizzato, allo scopo di distinguere gli ambiti di competenza.

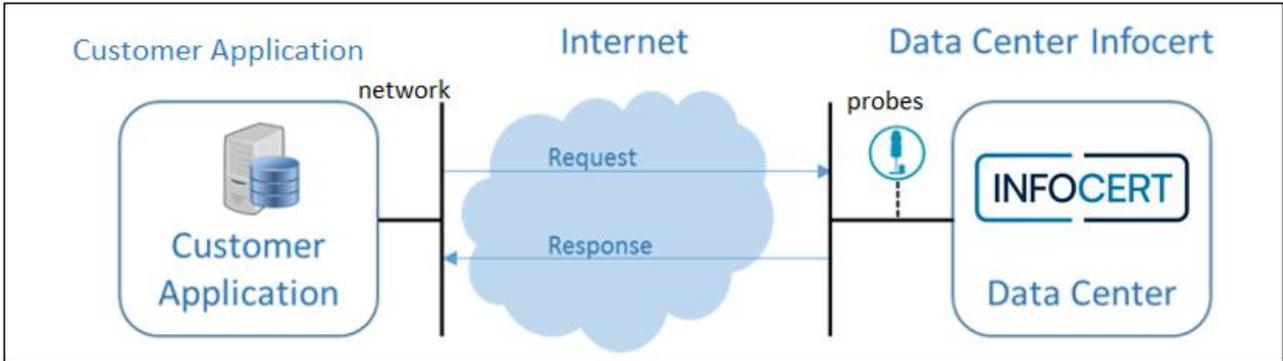


FIGURA 1- SCHEMA ESEMPLIFICATIVO DEL DIALOGO FRA LE APPLICAZIONI DEL CLIENTE ED IL DATA CENTER INFOCERT

Lo strumento utilizzato da InfoCert per misurare la disponibilità dei servizi è composto da sonde applicative (nella fig. sonde) che simulano in automatico l'attività del Cliente e consentono di rilevare e tracciare eventuali periodi di indisponibilità.

In termini di erogazione, si prevedono i seguenti valori di disponibilità del servizio:

KPI Disponibilità	Servizio	Orario	Disponibilità
D..	LegalCert	24x7	99,00%

TABELLA 1 | DISPONIBILITÀ SERVIZI

Di seguito sono descritte le modalità di calcolo dei KPI di disponibilità:

KPI	Ambito	Descrizione
D01, D02, ...	Disponibilità dei Servizi	<p>Il metodo di calcolo per gli indicatori di disponibilità si basa sui seguenti valori:</p> <p><b>periodo osservato</b> = durata in secondi del periodo di osservazione, al netto delle manutenzioni programmate</p> <p><b>tempo indisponibilità</b> = somma delle durate in secondi dei tempi di indisponibilità del servizio, nel periodo di osservazione</p> <p>Il valore di disponibilità è calcolato, per ogni servizio, tramite la seguente formula:</p> $D = \frac{\text{Periodo osservato} - \text{Tempo indisponibilità}}{\text{Periodo osservato}} * 100$

Il periodo di osservazione è mensile.

La violazione si individua quando **D < disponibilità concordata**

#### TABELLA 2 | CALCOLO KPI DISPONIBILITÀ

InfoCert limita la propria responsabilità all'erogazione dei propri servizi, non è quindi responsabile per eventuali anomalie di performance dovuti a indisponibilità o lentezza nella rete che connette il Cliente all'IDC.

InfoCert non è inoltre responsabile di anomalie derivanti da:

- incorretta configurazione o dimensionamento dell'infrastruttura del Cliente;
- incorretta installazione o configurazione di software che utilizzano servizi InfoCert sull'infrastruttura del Cliente.

#### ***KPI di Performance***

Per il Servizio OS sono stati identificati e misurati i seguenti indicatori di performance calcolato in millesimi di secondo:

- Tempo di apposizione firma: il 90% delle richieste viene evaso in 0.324s con un tempo medio di 0.285s;
- Tempo di emissione certificato: il 90% delle richieste viene evaso in 2.491s, con un tempo medio di 1.66s.