

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

**GARA A PROCEDURA APERTA AI SENSI DEL D.LGS. 36/2023 PER L'ACQUISIZIONE DI CERTIFICATI
DIGITALI PER INAIL – EDIZIONE 2**

**ID 2816
CAPITOLATO TECNICO**



INDICE

1.	PREMESSA	3
1.1	Prescrizioni in materia di sicurezza	4
1.2	Requisiti per l'erogazione dei servizi	5
1.3	Responsabile Unico delle Attività Contrattuali	5
1.4	Riservatezza	6
2.	IL CONTESTO DI RIFERIMENTO	6
2.1	Introduzione	6
2.2	Descrizione dell'attuale servizio	7
2.2.1	Servizi per i R.A.O.	7
2.2.2	Servizi di firma remota	7
2.2.3	Servizi di firma automatica	8
2.2.4	Servizi di marcatura temporale	8
2.2.5	Servizi di strong authentication	8
2.2.6	Servizi di emissione certificati web server	8
2.2.7	Servizi di sigillo elettronico	9
2.2.8	Dispositivi fisici di firma Wireless Key	9
2.2.9	Dispositivi business key di firma e accesso	9
2.2.10	Servizio di validazione dei files firmati	9
2.2.11	Servizio Get Info Certificate	9
2.3	Il framework INAIL di firma digitale	9
3.	OGGETTO E DURATA DEL CONTRATTO	13
4.	CARATTERISTICHE DELLA FORNITURA	13
4.1	Servizio Online	14
4.1.1	Portale web per i R.A.O. e per l'emissione dei certificati web server	15
4.1.2	Piattaforma integrabile con API per la gestione/creazione/verifica della firma remota, della firma automatica, della firma temporanea e del sigillo elettronico intestato a persona giuridica	15
4.1.2.1	Servizi di Firma remota, automatica e temporanea integrabile con API	16
4.1.2.2	Servizi di sigillo elettronico	17
4.1.2.3	SPID Professionale e SPID intestato a persona giuridica	17
4.1.3	Applicazione (e/o libreria API) da installare sui device per la firma.	17
4.2	Servizi Connessi	18
4.2.1	Consegna e installazione	18
4.2.2	Assistenza, Aggiornamento e Manutenzione	19
4.2.3	Servizi di Reportistica e accounting	19
4.3	Dispositivi di firma e accesso con CNS (Carta Nazionale dei Servizi)	20
4.4	Assistenza Specialistica	20
5.	VERIFICA DI CONFORMITÀ INIZIALE E ATTIVAZIONE DEL SERVIZIO	20
6.	LIVELLI DI SERVIZIO	21
7.	PENALI	21



1. **PREMESSA**

Il presente documento disciplina gli aspetti tecnici relativi all'affidamento dei certificati digitali per l'Istituto Nazionale Assicurazione contro gli Infortuni sul Lavoro (d'ora in poi INAIL o Istituto) come di seguito descritto.

Nel perimetro della Convenzione stipulata tra INAIL e Consip S.p.A. in data 17/03/2022, l'Istituto ha affidato a Consip S.p.A. un'iniziativa relativa all'acquisizione di servizi per la dotazione di certificati digitali (es. firma digitale remota, firma massiva, sigillo elettronico, marche temporali, SPID, ecc.) come descritto nel presente documento che ha lo scopo di definire le caratteristiche e i requisiti minimi relativi alla fornitura dei suddetti servizi per INAIL, in quantità, qualità e livelli di servizio.

Ai fini del presente documento, i termini di cui appresso, devono essere intesi come segue:

- **Capitolato Tecnico:** il presente documento;
- **Contratto:** il contratto che verrà stipulato tra INAIL e l'Impresa aggiudicataria, recante le clausole che disciplineranno i rapporti giuridici tra le parti (INAIL e Impresa) nell'esecuzione del Servizio;
- **Malfunctionamento:** qualsiasi anomalia funzionale e, in ogni caso, ogni difformità di quanto acquisito rispetto alla relativa documentazione tecnica e manualistica d'uso o alle specifiche del presente Capitolato, che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità di quanto fornito;
- **Stazione Appaltante:** Consip S.p.A.;
- **Fornitura:** il complesso delle prestazioni descritte nel presente documento;
- **Fornitore o Società:** il concorrente risultante aggiudicatario della presente procedura di gara;
- **Responsabile Unico delle Attività Contrattuali o Responsabile del Servizio:** la persona individuata dalla Società come interlocutore dell'Amministrazione e responsabile di tutte le attività contrattuali. Per talune attività meramente tecniche può delegare a un **Responsabile della Fornitura**;
- **Piattaforma:** la Piattaforma software per l'erogazione dei servizi oggetto della presente procedura di gara;
- **RUP e DEC:** rispettivamente il Responsabile Unico del Procedimento e il Direttore dell'Esecuzione del Contratto;
- **DCOD:** Direzione Centrale per l'Organizzazione Digitale di INAIL;
- **R.A.O. - Registration Authority Office:** la Pubblica Amministrazione che svolge l'attività di verifica dell'identità personale.
- **Titolare/i:** soggetto/i appartenente/i all'Istituto per cui è richiesta l'emissione di un certificato di firma digitale;
- **CAD:** Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale";
- **Dispositivo sicuro di firma:** dispositivo che soddisfa i requisiti dell'allegato II del Regolamento UE n. 2014/910 (Regolamento eIDAS) e conforme all'art. 35 del CAD;
- **Dispositivi fisici:** salvo diversa indicazione, nel corso della descrizione dei servizi oggetto della presente procedura, con questo termine si intendono i dispositivi di cui al successivo paragrafo 4.3.
- **Certificato qualificato:** certificato conforme al Regolamento eIDAS;
- **Firma digitale:** particolare tipo di firma qualificata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici, in conformità al CAD;
- **Sigillo elettronico qualificato:** conforme al Regolamento eIDAS;



- **HSM**: dispositivo sicuro per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche, in conformità all'art. 35 del CAD;
- **Firma remota**: procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse;
- **Firma automatica**: procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo, in conformità all'art. 35 del CAD;
- **Firma remota automatica**: particolare procedura informatica di firma automatica generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse;
- **Prestatore di servizi fiduciari qualificati**: l'operatore economico, iscritto all'apposito elenco di fiducia tenuto da AgID, ai sensi dell'art. 29 del CAD, per i servizi oggetto della presente iniziativa, ossia: certificato qualificato per firma elettronica (QCert for eSig); certificato qualificato per timbro elettronico (Qcert for eSeal); certificato qualificato per autenticazione siti web (QWAC) e marca temporale qualificata (Qtimestamp);
- **SPID**: Sistema Pubblico di Identità Digitale;
- **Token OTP**: Dispositivo hardware personale in grado di visualizzare One Time Password (OTP) da utilizzare per l'autenticazione al sistema di firma remota;
- **Web service**: Servizio informatico erogato mediante protocollo HTTP o HTTPS per l'interazione server-to-server in rete. La sua interfaccia è descritta in un formato elaborabile da un server (WSDL);
- **WSDL**: Acronimo di Web Services Description Language;
- **Sistema Informativo**: il sistema informativo dell'INAIL che ha sede in Roma, Via del Santuario Regina degli Apostoli 33.

Se non diversamente specificato i termini temporali espressi nel presente documento sono tutti da intendersi come solari.

1.1 Prescrizioni in materia di sicurezza

Tutte le forniture devono essere conformi alla normativa vigente che regola la loro produzione, commercializzazione ed utilizzazione; devono inoltre rispettare, ciascuna per le singole specifiche caratteristiche, le seguenti prescrizioni in materia di sicurezza, ove applicabili in relazione alla natura della prestazione:

- Legge 1° marzo 1968, n. 186 "Disposizioni concernenti la produzione di materiali, apparecchiature, macchinari, installazioni e impianti elettrici ed elettronici";
- D.Lgs. 19 maggio 2016 n. 86, "Attuazione della direttiva 2014/35/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato del materiale elettrico destinato ad essere adoperato entro taluni limiti di tensione";
- D.Lgs. 25 luglio 2005, n. 151, "attuazione delle direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti";
- D. Lgs. 3 aprile 2006, n. 152, "Norme in materia ambientale";
- D. Lgs. 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro";
- D.Lgs. 4 settembre 2024, n. 138, recante "Recepimento della direttiva (UE) 2022/2555, relative a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del



regolamento (UE) m. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148”;

- Norme UNI e CEI di riferimento.

Con riferimento ai dispositivi fisici:

- è fatto obbligo al Fornitore di garantire la sicurezza di quanto fornito, documentando, in particolare, l'eventuale presenza di sostanze nocive o cancerogene;
- le apparecchiature fornite devono essere marcate CE e devono essere corredate di informazioni utili al loro smaltimento integrale o di parti di esse, in conformità con la vigente normativa in materia.

1.2 Requisiti per l'erogazione dei servizi

La fornitura e i servizi dovranno essere erogati dal Fornitore che **dovrà mantenere, per tutta la durata del Contratto, la qualifica di prestatore dei servizi fiduciari qualificati oggetto della presente iniziativa, iscritto all'apposito elenco tenuto dall'AgID ai sensi dell'art. 29 del CAD, così come richiesta per la partecipazione alla presente iniziativa nel Disciplinare di Gara.**

Le componenti ed i servizi forniti devono essere conformi alla normativa vigente ed alle relative regole tecniche, ove applicabili in relazione alla natura della prestazione, tra cui, in particolare:

- Determinazione AgID n. 147/2019 (Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate) e s.m.i.;
- DPCM 10 febbraio 2010 (Autocertificazione dispositivi automatici di firma) e s.m.i.;
- DPCM 19 luglio 2012 (Decreto sui dispositivi automatici di firma - HSM) e s.m.i.;
- DPCM 22 febbraio 2013 (Nuove Regole Tecniche) e s.m.i.;
- DPCM 5 febbraio 2015 (Dispositivi certificati per apposizione di firme elettroniche) e s.m.i.;
- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale” (CAD) e s.m.i.;
- Regolamento UE n. 910/2014 (c.d. Regolamento eIDAS) e s.m.i.
- Regolamento per le Infrastrutture Digitali e per i Servizi Cloud per la Pubblica Amministrazione (Regolamento Cloud), ai sensi dell'articolo 33-septies, comma 4, dell'D.L. 179/2012, convertito, con modificazioni, in legge 221/2012, adottato dall'Agenzia per la Cybersicurezza Nazionale (ACN) con Decreto Direttoriale n. 21007/24 del 27 giugno 2024.

1.3 Responsabile Unico delle Attività Contrattuali

Il Fornitore dovrà comunicare, prima della stipula del Contratto, congiuntamente alla documentazione per la stipula presentata, il nominativo del proprio rappresentante, designato quale **Responsabile Unico delle Attività Contrattuali (RUAC)** e del coordinamento delle stesse, configurandosi pertanto come **Responsabile del Servizio**, nonché interlocutore unico dell'Istituto per gli aspetti amministrativi, per l'organizzazione ed il coordinamento delle attività contrattuali.

Il Fornitore deve provvedere in piena autonomia al coordinamento ed all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti dall'Istituto.

Sarà cura del RUAC curare la gestione amministrativa del contratto e delle connesse attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

Al fine di assicurare il coordinamento della fornitura e del servizio di manutenzione, il RUAC dovrà garantire la reperibilità negli orari di esecuzione della fornitura e dei servizi richiesti.



In qualsiasi momento, nel corso dell'esecuzione contrattuale, il RUAC potrà delegare una o più attività, **meramente tecniche**, tra quelle di propria competenza, a un **Responsabile della Fornitura**, dandone previa comunicazione scritta a INAIL.

Sarà cura del RUAC verificare il rispetto di tutti gli adempimenti contrattuali, curando in particolare il rispetto dei tempi e delle modalità di consegna della documentazione e dei prodotti.

Ogni comunicazione riguardante aspetti contrattuali dovrà essere scambiata tra il responsabile INAIL e il RUAC.

1.4 Riservatezza

A maggior dettaglio rispetto a quanto previsto nelle Condizioni Generali del Contratto, tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra il Fornitore e INAIL sono riservati; pertanto, è richiesta la massima attenzione per il loro utilizzo, in particolare se questo avviene al di fuori delle sedi INAIL.

Il Fornitore non potrà utilizzare, a nessun titolo, la documentazione ricevuta o prodotta, al di fuori delle attività oggetto del presente Capitolato.

Il Fornitore non potrà utilizzare, a nessun titolo, la documentazione e i prodotti software forniti da INAIL o realizzati per il servizio, al di fuori delle attività oggetto del presente capitolato.

2. IL CONTESTO DI RIFERIMENTO

2.1 Introduzione

Il percorso della *digital transformation* dell'INAIL continua a far leva sui processi interni di dematerializzazione e digitalizzazione per migliorarne l'efficienza e l'affidabilità, utilizzando strumenti certificati al fine di produrre documenti informatici che ne garantiscano la sicurezza, l'integrità e l'immodificabilità e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. Nel corso degli anni l'Istituto ha messo in atto una serie di azioni consolidate attraverso l'integrazione nelle proprie componenti applicative dei servizi fiduciari erogati dall'attuale Fornitore. A tal riguardo sono stati acquistati dall'Istituto **servizi di firma digitale, dispositivi di firma e il servizio di supporto specialistico**. In particolare, attraverso l'iniziativa ID 2375, è stata acquisita la seguente fornitura:

I. Servizio Principale, comprendente le seguenti componenti:

- *Portale web per i R.A.O. (Registration Authority Office) e per l'emissione dei certificati web-server;*
- *Servizi di Firma remota, automatica e temporanea integrabile con API;*
- *Piattaforma per la gestione/creazione/verifica delle firme remote/automatiche;*
- *Sigillo elettronico (uno) intestato a persona giuridica (INAIL) integrabile con API;*
- *Applicazione (e/o libreria API) da installare sui device per la firma.*

Tale servizio principale è integrato con il framework INAIL di cui al successivo paragrafo.

II. Fornitura di:

- *Certificati remoti con OTP (APP);*
- *Certificati remoti con OTM (SMS);*
- *Certificati di firma automatica;*
- *Marche temporali*
- *Dispositivi fisici di firma digitale comprensivi di manutenzione;*
- *Certificati di firma temporanea*

III. Manutenzione correttiva del timbro digitale già di proprietà INAIL



IV. Manutenzione evolutiva del timbro digitale già di proprietà di INAIL

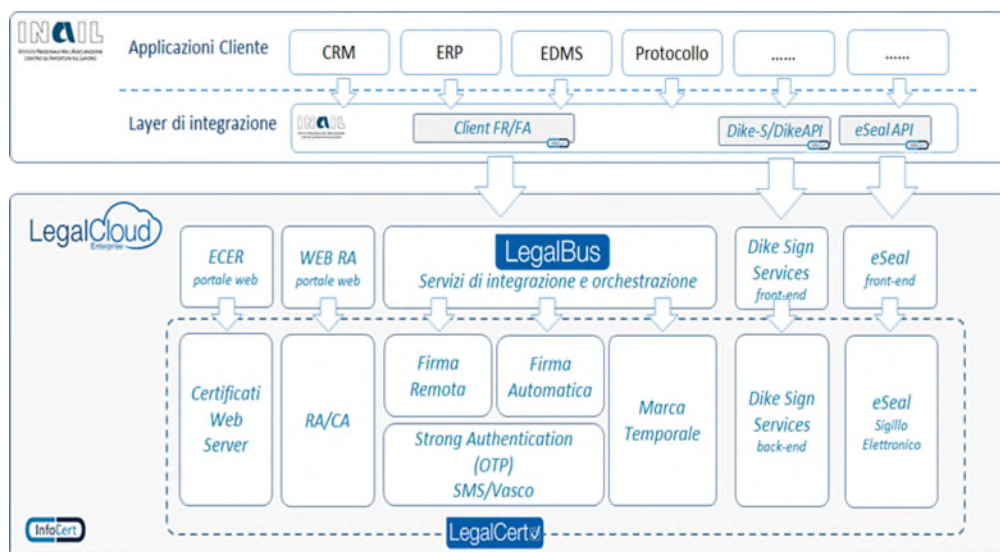
V. Assistenza Specialistica.

Per i dettagli dell'iniziativa precedente, ID 2375, si rimanda al sito Consip al seguente link:

<https://www.consip.it/bandi-di-gara/gare-e-avvisi/gara-certificati-di-firma-digitale>.

2.2 Descrizione dell'attuale servizio

L'attuale sistema in opera presso INAIL è una soluzione enterprise di servizi di firma digitale certificata. Di seguito la vista dell'architettura attualmente attiva, con evidenza della parte d'integrazione realizzata da INAIL (di seguito descritta):



2.2.1 Servizi per i R.A.O.

I R.A.O. hanno accesso ai portali dell'attuale Fornitore e sono adibiti alle:

- attività di registrazione dei dati dei Titolari, a cui sono/saranno intestati i certificati qualificati (siano essi di firma remota sia di firma automatica);
- attività di emissione dei certificati stessi.

Il Titolare del certificato qualificato ha accesso al portale web dell'attuale Fornitore per poter operare il controllo del proprio certificato (remoto/automatico) ai fini delle modifiche delle credenziali (quali il PIN), del proprio numero di cellulare ed eventualmente richiederne la sospensione.

Nell'ambito di tali servizi INAIL usufruisce di lotti di certificati (remoti/automatici) da poter rilasciare ai propri utenti.

2.2.2 Servizi di firma remota

I certificati qualificati di firma remota vengono emessi dai R.A.O. INAIL e sono utilizzati dai singoli Titolari per mezzo di servizi remoti integrati dagli applicativi INAIL tramite specifiche API fornite



dall'attuale Fornitore che semplificano l'accesso al servizio di firma remota. Inoltre, i certificati possono essere raggiunti direttamente tramite web services integrati nella piattaforma erogata dal fornitore.

In tal modo, gli utenti provvisti di certificato remoto possono sottoscrivere digitalmente documenti, in modalità del tutto trasparente, attraverso le funzionalità esposte dagli applicativi INAIL che hanno già integrato tali servizi di firma.

I servizi di firma remota consentono di sottoscrivere documenti nelle seguenti modalità:

- firma CADES (ovvero firma con estensione.p7m);
- firma PADES (ovvero firma con estensione.pdf);
- firma XADES (ovvero firma con estensione.xml).

2.2.3 Servizi di firma automatica

I certificati qualificati di firma automatica vengono emessi dai R.A.O. INAIL e sono utilizzabili dagli applicativi INAIL per sottoscrivere in modo massivo documenti generati da specifici processi interni aziendali e per i quali i certificati automatici sono stati rilasciati. I singoli Titolari possono in ogni momento abilitare/disabilitare il certificato tramite l'accesso al portale web dell'attuale fornitore. I servizi di firma automatica sono integrati negli applicativi INAIL tramite specifiche API fornite dall'attuale Fornitore che semplificano l'accesso al servizio di firma automatica e possono essere raggiunti direttamente tramite web services, integrati nella piattaforma erogata dall'attuale fornitore.

I servizi di firma automatica consentono di sottoscrivere documenti nelle seguenti modalità:

- firma CADES (ovvero firma con estensione.p7m);
- firma PADES (ovvero firma con estensione.pdf);
- firma XADES (ovvero firma con estensione.xml).

2.2.4 Servizi di marcatura temporale

Nell'ambito delle azioni di firma remota o automatica, INAIL beneficia di un numero di Marche Temporal che vengono utilizzate, in specifici casi previsti dalle proprie componenti applicative, contestualmente alle operazioni di firma.

La marcatura temporale viene apposta, quando espressamente richiesta, in fase di firma sempre attraverso l'integrazione applicativa effettuata da INAIL verso le API di firma remota o automatica.

2.2.5 Servizi di strong authentication

Nell'ambito della firma remota, gli utenti firmatari devono autorizzare l'azione di firma tramite Strong Authentication che richiede all'utente l'inserimento di due credenziali:

- il PIN di firma scelto dal Titolare in fase di emissione del certificato;
- la OTP (One Time Password) generata ad ogni transazione di firma.

Per la gestione della OTP, INAIL usufruisce di due modalità alternative per singolo certificato:

- invio OTP tramite SMS;
- invio OTP tramite APP.

2.2.6 Servizi di emissione certificati web server

Attraverso un portale web dell'attuale fornitore, INAIL gestisce autonomamente l'emissione di certificati web server, entro i limiti numerici stabiliti dal contratto. I certificati gestibili sono delle seguenti tipologie:

- Certificato Web di tipo "Wildcard" multidominio con validità 36 mesi;



- Certificati Web Server a dominio singolo con validità 36 mesi;
- Certificati Web Server SAN (Subject Alternative Name) con validità 36 mesi;
- Certificati Code-Sign con validità 36 mesi.

2.2.7 Servizi di sigillo elettronico

Per soddisfare l'esigenza di poter siglare documenti senza perdita di integrità del documento già sottoscritto, INAIL ha adottato la soluzione dell'attuale Fornitore (servizio certificato eIDAS) per l'emissione di sigilli elettronici basata su certificati qualificati eSeal intestati a persona giuridica. Tale servizio è stato integrato dagli applicativi INAIL abilitati all'apposizione del sigillo su documenti già sottoscritti (es. Protocollo Informatico), in modo tale da visualizzare sul documento le informazioni che accompagnino il sigillo (come, ad esempio, il numero di protocollo); il documento viene generato predisponendo in anticipo il relativo campo firma che sarà utilizzato per applicare il sigillo stesso.

I servizi di firma con sigillo elettronico sono utilizzati tramite le integrazioni applicative eseguite da INAIL, adottando le API, fornite dall'attuale fornitore, del servizio eSeal.

2.2.8 Dispositivi fisici di firma Wireless Key

Al fine di usufruire di dispositivi fisici che abilitino l'utente a sottoscrivere digitalmente anche da dispositivo mobile, INAIL ha acquisito dall'attuale Fornitore il nuovo dispositivo di firma denominato Wireless Key, ovvero una "chiavetta" di firma che consente all'utente di firmare anche con dispositivi mobile (tablet, smartphone) dotati di tecnologia Bluetooth.

Il dispositivo WirelessKey viene usato sia su desktop tramite USB che su tablet e smartphone per firmare digitalmente qualunque documento grazie alla possibilità di collegarlo direttamente all'app tramite Bluetooth.

2.2.9 Dispositivi business key di firma e accesso

Il nuovo dispositivo di firma denominato Business Key è un dispositivo che utilizza la CNS per consentire l'autenticazione sui siti della PA in modalità mobile (tablet, smartphone) oltre che per firmare digitalmente.

2.2.10 Servizio di validazione dei files firmati

Nell'ambito delle azioni di firma remota ed automatica, marca temporale e sigillo, Inail beneficia di un servizio di validazione dei files firmati attraverso l'integrazione applicativa effettuata da Inail verso le API di validazione dell'attuale fornitore.

2.2.11 Servizio Get Info Certificate

Servizio che espone in chiave pubblica i dettagli dei certificati di firma (es., common name, scadenza, CA con cui è stato emesso, etc.).

2.3 Il framework INAIL di firma digitale

L'Istituto ha progettato e realizzato un framework di firma digitale per consentire alle applicazioni software istituzionali e gestionali di poter utilizzare i servizi di firma erogati dall'attuale Fornitore e che **dovrà essere mantenuto a prescindere dall'aggiudicatario della presente procedura di gara**. Il sistema di firma digitale è principalmente costituito da tre componenti:



- **InailSign:** Web Application disponibile a tutte le applicazioni censite all'interno dell'archivio del Servizio di Firma Digitale i cui compiti sono:
 - gestire le richieste di back-end dalle applicazioni Web integrate con il sistema;
 - richiedere le credenziali di firma all'utente (alias/pin/OTP);
 - interfacciarsi con il Middleware per la generazione di un token di sessione che consenta la firma via API;
 - veicolare il token generato all'applicazione che l'ha richiesto, in modo che possa utilizzarlo per creare una sessione di firma.
- **Servizi "API":** utilizzati dalle procedure per applicare il servizio di firma nei documenti. Rappresentano lo strato di Web Services (Middleware) che ha il compito di gestire le richieste di apposizione della firma digitale provenienti dalle Web Application dell'Istituto che interagiscono con gli utenti, utilizzando i servizi dell'attuale fornitore. Le principali operazioni esposte dal Middleware sono le seguenti:
 - *Signsinglepades:* permette di firmare un file PADES con PDF layout da file .pdf a Firmato_nomeFile.pdf.
 - *Signsinglecades:* permette di firmare un file CADES da .* a Firmato_*.p7m.
 - *Signmultipades:* permette di firmare più file in modalità PADES con PDF Layout per ciascun file – da .pdf a Firmato_.pdf.
 - *Signmulticades:* permette di firmare un insieme di file di qualsiasi tipo in modalità Firma multi CADES da .* a Firmato_*.p7m.
 - *Signmultixades:* permette di firmare in modalità MULTI XADES da .xml a Firmato_.xml.
 - *Signautomaticfiles:* permette di firmare un insieme di files pdf all'interno della stessa sessione di firma e all'occorrenza di apporre un Timestamp per ciascun file durante la stessa sessione.
 - *Sigillosignature:* consente di apporre a uno o più documenti una firma digitale con certificato intestato a persona giuridica – E-Seal.
 - *Servicetimestamp:* permette di effettuare l'operazione di timestamp di un file pdf.
 - *Servizio di verifica:* permette di effettuare l'operazione di timestamp di un file pdf.
 - *Servizio di validation:* consente di verificare file firmati PADES, XADES, CADES e TIMESTAMP.;
- **Console di enrollment:** contiene gli strumenti utili a gestire i certificati di firma digitale (rilascio, revoca, verifica, relazione con strumenti dell'attuale fornitore); Strumento ad uso dei responsabili del Servizio di Firma Digitale e dei RAO; alimenta, tramite integrazione con Api Legal Mail, un archivio locale all'Istituto che consente verifiche, monitoraggi e statistiche sui certificati emessi per le diverse tipologie di Utenti in coerenza con la classificazione degli incarichi presenti nei sistemi Human Resources dell'Istituto. Contiene la lista delle procedure integrate con il Sistema di Firma Digitale e autorizzate ad utilizzare le Api di Firma Digitale.

Tali componenti integrano tutti i servizi erogati dalla piattaforma dell'attuale Fornitore realizzando una completa trasversalità rispetto alla complessità delle componenti applicative interne INAIL, grazie alla versatilità dei servizi esposti: librerie, per integrazioni più semplici e delimitate; servizi più sofisticati in grado di assolvere maggiori e specifici compiti, con funzionalità più ampie e rivolte ad un utilizzo trasversale rispetto al tipo di dispositivo adottato. Le componenti sono state progettate per poter gestire tutte le esigenze delle applicazioni istituzionali di firma digitale, fornendo un modello di dialogo verso i servizi dell'attuale Fornitore disaccoppiando i due sistemi



in modo da facilitare la selezione del servizio, tra quelli offerti dal fornitore, più idoneo alla richiesta proveniente dall'applicazione.

Da un punto di vista organizzativo la gestione è stata centralizzata su uno specifico team di risorse specialistiche interno alla struttura DCOD (Direzione Centrale per l'Organizzazione Digitale) che si occupa:

- dell'assicurazione della fruizione dei servizi di firma da parte degli utenti fisici e delle applicazioni;
- del monitoraggio delle attività richieste sia lato procedurale che verso le applicazioni software che utilizzano i servizi di firma;
- assicurano il corretto esercizio del sistema integrato "framework-LegalCloud".

Il team interagisce con il supporto specialistico dell'attuale fornitore, effettua sviluppo software, esegue il monitoraggio ed eroga supporto alla struttura tecnica e agli utenti interni nonché verso il Fornitore per la gestione/rinnovo dei certificati e la proposizione di nuove soluzioni di integrazione con le applicazioni.

Il framework è monitorato dai servizi di Service Control Room interna alla DCOD per rilevare e segnalare malfunzionamenti, misurare il rispetto dei livelli di servizio e attivare i gruppi specialistici di intervento. Tale Service Control Room viene integrata con gli sviluppi di un sistema di gestione e di monitoraggio per la segnalazione di eventuali indisponibilità del sistema di firma.

Infine, il Framework INAIL viene costantemente evoluto in ottica di servizi DevOps verso le applicazioni che si stanno realizzando applicando la logica a microservizi.

A titolo meramente esemplificativo e non esaustivo, si indicano di seguito i dati relativi all'utilizzo del sistema negli anni passati. Il numero di eventi di firma alla data del 30 aprile 2024 è riportato nella seguente tabella:

Tipologia di certificato	Numerosità
Firma automatica/massiva	1.956.470
Firma remota PADES	1.613.997
Firma remota CADES	202.028
Firma remota XADES	10
Marca temporale	1.068
Servizio di Verifica	817.272
Sigillo	19.932
Get info Certificate	275.136

I numeri di certificati personali di firma remota sono:

- Rilasciati: 1.250;
- Numero di certificati automatici in uso: 3.

Complessivamente, dal 1° gennaio 2020 al 30 aprile 2024, le varie applicazioni integrate con il servizio di firma sono state interessate secondo la seguente tabella:

Rilevazione dal 01 Gennaio 2020 al 30 Aprile 2024		
ID	Applicazioni integrate con il servizio di firma	Firme eseguite



Rilevazione dal 01 Gennaio 2020 al 30 Aprile 2024		
1	AP Formazione	240
2	Arco Audit	460
3	Banca Dati Silice	20
4	Bando formazione integrazioni	128
5	Batc_Client Fattura PA	8117
6	Cash Management	3684
7	CCR_Prod	1
8	Dimora	2490
9	Emissioni Acustiche	434
10	eRIS	11837
11	Fidia Prod	1955
12	Firma EBS	27009
13	FOIA	813
14	Gestione Contratti Digitali	25631
15	Gestione Determine	8707
16	Gestione Rimborsi Conto Stato	8
17	GRA WEB	146923
18	ISI_BO	8211
19	ISI_Console	3
20	ISI Back Office	21354
21	POM SPA	58037
22	PRince	409910
23	Sailfor	6414
24	SM_ITBM	7998
25	Teleforum	1137
26	Vigilanza Web_upgrade	4194
27	Websigner	98564
TOTALE		1.104.902



3. OGGETTO E DURATA DEL CONTRATTO

Oggetto del Contratto saranno i servizi come di seguito articolati, secondo le quantità stabilite nel Disciplinare di Gara:

- a) Servizio online per l'utilizzo di:
 - a.1) Portale web per i R.A.O. e per l'emissione dei certificati web-server;
 - a.2) Piattaforma integrabile con API per la gestione/creazione/verifica della firma remota, della firma automatica, della firma temporanea e del sigillo elettronico intestato a persona giuridica;
 - a.3) Applicazione (e/o libreria API) da installare sui device (smartphone e desktop) per la firma;
- b) Fornitura di Certificati Digitali di:
 - b.1) Certificati remoti con OTP (APP)
 - b.2) Certificati di firma automatica
 - b.3) Marche temporali
 - b.4) Certificato qualificato per sigillo elettronico intestato a persona giuridica
 - b.5) Firme temporanee per utilizzo one-shot (usa e getta)
 - b.6) Dispositivi fisici di firma digitale con CNS (comprensivi di manutenzione)
 - b.7) Spid professionali (opzionali)
 - b.8) SPID intestato a persona giuridica (opzionale)e relativi servizi connessi inclusi nella fornitura (consegna, reportistica, aggiornamento e manutenzione);
- c) Assistenza Specialistica.

Per l'intera durata contrattuale dovrà essere assicurata la validità di tutti i certificati senza oneri aggiuntivi, nonché l'aggiornamento tecnologico dei dispositivi di firma e l'adeguamento alla normativa in corso di vigenza.

Il Fornitore aggiudicatario della presente iniziativa dovrà supportare l'Istituto nell'aggiornamento del layer di integrazione senza alcun onere aggiuntivo.

4. CARATTERISTICHE DELLA FORNITURA

Nei seguenti sotto paragrafi sono indicate le caratteristiche richieste per la fornitura e i servizi, secondo le quantità e le modalità di remunerazione previste nel Disciplinare di Gara.

In aggiunta, rispetto alle caratteristiche dei singoli servizi, riportate nei successivi paragrafi, si evidenzia quanto segue.

Il Fornitore sarà libero di erogare le prestazioni mediante soluzioni fruibili in modalità cloud, ma in tal caso dovrà darne specifica evidenza in sede di partecipazione alla gara, secondo quanto previsto dal Disciplinare di Gara.



Infatti, in tal caso, le prestazioni dovranno essere erogate nel rispetto dei requisiti descritti dall'ACN, in tema di qualificazione dei servizi e di adeguamento delle infrastrutture cloud e troverà applicazione quanto previsto dal Regolamento Cloud

La tipologia di dato trattato ai fini della presente iniziativa è quello **Ordinario**.

Pertanto, nei casi in cui le prestazioni siano erogate mediante soluzioni fruibili in modalità cloud, ai fini della stipula del Contratto, come meglio indicato nel Disciplinare di Gara, dovrà essere dimostrato il possesso della qualificazione **QC1** per i servizi cloud (erogati da infrastrutture dei servizi cloud per le pubbliche amministrazioni con adeguamento almeno **A11**). Tale livello di qualificazione/adeguamento minimo dovrà essere mantenuto per tutta la durata del Contratto.

Nei casi di cui all'art. 19, comma 9, 20, commi 3 e 4 e 21 comma 5 del Regolamento Cloud, e in ogni caso di avvio di qualsivoglia procedimento finalizzato alla revoca/sospensione/dichiarazione di inadeguatezza da parte di ACN, il Fornitore dovrà comunicare a INAIL quanto ivi previsto entro 5 giorni solari dalla rispettiva comunicazione di ACN, pena l'applicazione di apposita penale.

Resta salvo il diritto dell'INAIL di acquisire le corrispondenti informazioni anche d'ufficio, con la conseguenza che, laddove emergesse la mancata comunicazione a INAIL nel termine sopra riportato, quest'ultima applicherà la penale prevista.

In ogni caso di procedimenti di cui sopra, il Fornitore si impegna a comunicare all'INAIL qualsivoglia indicazione ricevuta da ACN, entro 5 giorni solari dalla relativa ricezione, e a prestare, ove possibile, la necessaria collaborazione all'eventuale diverso produttore/proprietario del servizio cloud/infrastruttura, pena l'applicazione della medesima penale sopra richiamata.

In caso di revoca della qualificazione e/o di dichiarazione di inadeguatezza si applica quanto previsto dall'art. 21 del Regolamento Cloud.

Resta inteso che:

- in caso di revoca della qualificazione o dichiarazione di inadeguatezza dell'adeguamento;
- in caso di mancato rinnovo della qualificazione;
- in caso di sospensione della qualificazione, se quest'ultima non possa consentire la continuità delle prestazioni contrattuali per un tempo superiore a 15 giorni;

troverà applicazione quanto previsto in tema di "Risoluzione" nel Contratto.

4.1 Servizio Online

Il servizio Online richiesto sarà realizzato in modalità remota e comprenderà le seguenti componenti riportate al precedente paragrafo 3 (lettere a.1), a.2) e a.3)) e descritte successivamente.

Fermo restando quanto previsto nel successivo paragrafo 4.2, il servizio online dovrà essere integrabile con il framework INAIL di cui alla precedente sezione 2.3 attraverso librerie, API o qualunque altra modalità per l'integrazione, **senza alcun onere aggiuntivo per l'Istituto e senza soluzione di continuità con l'attuale servizio adoperato dall'INAIL**. Tale servizio dovrà essere raggiunto attraverso un collegamento di rete, senza costi aggiuntivi per l'Istituto. Tale collegamento dovrà avvenire solo attraverso un canale di comunicazione cifrato e previa mutua identificazione ed autorizzazione. Le apparecchiature per l'erogazione del servizio di firma (HSM) dovranno essere installate presso il CED del Fornitore o comunque nelle sue disponibilità, all'interno del territorio dell'Unione Europea. Il Fornitore dovrà consegnare a INAIL copia del relativo Manuale Operativo.



4.1.1 Portale web per i R.A.O. e per l'emissione dei certificati web server

I R.A.O. (di INAIL) dovranno avere accesso al portale del Fornitore oppure a un portale adibito *ad hoc* per le seguenti attività:

- registrazione dei dati dei “Titolari del certificato qualificato”, a cui sono/saranno intestati i certificati qualificati (siano essi di firma remota sia di firma automatica);
- emissione dei certificati stessi.

Il Titolare del certificato qualificato deve avere accesso ad un portale web per poter operare il controllo del proprio certificato (remoto/automatico) ai fini delle modifiche delle credenziali (quali il PIN), del proprio numero di cellulare ed eventualmente richiederne la sospensione.

Nell'ambito di tali servizi INAIL deve poter usufruire di lotti di certificati (remoti/automatici) da poter rilasciare ai propri utenti, come descritto successivamente.

4.1.2 Piattaforma integrabile con API per la gestione/creazione/verifica della firma remota, della firma automatica, della firma temporanea e del sigillo elettronico intestato a persona giuridica

Il Fornitore dovrà garantire all'Istituto l'utilizzo in modalità remota della sua piattaforma per la gestione/creazione/verifica della firma remota, della firma automatica, della firma temporanea e del sigillo elettronico intestato a persona giuridica.

Nell'ambito della firma remota, gli utenti firmatari devono poter autorizzare l'azione di firma tramite Strong Authentication che richiede all'utente l'inserimento di due credenziali:

- il PIN di firma scelto dal Titolare in fase di emissione del certificato;
- la OTP (One Time Password) generata ad ogni transazione di firma.

Per la gestione della OTP si prevede soltanto la modalità tramite APP per singolo certificato.

Nel caso di errore sull'autenticazione è richiesta una diagnostica dettagliata (quale ad esempio l'utente ha fornito una password errata, il valore dell'OTP è fuori sincronismo, ecc.).

Attraverso il portale di cui al punto 4.1.1, INAIL dovrà poter gestire autonomamente l'emissione di certificati web server, entro le quantità stabilite dal Contratto, e i certificati gestibili dovranno essere delle seguenti tipologie:

- Certificato Web di tipo “WildCard” multidominio con validità 36 mesi;
- Certificati Web Server a dominio singolo con validità 36 mesi;
- Certificati Web Server SAN (Subject Alternative Name) con validità 36 mesi;
- Certificati Code-Sign con validità 36 mesi.

Il Fornitore dovrà fornire il Manuale Operativo che regola il servizio di firma remota. L'emissione dei certificati potrà essere richiesta in qualunque momento nel corso del periodo della durata del contratto. Nel caso di smarrimento/furto/malfunzionamento del token OTP è possibile richiederne la sostituzione senza revoca del certificato.

- Il Fornitore dovrà fornire ai Titolari i seguenti servizi per la gestione delle credenziali di attivazione del sistema di firma remota, in modalità sicura mediante il servizio di assistenza dedicato di cui alla successiva sezione 4.2.2 o attraverso lo stesso portale web, disponibili al Titolare H24 per 365 giorni l'anno:
- funzioni per il cambio password;



- funzioni per lo sblocco dell'utenza;
- funzione di risincronizzazione tra il sistema di autenticazione ed il dispositivo OTP.

La gestione del ciclo di vita dei certificati per il sistema di firma remota e automatica avrà durata fino alla conclusione dell'ultimo certificato emesso. La procedura di revoca e/o sospensione dei certificati deve essere fruibile per tutto il periodo di validità dei certificati emessi. Dovranno essere previste più modalità di attivazione di tale procedura (mail, portale web, ecc).

4.1.2.1 Servizi di Firma remota, automatica e temporanea integrabile con API

I certificati qualificati di **firma remota** devono poter essere emessi dai R.A.O. INAIL, utilizzati dai singoli Titolari per mezzo di servizi remoti integrati dagli applicativi INAIL tramite specifiche API fornite dal Fornitore che semplificano l'accesso al servizio di firma remota, **e devono poter essere raggiunti direttamente tramite web services esposti.**

In tal modo, gli utenti provvisti di certificato remoto possono sottoscrivere digitalmente documenti, in modalità del tutto trasparente, attraverso le funzionalità esposte dagli applicativi INAIL che hanno già integrato tali servizi di firma.

I servizi di firma remota devono consentire di sottoscrivere documenti nelle seguenti modalità:

- firma CADES (ovvero firma con estensione.p7m);
- firma PADES (ovvero firma con estensione.pdf);
- firma XADES (ovvero firma con estensione.xml).

I certificati qualificati di **firma automatica** devono essere emessi dai R.A.O. INAIL e utilizzabili dagli applicativi INAIL per sottoscrivere in modo massivo documenti generati da specifici processi interni aziendali per i quali i certificati automatici sono stati rilasciati. I singoli Titolari possono in ogni momento abilitare/disabilitare il certificato tramite l'accesso ad un portale web.

I servizi di firma automatica devono essere integrati negli applicativi INAIL tramite specifiche API fornite dal fornitore, che semplificano l'accesso al servizio di firma automatica, **e possono essere raggiunti direttamente tramite web services esposti.**

I servizi di firma automatica devono consentire di sottoscrivere documenti nelle seguenti modalità:

- firma CADES (ovvero firma con estensione.p7m);
- firma PADES (ovvero firma con estensione.pdf);
- firma XADES (ovvero firma con estensione.xml).

I certificati qualificati di **firma temporanea**, cosiddetta "one-shot", dovranno essere emessi con le stesse modalità descritte nel capoverso relativo alla firma remota e avranno una durata limitata all'evento previsto da tale firma, ovvero la firma di firma verbali ispettivi, del consenso informato ed altre tipologie di documenti che prevedono un'interazione fra l'Istituto e un soggetto potenzialmente sprovvisto di firma digitale.

Deve essere garantita anche la **marcatatura temporale**: infatti nell'ambito delle azioni di firma remota o automatica, INAIL dovrà beneficiare di Marche Temporalì che verranno utilizzate, in specifici casi previsti dalle proprie componenti applicative, contestualmente alle operazioni di firma.

La marcatatura temporale viene apposta, quando espressamente richiesta, in fase di firma sempre attraverso l'integrazione applicativa effettuata da INAIL verso le API di firma remota o automatica. Le marche temporalì prodotte dal Fornitore dovranno essere conformi alle normative vigenti indicati al paragrafo 1.2.

Il servizio di emissione di marche temporalì dovrà essere accessibile da rete Internet, realizzato mediante protocollo HyperText Transfer Protocol (HTTP) in conformità a quanto espresso da RFC 3161 e successive modificazioni e deve poter essere richiesto anche mediante protocollo HTTPS. In particolare, deve essere utilizzato il comando HTTP POST che utilizza come dato di input il valore del TimeStampRequest, conforme alla normativa RFC 3161, in formato DER.



Il servizio di emissioni marche temporali dovrà essere erogato in maniera protetta tramite l'uso di credenziali di identificazione ed autenticazione (basic authentication).

Il servizio di firma dovrà essere dimensionato per gestire fino ad **almeno 10 (dieci) firme digitali** al secondo, garantendo l'alta affidabilità del servizio. Potrà essere in seguito richiesto l'upgrade delle prestazioni del sistema, con incrementi di **ulteriori 1 (una) firma al secondo, fino ad un massimo di 100 (cento) firme al secondo.**

Il Fornitore dovrà attivare i suddetti incrementi in un tempo non superiore a 20 (venti) giorni lavorativi dalla ricezione della richiesta.

Il servizio di erogazione delle marche temporali dovrà essere dimensionato per emettere **almeno 2 marche temporali al secondo**, garantendo l'alta affidabilità del servizio. Potrà essere in seguito richiesto l'upgrade delle prestazioni del sistema, con incrementi di **ulteriori 1 marca al secondo, fino ad un massimo di 10 marche al secondo.**

Il Fornitore dovrà attivare i suddetti incrementi in un tempo non superiore a 20 giorni lavorativi dalla ricezione della richiesta.

4.1.2.2 Servizi di sigillo elettronico

Per soddisfare l'esigenza di poter siglare documenti senza perdita di integrità del documento già sottoscritto, INAIL ha necessità di una soluzione (un **sigillo elettronico**) per l'emissione di sigilli elettronici basata su certificati qualificati eSeal intestati a persona giuridica.

Tale servizio dovrà essere integrato con gli applicativi INAIL abilitati all'apposizione del sigillo su documenti già sottoscritti (es. Protocollo Informatico), in modo tale da visualizzare sul documento le informazioni che accompagnino il sigillo (come, ad esempio, il numero di protocollo), il documento dovrà essere generato predisponendo in anticipo il relativo campo firma che sarà utilizzato per applicare il sigillo stesso.

I servizi di firma con sigillo elettronico dovranno essere utilizzati tramite le integrazioni applicative eseguite da INAIL, adottando le API fornite dal Fornitore che semplificano l'integrazione verso il servizio eSeal erogato da remoto.

4.1.2.3 SPID Professionale e SPID intestato a persona giuridica

Il Fornitore dovrà garantire l'eventuale richiesta da parte di INAIL della fornitura di SPID professionali e SPID intestato a persona giuridica, nelle quantità previste dal Disciplinare di Gara. Entrambe le fattispecie di identità digitale dovranno essere sempre conformi alla normativa vigente in materia.

4.1.3 Applicazione (e/o libreria API) da installare sui device per la firma.

Dovrà essere garantita l'installazione di un'applicazione oppure di un'opportuna libreria API sui device che si adopereranno per la firma.

Tale componente client, comprensiva di licenza d'uso, sarà distribuita senza oneri aggiuntivi secondo quanto la struttura preposta dell'Istituto indicherà e sarà in grado di effettuare sia le operazioni di firma utilizzando il servizio di firma remota sia la verifica in locale dei documenti firmati. È richiesta l'interazione in modalità sicura con la componente server del Fornitore esposta su Internet. Tale componente client deve poter essere configurabile in modo da utilizzare un proxy di tipo HTTP per collegarsi alla componente server tramite collegamento Internet.

La componente client dovrà poter essere installata ed eseguita sui seguenti sistemi operativi, sia a 32 che a 64 bit, e successive evoluzioni:



- Windows 7 e Windows 10;
- Linux;
- Mac OS X.

Se richiesto dall'utente tale componente client dovrà essere in grado di apporre marche temporali, prodotte dall'apposito servizio di emissione come descritto in precedenza, al documento firmato. Dovrà essere disponibile anche un'App da installare sugli smartphone presente nei principali App Store mobili.

4.2 Servizi Connessi

4.2.1 Consegna e installazione

Il Fornitore, entro cinque giorni dalla stipula del Contratto, dovrà coordinarsi con le strutture tecniche dell'Istituto per la pianificazione dell'integrazione della piattaforma con il framework di INAIL, di cui alla precedente sezione 2.3, al fine di garantire la continuità operativa dei servizi una volta effettuata la migrazione dall'attuale Fornitore dei servizi all'aggiudicatario della presente procedura di gara, minimizzando la finestra temporale di eventuali sospensioni.

Qualora l'aggiudicatario della presente procedura di gara dovesse risultare il medesimo operatore economico che attualmente fornisce i servizi all'Istituto, l'erogazione di quanto previsto dal presente Capitolato dovrà avvenire senza soluzione di continuità rispetto a quanto già in corso d'opera.

Entro quindici giorni dalla stipula del Contratto (salvo quanto diversamente stabilito di concerto con la struttura tecnica dell'Istituto che dovrà garantire l'integrazione della piattaforma con il framework INAIL), il Fornitore dovrà garantire il "pronti al collaudo" per la verifica di conformità iniziale di cui al successivo paragrafo 5.

Entro cinque giorni dalla "Data di accettazione del Servizio", il servizio online deve essere messo in esercizio.

In funzione dell'esigenza di raccolta dai referenti interni della gestione della firma digitale in DCOD, dovrà essere attivato il rispettivo lotto di fornitura (certificati, marche, dispositivi) dal referente di INAIL abilitato a formulare richieste di fornitura.

La richiesta viene effettuata e tracciata nel sistema del Fornitore e resa disponibile dal Fornitore con accesso unico del Responsabile INAIL. La richiesta non potrà essere modificata e/o annullata e dovrà essere evasa entro 15 giorni solari da parte del fornitore, pena l'applicazione delle penali di cui al successivo paragrafo 7.

Entro le tempistiche sopra indicate, salvo quanto diversamente stabilito dalle strutture tecniche di INAIL, il Fornitore dovrà effettuare la consegna dei dispositivi fisici richiesti nonché le credenziali di autenticazione al servizio di firma remota, opportunamente protette (es. busta cieca, scratchcard, ecc.), direttamente ai Referenti che verranno indicati dall'Istituto.

I dispositivi fisici dovranno essere immediatamente attivabili non appena avverrà il passaggio dall'attuale Fornitore dei servizi all'aggiudicatario della presente procedura di gara, come stabilito al capoverso precedente.

Contestualmente alla consegna dei dispositivi fisici, il Fornitore garantirà la messa a disposizione dell'Applicazione di cui al precedente sotto paragrafo 4.1.33, nonché fornirà collaborazione con le strutture tecniche dell'Istituto per la relativa installazione sui terminali degli interessati, senza alcun onere aggiuntivo. Dovrà essere garantita, tanto per i dispositivi quanto per l'Applicazione di cui al precedente periodo, tutto il supporto e l'aggiornamento hardware e software per l'intera durata del contratto. Analogamente le App per la connessione dai dispositivi mobili dovranno essere sempre aggiornate e rese disponibili sui marketplace delle varie piattaforme mobili (iOS e



Android). La fornitura dei dispositivi fisici verrà consegnata presso la Direzione Centrale Organizzazione Digitale di INAIL, in Viale Santuario Regina degli Apostoli, 33 ROMA.

4.2.2 Assistenza, Aggiornamento e Manutenzione

Durante l'intera durata di esecuzione del contratto, il Fornitore garantirà l'assistenza progettuale e organizzativa durante le intere fasi, dall'attività iniziale alla conclusione delle attività e quindi alla successiva fase di phase out e di conseguente migrazione al successivo aggiudicatario.

Sarà quindi garantito un team di risorse opportunamente dimensionate in grado di fornire la massima collaborazione alla struttura tecnica dell'Istituto, con particolare riferimento alla fase di inizio e di conclusione del servizio erogato, garantendo se necessario le opportune escalation.

Il Fornitore, durante l'intera esecuzione del Contratto, garantirà il funzionamento e la manutenzione della piattaforma H24 con i livelli di servizio descritti successivamente.

A tal fine sarà resa disponibile un'assistenza dedicata per realizzare un servizio di "help desk": tale servizio dovrà essere garantito tutti i giorni, ventiquattro ore su ventiquattro, senza alcun limite sul numero di contatti. A tal fine, contestualmente alla stipula del Contratto, il Fornitore comunicherà un indirizzo e-mail ed un numero di telefono attraverso i quali verrà garantito tale servizio.

L'organizzazione del suddetto servizio di comunicazione dovrà essere a carico del Fornitore.

Resta inteso che, per tutta la durata contrattuale, il Fornitore dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione, informando tempestivamente INAIL di eventuali modifiche.

Tutte le attività e la documentazione saranno in lingua italiana.

4.2.3 Servizi di Reportistica e accounting

Per l'intera durata contrattuale, il Fornitore consegnerà entro il giorno 10 del mese successivo al trimestre di riferimento, un report trimestrale, secondo un formato concordato con la struttura tecnica dell'Istituto, che conterrà almeno le seguenti informazioni:

- indicazione del tempo di disponibilità del servizio nell'arco del trimestre di riferimento, secondo una finestra temporale di una settimana;
- numero dei dispositivi fisici acquisiti e attivati nell'arco del trimestre di riferimento, suddivisi per tipologia;
- numero dei certificati attivati nell'arco del trimestre di riferimento suddivisi per tipologia;
- numero delle marche temporali emesse nell'arco del trimestre di riferimento;
- numero di firme eseguite nell'arco del trimestre di riferimento, suddivise per tipologia (remota, automatica, temporanea) e con l'indicazione dell'eventuale applicazione del framework INAIL di provenienza;
- indicazione della velocità di esecuzione della firma remota dalla quale si evinca il rispetto o meno del requisito di cui alla precedente sezione 4.1.2.1;
- indicazione della velocità di emissione delle marche temporali dalla quale si evinca il rispetto o meno del requisito di cui alla precedente sezione 4.1.2.1;
- numero di SPID professionali eventualmente attivati.

Eventuale altra reportistica dovrà essere concordata fra le parti e non potrà comportare ulteriori costi aggiuntivi all'Amministrazione. Tale report trimestrale sarà approvato da INAIL entro 10 giorni.

Attraverso un'applicazione web, accessibile in modalità sicura su Internet, il Fornitore dovrà garantire all'Istituto la consultazione delle seguenti informazioni relative ai certificati emessi a favore di ogni Titolare su HSM per la firma remota:



- Cognome
- Nome
- Codice Fiscale
- Data emissione certificato
- Data scadenza certificato
- Eventuale data di consegna del kit (token OTP, ...)
- Tipologia di firma (remota, automatica, temporanea)
- Identificativo del token OTP

Analogamente, dovrà essere garantita la consultazione delle seguenti informazioni relative alle marche temporali erogate, con indicazione del consuntivo mensile delle marche emesse e del residuo delle marche temporali da emettere.

Da tale applicazione web dovrà essere possibile la creazione di un report esportabile in formato compatibile con i fogli di calcolo (es. Microsoft Excel).

Tale servizio dovrà essere attivo per tutta la durata del contratto, ovvero fino al termine dell'ultimo certificato emesso.

4.3 Dispositivi di firma e accesso con CNS (Carta Nazionale dei Servizi)

L'INAIL richiede anche dispositivi di firma che utilizzano la CNS per consentire l'autenticazione sui siti della PA in modalità mobile (tablet, smartphone) oltre che per firmare digitalmente.

Questa tipologia di dispositivi è estremamente versatile in quanto possono essere utilizzati in qualsiasi contesto anche in assenza di rete. Comprende sia l'autenticazione del soggetto che firma ed inoltre per l'Istituto rappresenta una necessità nei contesti ispettivi e legali (avvocatura), in cui potrebbero verificarsi problematiche di connettività di rete che non consentirebbero l'uso della firma remota.

4.4 Assistenza Specialistica

L'assistenza specialistica consiste nella messa in campo di un team di risorse specializzate che possano supportare operativamente l'Amministrazione nell'interfaccia fra la piattaforma che eroga il servizio online e il framework INAIL, coadiuvando e personalizzando i vari blocchi del sistema informativo INAIL che si interfacciano con le risorse tecnologiche dell'aggiudicatario per l'erogazione dei servizi richiesti.

5. VERIFICA DI CONFORMITÀ INIZIALE E ATTIVAZIONE DEL SERVIZIO

Come descritto nel precedente paragrafo 4.2.1, entro quindici giorni dalla stipula del Contratto, salvo quanto diversamente stabilito di concerto con la struttura tecnica dell'Istituto che dovrà garantire l'integrazione della piattaforma con il framework INAIL, il servizio Online sarà sottoposto alla verifica di conformità iniziale, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

Nel caso di ritardo cagionato dall'Aggiudicatario nell'avvio delle predette attività di verifica, saranno applicate le penali di cui al successivo paragrafo 7.

Pertanto, saranno espletate le seguenti attività:

- saranno effettuati gli aggiornamenti della scadenza dei certificati in essere, qualora l'aggiudicatario coincida con il Fornitore uscente;
- verrà fornita tutta la documentazione e i parametri per l'integrazione con il framework INAIL;
- sarà verificato ed adeguato il dialogo con il framework che garantisce la fruibilità dei servizi di firma da parte dell'Istituto;
- sarà verificato il corretto funzionamento dei servizi di portale;



- sarà verificato il sistema di richiesta di fornitura;
- sarà verificato il funzionamento del sistema di firma digitale per ogni tipologia prevista con appositi certificati e dispositivi di test. I certificati digitali di test così come le marche temporali impiegate nei test non eroderanno il massimale previsto dalla gara e non saranno remunerati;
- sarà verificato il funzionamento dell'assistenza tecnica;
- verrà attivata l'eventuale richiesta per l'approvvigionamento dei lotti in funzione dell'esigenza.

Le suddette azioni saranno oggetto della fase di verifica di conformità che, in caso positivo, potranno dare il via alla fase di erogazione del servizio a regime.

Il Fornitore è tenuto a prestare all'Istituto, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione quanto necessario alle operazioni di verifica di conformità e potrà intervenire anche attraverso propri rappresentanti. In tal caso detti rappresentanti sono tenuti a sottoscrivere i documenti di verifica di conformità che verranno redatti dall'Istituto (es. verbali, ecc.).

In caso di esito negativo della verifica di conformità, ferma restando l'applicazione delle penali, di cui al successivo paragrafo 6, il Fornitore dovrà provvedere, a propria cura e spese, entro il termine che le verrà comunicato dall'Istituto, alla eliminazione dei difetti e/o delle carenze riscontrati.

Dopo la comunicazione, da parte del Fornitore, dell'avvenuta eliminazione dei difetti e/o delle carenze, l'Istituto procederà a nuova verifica di conformità nei termini e con le modalità di cui alla presente sezione.

In caso di ulteriore esito negativo della verifica di conformità, l'Istituto avrà facoltà di risolvere il contratto e di fare eseguire tutta o in parte la fornitura a terzi in danno della Società e fatto salvo in ogni caso il diritto al risarcimento di tutti i danni comunque subiti.

A completamento della verifica positiva sarà prodotto il "Verbale di conformità" che dovrà essere sottoscritto dal Responsabile Unico delle Attività Contrattuali, di cui al precedente paragrafo 1.3, e dal referente nominato all'uopo dall'Istituto.

La data del verbale verrà considerata quale "Data di Accettazione del Servizio".

6. LIVELLI DI SERVIZIO

Il tempo di disponibilità del servizio principale, ovvero relativamente al servizio di firma (remota, automatica e temporanea) e al servizio di emissione di marche temporali, dovrà essere maggiore o uguale al 99,85% del periodo temporale di riferimento, pari a quattro mesi (l'indisponibilità massima del servizio è pari quindi a 4 ore in un quadrimestre). Si precisa che tale disponibilità deve essere sempre garantita anche nel caso di aumento delle prestazioni richieste per i servizi di firma e di marca temporale, come descritto nel precedente paragrafo 4.1.2. Nel periodo temporale di riferimento, il tempo massimo tollerato di disservizio per evento è pari a 2 ore, pena l'applicazione della relativa penale.

7. PENALI

INAIL applicherà le penali previste nello schema di contratto.

ID	Riferimento Capitolato Tecnico	Descrizione	Importo Penale applicata
----	-----------------------------------	-------------	--------------------------



SLA01	§ 4.2.1	Tempo di consegna di ciascun lotto di fornitura	1 per mille del valore del corrispettivo contrattuale massimo relativo al singolo lotto di fornitura, per ogni giorno solare di ritardo
SLA02	§ 4.1.2.1	Richiesta di incremento del requisito prestazionale previsto per il servizio di firma e per il servizio di marcatura temporale	1 per mille del valore dell'importo contrattuale complessivo, per ogni giorno lavorativo di ritardo
SLA03	§ 4.1.2.1	Mancato raggiungimento del requisito prestazionale, eventualmente incrementato, in una settimana	1 per mille del valore dell'importo contrattuale complessivo, per ogni giorno lavorativo di ritardo
SLA04	§ 5	Avvio delle attività di verifica di conformità e messa in esercizio del servizio online	1 per mille del valore del corrispettivo contrattuale massimo relativo al Servizio online, per ogni giorno solare di ritardo. Qualora il ritardo nella messa in esercizio sia causato dall'esito negativo della verifica di conformità iniziale, troverà applicazione solamente la penale identificata SLA05.
SLA05	§ 5	Esito negativo della verifica di conformità iniziale	1 per mille del valore del corrispettivo contrattuale massimo relativo al Servizio online, per ogni giorno solare di ritardo intercorrente fra la data di verbale negativo e, a seconda della prestazione oggetto di verifica, la data di accettazione del servizio
SLA06	§ 6	Indisponibilità del servizio in un quadrimestre di riferimento	1 per mille dell'importo contrattuale complessivo per ogni ora di indisponibilità del servizio successiva alle quattro ore
SLA07	§ 4	Ritardi nelle comunicazioni relative ai servizi/infrastrutture cloud	1 per mille per ogni giorno solare di ritardo negli adempimenti previsti al paragrafo 4, rispetto a ciascuna delle tempistiche ivi previste