Allegato Tecnico
Firma Elettronica Avanzata

Sommario

***

1. RIFERIMENTI ESTERNI

Documentazione	Link di dettaglio
CP e CPS (Manuale Operativo) emissione certificati non qualificati per firma elettronica avanzata	ICERT_INDI_FEA.pdf
PDS (PKI Disclosure Statement) emissione certificati non qualificati per firma elettronica avanzata	ICERT-INDI-PDSFEA.pdf

2. DESCRIZIONE DEL SERVIZIO - INTRODUZIONE

Tinexta Infocert opera in qualità di prestatore di servizi fiduciari qualificati e non qualificati. Il Servizio descritto nel presente Allegato Tecnico è un servizio di firma elettronica avanzata con certificato non qualificato (di seguito anche il "**Servizio**"), nel rispetto del Manuale Operativo ICERT-INDI-FEA (d'ora in avanti anche "**CPS**") e del *PKI Disclosure Statement* ICERT-INDI-PDSFEA (d'ora in avanti, "**PDS**"). Per tale Servizio Tinexta 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 del Parlamento Europeo e del Consiglio dell'11 Aprile 2024 (d'ora in avanti, "**Regolamento eIDAS**") e delle norme ETSI EN 319 401, ETSI EN 319 411-1**,** secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319 403 e UNI CEIISO/IEC 17065:2012 (collettivamente, d'ora in avanti, la "**Normativa Applicabile**").

La Firma Elettronica Avanzata (d'ora in avanti anche "**FEA**" o "**Servizio FEA**") è lo strumento che consente di firmare i documenti direttamente da PC o smartphone. È il risultato di una trasformazione crittografica dei dati che fornisce un meccanismo per verificare l'origine, l'integrità dei dati e la non ripudiabilità della firma. Le chiavi crittografiche utilizzate per questa operazione sono conservate su un dispositivo remoto. Le chiavi sono associate ad un soggetto attraverso un certificato digitale non qualificato (d'ora in avanti anche "**Certificato**"), che contiene i suoi dati identificativi.
Le chiavi di crittografia sono generate, conservate e utilizzate attraverso un dispositivo sicuro denominato "Signature Creation Device" (d'ora in avanti anche "**SSCD**").
La coppia di chiavi viene generata su un dispositivo crittografico denominato "HSM" (Hardware Security Model) presso la sede di Tinexta Infocert.
Il tipo di Certificato è contraddistinto da un numero chiamato "O.I.D." (Object Identifier), ossia un codice che identifica il Certificatore Tinexta Infocert, l'uso del Certificato e la "*policy and procedure"* a cui esso è conforme. La definizione e descrizione completa degli O.I.D. si trova nel CPS (Certificate Practice Statement).
Il Certificato emesso viene firmato da una Certification Authority ("**CA**"), nel caso di specie Tinexta Infocert, che ha ottenuto il riconoscimento da parte di Adobe e quindi risulta presente negli store dei certificati attendibili denominato "AATL" (Adobe Approved Trusted List).
Il presente Allegato Tecnico costituisce parte integrante e sostanziale del contratto di acquisto dei servizi (di seguito, l"Accordo"), stipulato con il Cliente.
Ai soggetti che attivano, utilizzano o fanno affidamento sul Servizio si applicano le Condizioni Generali di Attivazione (di seguito, "CGA"), di cui il presente Allegato Tecnico costituisce parte integrante, fermo restando che, nei rapporti con il Cliente, trovano applicazione anche le disposizioni dell'Accordo.

2.1 DEFINIZIONE DELLE PARTI

Soggetto/Titolare: Il Soggetto, definito anche **Titolare**, si riferisce alla persona fisica o giuridica titolare del Certificato non 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 a Tinexta Infocert 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.

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 Rilascio e Utilizzo del Servizio FEA

Il Servizio FEA è erogato da Tinexta Infocert in favore del Soggetto, in forza del presente Allegato Tecnico e dell'Accordo stipulato con lo stesso.
Il Richiedente deve chiedere a Tinexta Infocert la registrazione e l'emissione del Certificato seguendo le modalità stabilite nel Manuale Operativo, utilizzando l'apposita Richiesta di Attivazione fornita da Tinexta Infocert (d'ora in avanti "**Richiesta di Attivazione**").
L'emissione del Certificato da parte di Tinexta Infocert in favore del Soggetto è subordinata all'esito positivo della preventiva e necessaria procedura di identificazione di quest'ultimo, come rappresentata nel par. 3.2.3 del CPS e nel par. 3.1.3 del presente documento.
Pertanto, in caso di esito negativo dell'identificazione, il Certificato non sarà emesso; mentre in caso di esito positivo dell'identificazione, il Certificato viene rilasciato al Soggetto ai sensi del CPS.
Il Certificato rilasciato può essere utilizzato per firmare documenti utilizzando strumenti messi a disposizione da Tinexta Infocert o dal Richiedente non Titolare, per sbloccare le chiavi di firma e, dopo aver svolto un processo di autenticazione tramite strumenti dedicati, la CA conserverà le informazioni relative alla reale identità del Titolare per almeno venti (20) anni dalla scadenza del certificato stesso, fino a un massimo di 23 (ventitré) anni dalla data di emissione.
Nel caso in cui Tinexta Infocert termini la propria attività, provvederà al trasferimento di tali informazioni a terze parti, alle medesime condizioni ivi esposte, così come indicato nel Manuale Operativo.

3.1.2 Certificato digitale

Un Certificato digitale è un documento elettronico, firmato da Tinexta Infocert, che certifica l'associazione tra il Soggetto e la sua coppia di chiavi crittografiche (pubblica e privata).
Le chiavi vengono generate e gestite in un dispositivo crittografico sicuro sotto il controllo di Tinexta Infocert.
Tinexta Infocert garantisce la corretta associazione delle chiavi con il Soggetto, emettendo il Certificato conformemente alla Normativa Applicabile e al Manuale Operativo.

3.1.3 Processo di verifica dell'identità

Sono accettabili esclusivamente i documenti elencati nel "CPS Addendum – Documenti di identità accettabili" presente sul sito Tinexta Infocert al seguente link: CPS-ADDENDUM.
Le modalità di identificazione di seguito elencate sono descritte dettagliatamente nel paragrafo 3.2.3 del CPS:

- LiveID
- AMLID
- SignID
- AutID
- VideoID
- SelfID

Laddove previsto, prima di procedere con il riconoscimento, il Titolare deve assicurarsi di essere in possesso dei documenti di identità in formato originale e del codice fiscale o analogo identificativo univoco.
I documenti devono essere in originale, in buono stato e in corso di validità.

3.1.4 Rinnovo del Certificato

Il Soggetto può rinnovare il Certificato, prima della sua scadenza, utilizzando gli strumenti messi a disposizione da Tinexta 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 e diventa quindi necessaria una nuova identificazione.
In merito alle disposizioni in materia di durata e rinnovo previste dall'Accordo, nel caso in cui il Titolare dia la disdetta anticipata rispetto al rinnovo automatico annuale del suddetto Accordo, la possibilità di utilizzare il Certificato verrà bloccata e, su richiesta del Titolare e/o laddove previsto del Richiedente, 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), ovvero su iniziativa della CA.
Gli ulteriori dettagli in materia sono regolati nel Manuale Operativo.

3.2 SERVIZI

3.2.1 Certificati non qualificati di firma remota avanzata

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

Servizio	OID
Emissione certificato non qualificato per firma remota avanzata	1.3.76.36.1.1.8.3
Emissione certificato non qualificato per firma remota avanzata automatica	1.3.76.36.1.1.8.5

3.2.2. Firma remota

Il Servizio ha ad oggetto la generazione di una coppia di chiavi crittografiche, l'emissione di un Certificato non qualificato di firma elettronica avanzata con durata triennale, fatta salva una diversa durata eventualmente stabilita dalla legislazione vigente, e il servizio di firma.
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 non qualificati per procedure di firma remota avanzata, rilasciati da Tinexta Infocert, sono utilizzati mediante apposite procedure informatiche che si collegano in maniera sicura al servizio di firma erogato da Tinexta Infocert.
Il Servizio prevede che al Titolare sia messa a disposizione una procedura informatica, implementata sui sistemi di Tinexta Infocert o del Richiedente non Titolare, quando presente, mediante la quale il medesimo Titolare può gestire il proprio Certificato.

Le chiavi crittografiche necessarie per la firma sono custodite in un SSCD, gestito da Tinexta Infocert.
Il Titolare mantiene il controllo esclusivo sull'apposizione della firma mediante un processo di autenticazione di livello sostanziale o elevato, che prevede di regola l'utilizzo combinato di PIN e OTP.
Laddove previsto, l'autenticazione può essere delegata al Richiedente.
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 dispositivo mobile.
La firma remota può essere utilizzata tramite applicativi di firma messi a disposizione da Tinexta Infocert, oppure integrati via API (Application Programming Interface) dall'applicazione messa a disposizione dal Richiedente non Titolare.

3.2.3. Firma remota automatica

La firma automatica è una particolare applicazione della firma elettronica, utilizzata in modalità remota.
Il Titolare deve impiegare una coppia di chiavi crittografiche dedicata esclusivamente a tale funzione, distinta da quelle utilizzate per altri scopi, garantendo il rispetto dei requisiti di sicurezza e integrità previsti per le firme avanzate.

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.

3.2.4 Firma remota One Shot

La Firma Elettronica Avanzata One Shot (d'ora in avanti, "**FEA 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.

La FEA OS consente al Titolare, previo riconoscimento della sua identità e di una conferma attraverso codice OTP, di autenticarsi e di utilizzare la FEA OS collegata al Certificato, nel termine di durata di validità dello stesso, pari a 60 minuti o 30/45/60 giorni, ai fini della sottoscrizione dei documenti

informatici. I certificati con durata pari a 60 minuti hanno una validità che è inferiore al tempo massimo per evadere una richiesta di revoca, pertanto per questi certificati non è prevista la possibilità di revoca.
Il rilasciodel Certificato da parte di Tinexta 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 nell'Accordo in materia di recesso, poiché la FEA OS, per sua natura, richiede l'esecuzione immediata, il Titolare, se Consumatore, accetta espressamente la perdita del diritto di recesso ai sensi dell'art. 16, lett. a), della Direttiva 2011/83/UE sui diritti dei consumatori e ss.mm.ii., purché tale disposizione risulti applicabile al contesto specifico.
Qualora il Certificato abbia la durata di 60 minuti, in deroga a quanto previsto dal paragrafo 3.1.5 del presente documento, essendo la durata del Certificato minore o uguale al 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 FEA OS 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 presente, del Richiedente non Titolare sono determinati dalla Normativa Applicabile, dal presente Allegato Tecnico, dal Manuale Operativo pertinente e dall'Accordo 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 a Tinexta Infocert e/o a terzi dall'inesattezza delle informazioni contenute nel Certificato.
Il Richiedente non Titolare e/o il Soggetto sono tenuti a garantire e manlevare Tinexta Infocert da eventuali richieste di risarcimento danni. Il Richiedente non Titolare e/o il Soggetto sono anche responsabili per i danni derivanti a Tinexta Infocert e/o a terzi in caso di ritardo nell'attivazione delle procedure di revoca o sospensione del Certificato, come previsto dal Manuale Operativo. Inoltre, 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 di Tinexta 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, e conservandoli in un luogo sicuro.
Il Titolare, consapevole che l'utilizzo di un Certificato è riconducibile unicamente alla sua persona, è obbligato ad osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione messi a disposizione da Tinexta Infocert 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 sostanziale o elevato di sicurezza come previsto dal Regolamento di Esecuzione (UE) 2015/1502 e ss.mm.ii. e secondo le modalità concordate con Tinexta Infocert.
È inoltre tenuto a impedire l'uso del Certificato dopo la sua scadenza, revoca o sospensione e a manlevare Tinexta Infocert da ogni responsabilità per l'uso improprio del Certificato.

3.3.4 Obblighi di Tinexta Infocert

Gli obblighi di Tinexta Infocert sono esclusivamente quelli indicati dalla Normativa Applicabile, dal presente Allegato Tecnico, dal Manuale Operativo e dall'Accordo.
In particolare, Tinexta Infocert si obbliga a conservare in un apposito archivio digitale non modificabile per 20 (venti) anni tutti i certificati emessi, i *log* di attivazione degli stessi e le evidenze di riconoscimento, nelle modalità previste dal Manuale Operativo.
In particolare, Tinexta Infocert 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 e del Certificato, rispetto a quelli previsti dalle norme italiane vigenti e dal Manuale Operativo;
- 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).

Tinexta Infocert garantisce unicamente il funzionamento del Servizio, secondo i livelli di servizio indicati al Titolare nel Manuale Operativo.

3.3.5 Ruolo e Organizzazione

Conformemente al Manuale Operativo e alle normative vigenti, 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, in qualità di Terzo Interessato, comunicare a Tinexta 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.

4. SLA

4.1 SLA di servizio

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