Manuale Operativo

Telepass S.p.A.

10 ottobre 2024

SOMMARIO

1. RIFERIMENTI

1.1 Versione

Versione	Autore	Descrizione	Data

1.2 Lista di distribuzione

Numero copie	Società	Persona

1.3 Documenti allegati

Numero copie	Titolo documento
1	Modulo di revoca

2. INTRODUZIONE

Il presente documento è stato realizzato da Telepass S.p.A. in quanto erogatore di servizi di sottoscrizione di documento con Firma Elettronica Avanzata (FEA) integrata con certificati FEA emessi da Intesi Group con verifica via One Time Password (OTP).

La tipologia dei documenti che possono prevedere la sottoscrizione del richiedente (**utente**) che si presenti, anche in forma telematica (via app o web) può essere ampio, e l'elenco completo dei documenti sottoscrivibili elettronicamente verrà comunicato direttamente dall'Operatore delle società che utilizzano il servizio di FEA.

Telepass S.p.A. provvederà a pubblicare il presente Manuale Operativo e lo manterrà aggiornato per recepire eventuali variazioni sui processi. Provvederà inoltre annualmente alla verifica della conformità della propria soluzione di Firma Elettronica Avanzata e, ove si renderà necessario, aggiornerà questo documento, anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

2 DEFINIZIONI

2.1 Definizioni riguardanti i soggetti

Soggetto	Illustrazione
Soggetti che erogano servizi di Firma Elettronica Avanzata (Telepass S.p.A. che propone la FEA come art. 55 comma 2 lettera “a”. di seguito 55.2.a)	Soggetti giuridici che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti che le realizzano come attività di impresa.
Soggetti realizzatori dei servizi di firma elettronica avanzata (Intesi Group come art. 55 comma 2 lettera “b” di seguito 55.2.b)	Soggetti giuridici che, quale oggetto dell’attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore di Soggetti erogatori.
Operatore	Addetto che si avvale dei servizi FEA, che si occupa di assistere il richiedente durante l'operazione di Firma Elettronica avanzata.
Richiedente	Soggetto che si rivolge a Telepass, per usufruire di uno dei servizi offerti. Può essere: utente/cliente persona fisica utente/cliente persona giuridica

2.2 Definizioni riguardanti gli acronimi e i termini utilizzati

Sigle	Illustrazione
AgID	Agenzia per l’Italia Digitale (come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22) ha sostituito CNIPA e DigitPa

CA FEA	**Certification Authority**, ente preposto alla generazione di certificati FEA per la realizzazione di Firme Elettroniche Avanzate
Certificato di firma elettronica	Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona
Certificato qualificato di firma elettronica	Certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS
Chiave privata	È la chiave di crittografia utilizzata in un sistema di crittografia asimmetrica al fine di proteggere la firma apposta. La chiave privata è associata a una chiave pubblica ed è in possesso del Titolare che la utilizza per firmare digitalmente i propri documenti.
Chiave pubblica	È la chiave crittografica in un sistema di crittografia asimmetrica ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica. Tale chiave è associata ad una chiave Privata.
Copia Informatica di documento informatico	Documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;
Documento analogico	Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva

Documento Informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato Informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
FE	Firma Elettronica
FEA	Firma Elettronica Avanzata, ovvero firma elettronica connessa unicamente al firmatario e idonea a identificarlo, ottenuta mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo e collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica dei dati medesimi
FEQ	Firma Elettronica Qualificata, ovvero firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche
FES	Firma Elettronica Semplice, ovvero dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
Firma digitale	Particolare tipo di firma qualificata basata 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
Hash	Funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
HSM	**Hardware Security Module,** è un server sul quale vengono realizzate operazioni per mezzo di chiavi digitali in modalità sicura, protetta e remota
LRA	Local Registration Authority
IUO	Identificativo Univoco Operatore. È il codice che il software interno stampa sul modello di documento richiamato a sistema in seguito alla compilazione in sostituzione della firma analogica dell'operatore. È associato automaticamente al login dell'operatore.
Marca Temporale	Riferimento temporale che consente la validazione temporale (data certa) e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
OTP	**One Time Password,** è un codice di sicurezza richiesto per la disposizione della sottoscrizione, monouso, solitamente pervenuto via SMS o su apposita app mobile o via mail o su token fisico, direttamente al possessore del certificato di firma su HSM. Numero di cellulare, e-mail, app mobile o token fisico saranno prima stati certificati dall'azienda emittente

PAdES	Formato di busta crittografica definito nella specifica tecnica ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche
CAdES	Formato di busta crittografica definito nella specifica tecnica ETSI TS 101 733 e successive modifiche
XAdES	Formato di busta crittografica definito nella specifica tecnica ETSI TS 101 903 e successive modifiche
PDF	Standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization)
RAO	Registration Authority Officer
RSA	Algoritmo di crittografia asimmetrica che si basa su utilizzo di chiave pubblica e privata
Soluzione di Firma Elettronica Avanzata	Soluzioni strumentali alla generazione e alla verifica della firma elettronica avanzata

3 RIFERIMENTI NORMATIVI

Riferimenti	Descrizione
D. Lgs. n. 196/2003 – Codice Privacy	Decreto legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali
D. Lgs. n. 82/2005 – CAD	Decreto legislativo 07 marzo 2005 n. 82, Codice dell'Amministrazione digitale
Regole Tecniche DPCM 22.02.2013	Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 "Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lett. b), 35, comma 2, 36, comma 2, 3 e 71.
Reg. UE n. 910/2014 - eIDAS	Regolamento UE n. 910/2014 sull'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
Reg. UE n. 2016/679 - GDPR	Regolamento UE n. 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
D. Lgs. n. 101/2018	Decreto legislativo di adeguamento della normativa nazionale alle disposizioni del regolamento UE 679/2016

Con il Decreto Legislativo del 10 agosto 2018, n. 101 è stata adeguata la normativa nazionale in materia di protezione dei dati personali alla normativa europea (Regolamento UE 2016/679). A seguito dell'entrata in vigore del citato decreto (19.09.2018), sono stati abrogati numerosi articoli del Decreto Legislativo n. 196/2003-Tuttavia, fino a quando il Garante non adotterà le

citate misure, continueranno ad applicarsi le (precedenti) disposizioni del D. Lgs. n. 196/2003, in quanto compatibili con il Regolamento UE 2016/679.

Alla data odierna, l'Azienda che utilizza processi FEA, deve predisporre alcuni documenti per soddisfare i requisiti espressi nell'Articolo 57 del DPCM del 22/02/2013 in vigore dal 05/06/2013. Il DPCM è reperibile qui:

http://www.gazzettaufficiale.it/eli/id/2013/05/21/13A04284/sg

Questi sono:

1. la predisposizione **dell'Informativa sull'uso degli strumenti FEA** da parte dell'azienda verso i terzi firmatari e sul trattamento dei dati personali ex art. 13 Reg. UE 679/2016 e del relativo **Modulo di accettazione delle condizioni di servizio** (v. art. 57, c.1 lett. a DPCM)
2. eventuale **Modulo di richiesta di copia della documentazione di accettazione FEA** (v. art. 57, c. 1 lett.c DPCM), nel caso l'Azienda preveda l'utilizzo di un modulo ad hoc per questa attività
3. la predisposizione di un **modulo di recesso dal servizio**
4. la **pubblicazione** degli stessi eventualmente sotto forma di Manuale operativo, **sul sito internet** assieme ai dati dell'**assicurazione professionale a copertura dei rischi derivanti** ed alle **caratteristiche tecniche impiegate per rispondere alle Regole Tecniche sulla FEA**

4 GLI ATTORI

4.1 Soggetto che eroga la soluzione di FEA

Telepass S.p.A., come da articolo 55 comma 2 lettera a) del Decreto del Presidente del Consiglio dei Ministri datato 22 febbraio 2013, si identifica come Soggetto che eroga la soluzione di Firma Elettronica Avanzata al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi (clienti) per motivi societari.

4.1.1 Dati identificativi

Ragione Sociale	Telepass S.p.A.
Indirizzo sede	via Laurentina 449 - 00142 – Roma
Partita Iva	09771701001
Registro Imprese	C.F. e n. di Iscriz. al Reg. delle Imprese di Roma: 09771701001
Indirizzo E-Mail	telepass@pec.telepass.it
Numero Telefonico	+39 06 8716 8800
Indirizzo Sito Istituzionale	www.telepass.com

4.2 Soggetto che realizza la soluzione di FEA

In aderenza a quanto espresso nell'art 55 comma2 lettera b) del DCPM 22 febbraio 2013, si segnala che la soluzione di Firma Elettronica Avanzata utilizzata è stata realizzata da Intesi Group Spa.

4.3 Altri soggetti coinvolti

4.3.1 Selecta Digital Services

Società di consulenza in ambito Information Technology che ha redatto l'Informativa FEA, il modulo di accettazione delle condizioni FEA e del consenso al trattamento, il modulo di recesso dal servizio di FEA, il Manuale Operativo FEA e la Valutazione d'Impatto ex art. 35 Reg. UE 679/2016.

4.3.2 Selecta Digital Services

Società che, per conto del Cliente, realizza la conservazione digitale dei documenti informatici sottoscritti con soluzione di FEA.

5 LA FIRMA FEA

La Firma Elettronica Avanzata è una modalità di firma elettronica che possiede i requisiti tecnici e giuridici richiesti dalla normativa.

I requisiti tecnici sono previsti dagli artt.3, comma 1, n. 11) e 26 del Regolamento eIDAS e dall'art. 56 delle Regole Tecniche e sono i seguenti:

1) Identificazione del firmatario del documento;
2) Connessione univoca della firma al firmatario;
3) Controllo esclusivo del firmatario del sistema di generazione della firma;
4) Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5) Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6) Individuazione del Soggetto che eroga la soluzione di firma elettronica avanzata di cui all'articolo 55, comma 2, lettera (a) delle Regole Tecniche (DPCM 22.02.2013);
7) Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati;
8) Connessione univoca della firma al documento sottoscritto;

Il processo di Firma Elettronica Avanzata, così come realizzato da Telepass S.p.A., sul piano tecnico, permette all'utente di firmare i documenti informatici che soddisfino i requisiti previsti dalla normativa in essere.

A tale fine, Telepass S.p.A. per rispondere positivamente a quanto richiesto dalle normative vigenti in materia, ha adottato le seguenti misure:

Requisito	Caratteristica della soluzione
1) l'identificazione del firmatario del documento	Questo compito resta in carico al personale dell'ente erogatore del servizio, incaricato all'identificazione del soggetto ed alla certificazione dei suoi dati anagrafici e del documento di identità raccolto e conservato. La prima identificazione con la presentazione del consenso al servizio FEA si completa con l'acquisizione delle informazioni necessarie anche per l'emissione del certificato FEA associato all'utente. Questa associazione è eseguita con invio a Intesi Group dei dati di registrazione dell'utente con i dati personali e anagrafici, della copia del documento di riconoscimento, codice fiscale e indirizzo telefonico su cui far pervenire in Codice OTP di sblocco certificato. L'uso del certificato prevede la specificazione di un codice OTP fatto pervenire dal sistema. Le modalità di generazione e invio dipendono dalla soluzione scelta e in particolare: a) OTP SMS sul numero di cellulare certificato del soggetto; b) utilizzo della APP Valid ove il codice viene generato dalla APP medesima (l'OTP in questo caso è time based e viene

	generato attraverso un processo crittografico; c) OTP e-mail all'indirizzo certificato del soggetto. Il cellulare e/o l'indirizzo e-mail si assumono in uso esclusivo dell'utilizzatore per quel che riguarda l'apposizione delle firme elettroniche.
2) la connessione univoca della firma al firmatario	La firma elettronica sul documento avviene tramite certificato di firma con coppia di chiavi RSA pubblica e privata, emesso su richiesta dell'utente del servizio di Firma Elettronica. Il certificato elettronico sarà emesso su C.A. FEA di Intesi Group (o eventualmente di CA del Cliente e gestita da Intesi Group) e riportante i dati del soggetto quali Nome e Cognome, Codice Fiscale, e-mail e/o delegatario della firma, già memorizzati e certificati nel portale del servizio di firma elettronica. Nel certificato sarà ben evidente anche la ragione sociale del proponente il sistema di FEA. La firma Elettronica viene apposta sul documento per mezzo di algoritmi di criptazione su sistemi sicuri ed HSM del servizio di firma Elettronica, messi a disposizione dalla società Intesi Group, solo a seguito dell'inserimento di un codice OTP generato dai sistemi di firma ed inviato tramite un servizio di invio SMS al numero di cellulare certificato del soggetto, che si ritiene in suo uso esclusivo all'atto della firma. Il mittente specificato negli SMS avrà come alias una stringa alfanumerica identificativa del servizio o dell'azienda proponente del servizio di FEA, scelta da quest'ultima. Gli stessi meccanismi di sicurezza vengono adottati in caso di invio OTP tramite e-mail.

3) il controllo esclusivo del firmatario del sistema di generazione della firma	Il codice OTP che permette la generazione del certificato FEA è inviato direttamente al telefono dell'utente (fatto salvo il caso di utilizzo dell'APP Valid ove il codice OTP è generato automaticamente dalla APP che richiede il login a Time4Mind), numero segnalato dal cliente e verificato in fase di accettazione del servizio. Pertanto, il controllo di generazione del certificato è in capo al firmatario. In ogni caso, Intesi Group mantiene una sessione esclusiva delle operazioni che avvengono da parte del soggetto firmatario sulle pagine web del browser aperto sul device dell'utente e ne mantiene le tracce di connessione da associare alla transazione. La firma elettronica sul documento avviene su dispositivi sicuri ed HSM che in quel momento e con quella sessione, operano mantenendone traccia, con sessione appositamente aperta a quell'utente e su sua richiesta. Gli stessi meccanismi di sicurezza vengono adottati in caso di invio OTP tramite e-mail.
4) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma	Essendo i documenti sottoscritti in modalità PAdES (o CAdES o XAdES) con il certificato elettronico, ad ogni possibile modifica del documento in istanti successivi a quello dell'apposizione della firma stessa, ve ne resta traccia nel file ed evidenziata da un qualunque tool di visualizzazione del file in grado di interpretare le firme. Nel caso per esempio di firme PAdES può essere usato ad esempio il programma concesso in uso gratuito Adobe Reader della società Adobe.
5) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	Telepass S.p.A. fornisce sempre il documento completo tramite le proprie interfacce ed il documento completo di

	firma elettroniche dell'utente sarà inviato al cliente via mail al termine del processo di vendita andato a buon fine.
6) l'individuazione del soggetto di cui all'articolo 55, comma 2, lettera a)	L'azienda proponente apporrà sui documenti loghi e scritte identificative. Il programma può visualizzare il logo aziendale durante il processo di raccolta ed anche in appositi spazi delle pagine Web, la denominazione dell'azienda o della sua compagnia, e dell'incaricato dell'azienda che ha sottoposto il documento alla firma del soggetto firmatario. L'impiego di firme digitali qualificate di chiusura del documento, con certificato intestato a personale dell'azienda, potrà far valere anche la paternità.
7) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati	L'azienda proponente produrrà documenti firmati privi di elementi quali ad esempio script, in grado di modificare quanto scritto nel documento stesso senza invalidarne la firma. Al termine dell'elaborazione Telepass S.p.A. produce un nuovo file in formato PDF o P7M o XML, contenente le firme elettroniche raccolte in formato PAdES, CAdES o XAdES.
8) la connessione univoca della firma al documento sottoscritto	La soluzione adottata da Intesi Group impiega sistemi sicuri di apposizione della firma su server remoti HSM certificati QSCD, che creano la firma criptando l'hash del documento ed inserendo il risultato nel documento stesso in formato PAdES o CAdES o XAdES. La verifica di collegamento della firma al file potrà avvenire con un qualunque tool di verifica in grado di interpretare le firme PAdES o XAdES o CAdES. Per le firme PDF si può utilizzare ad esempio il programma concesso in uso gratuito Adobe Reader della società Adobe.

Tutto ciò nel rispetto dei requisiti richiesti nell'articolo 56 delle Regole Tecniche (DPCM 22/02/2013).

6 VALORE GIURIDICO DELLA FEA

La soluzione proposta da Telepass S.p.A. per la sottoscrizione elettronica dei documenti soddisfa i requisiti richiesti dalla normativa FEA, con le conseguenze che ne derivano in tema di forma del documento sottoscritto e sua efficacia, nonché di limiti d'uso.

6.1 Forma

Il documento sottoscritto con soluzioni di FEA soddisfa il requisito della forma scritta, così come stabilito dall'art. 20, comma 1 bis CAD.

6.2 Efficacia probatoria

Il documento sottoscritto con soluzioni di FEA ha la stessa efficacia probatoria delle scritture private riconosciute, ovvero fa piena prova fino a querela di falso della provenienza delle dichiarazioni dal firmatario, così come stabilito dall'art. 20, comma 1 bis CAD e dall'art. 2702 c.c.

6.2.1 Limiti d'uso

In generale, la soluzione di FEA può essere utilizzata per sottoscrivere qualsiasi documento, ad eccezione di:

- contratti previsti dall'art. 1350, comma 1 nn. da 1 a 12 c.c., salvo che la firma venga autenticata;
- atti pubblici.

La FEA non consente il libero scambio di documenti informatici: il suo uso è limitato al contesto.

Infatti, tale sistema di firma ha valenza esclusivamente *inter-partes*, ovvero tra il firmatario e chi eroga la soluzione di FEA, ed è utilizzata nel processo di dematerializzazione per motivi istituzionali, societari o commerciali, così come disposto dall'art. 60 DPCM 22 febbraio 2013.

Nel rispetto della citata normativa, Telepass S.p.A. ha deciso di proporre la soluzione di FEA ai propri utenti/clienti diretti persone fisiche, utenti/clienti persone giuridiche e nuovi utenti/clienti per la sottoscrizione di contratti.

7 ADEMPIMENTI PER IL RISPETTO DELLE NORME SULLA FEA

I soggetti che erogano soluzioni FEA (Telepass S.p.A.) hanno una serie di obblighi da rispettare, al fine di garantire il rispetto di tutti i requisiti richiesti dalla normativa in vigore.

In particolare, devono (art 57 DPCM 22.02.2013):

1) Identificare in modo certo il richiedente tramite un valido documento di riconoscimento;
2) Informare il richiedente in relazione agli esatti termini e condizioni d'uso del servizio, compresa ogni eventuale limitazione d'uso (Informativa FEA– All. 1);
3) Subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte del richiedente (Accettazione FEA – All. 1);
4) Conservare per almeno 20 anni copia del documento di riconoscimento, la dichiarazione del punto 3 e le informazioni di cui al punto 2, garantendone la disponibilità, integrità, leggibilità e autenticità;
5) Fornire liberamente e gratuitamente copia dei documenti di cui ai punti 2 e 3 al firmatario, su sua richiesta. La richiesta della copia dei documenti potrà essere inviata all'indirizzo mail: richiestadoctelepass@datlasgroup.com;
6) Rendere note le modalità con cui effettuare la richiesta di cui al punto 5;
7) Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dalle Regole Tecniche articolo 56, comma 1;
8) Specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;
9) Prevedere la possibilità di revoca del servizio da parte del richiedente (Revoca FEA – All. 3), rendendo note le modalità con cui effettuare tale richiesta, pubblicandole anche sul proprio sito internet;
10) Dotarsi di copertura assicurativa per la responsabilità civile, rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali.

Nei paragrafi successivi verranno analizzati i singoli obblighi.

7.1 Identificazione del firmatario

In un processo FEA l'identificazione riveste un momento fondamentale. Questo perché esistono solitamente due differenti tipologie di identificazione: la prima che si effettua con la prima identificazione e prevede anche la raccolta di specifica documentazione (paragrafo 8.1.1); la seconda è un'identificazione successiva, quando il firmatario, che ha già accettato il servizio FEA, si ripresenta per sottoscrivere ulteriori documenti (paragrafo 8.1.2). Con la tipologia di FEA illustrata in questo documento, si considera una terza tipologia di identificazione, effettuata ai fini della registrazione dei dati dell'utente per l'emissione del Certificato FEA (paragrafo 8.1.3). Le modalità di identificazione del firmatario sono invece riportare nel paragrafo 8.2.

7.1.1 Prima identificazione

L'identificazione del firmatario viene effettuata dagli operatori preposti e proponenti i documenti da sottoporre alla FEA secondo diverse modalità, che prevedono la richiesta di un documento di riconoscimento, che deve essere in corso di validità.

Telepass S.p.A. ha deciso di considerare validi solo alcuni dei documenti di riconoscimenti previsti dall'articolo 35 del DPR 445/2000, e in particolare:

- Carta d'identità
- Passaporto
- Patente

In questa fase, se si desidera attiva, per le successive identificazioni processi digitali sicuri, si può procedere con la richiesta di ulteriori informazioni, finalizzate all'identificazione remota quali, ad esempio:

- Numero di telefono mobile
- Indirizzo e-mail

La copia del documento, in prima identificazione, viene conservata con la relativa informativa del servizio e il modulo di accettazione debitamente sottoscritto. Il tutto sarà conservato per 20 anni.

7.1.2 Identificazioni successive

Non previste dal processo operativo Telepass.

7.1.3 Identificazione per Registrazione

L'identificazione del firmatario, per la registrazione dei dati al fine del rilascio di un Certificato FEA, prevede l'acquisizione di ulteriori informazioni obbligatorie:

- Nome e cognome;
- Data di Nascita, Citta e Nazione di nascita;
- Nazione di residenza;
- Numero di telefono mobile;
- Indirizzo email;
- Dati del documento di identificazione (numero del documento, data e ente di emissione).

Se il richiedente rappresenta una persona giuridica si deve anche fornire:

- Nome dell'organizzazione;
- Codice fiscale dell'organizzazione;
- Indirizzo dell'organizzazione (nazione, città, indirizzo);
- Numero di telefono e indirizzo e-mail dell'organizzazione;
- Attestazione o evidenza che dimostri l'autorizzazione ad agire per conto della persona giuridica.

Queste informazioni possono essere raccolte direttamente utilizzando gli strumenti e servizi messi a disposizione da Intesi Group, ovvero direttamente da Telepass S.p.A. e poi comunicate a Intesi Group a mezzo di canali concordati.

7.2 Modalità di identificazione

In pieno rispetto di quanto previsto nell'articolo 56 comma 1 del DPCM 22 febbraio 2013, al fine di darne evidenza, si acquisisce copia del documento di riconoscimento. Poiché la soluzione scelta è di operare con modalità digitale, la copia del documento verrà acquisita mediante scansione.

Telepass S.p.A. ha scelto come modalità di riconoscimento e identificazione sicura dell'utente a cui viene rilasciato un certificato di FEA:

1. Modalità riconoscimento De visu;
2. Processo di riconoscimento a cura del cliente

Di seguito si illustrano le modalità consigliate da Intesi Group.

7.2.1 Modalità De visu

L'operatore raccoglie tramite app la documentazione identificativa dell'utente (scansione dei documenti previsti: carta d'identità e codice fiscale per i cittadini italiani, passaporto per altri), ottiene i consensi necessari e li inserisce nell'app che raccoglie i dati che vengono utilizzati per compilare il contratto che verrà firmato, con un proprio certificato, a conferma della validità della operazione dei dati forniti, per la conservazione per i tempi previsti.

7.3 Informazione del richiedente firmatario

Identificato il cliente, gli operatori, prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, procedono a informare il richiedente firmatario sulle condizioni di uso del servizio, ivi comprese le limitazioni d'uso, presentandogli anche l'apposita Informativa, che verrà mostrata insieme al contrato da firmare e allegata al contratto sottoscritto una volta terminato il processo.

7.4 Dichiarazione di accettazione del servizio dal firmatario

Gli operatori, dopo aver adeguatamente informato il richiedente, sottopongono a quest'ultimo la sottoscrizione della dichiarazione di accettazione delle condizioni di erogazione del servizio. Tale documento, riportato in allegato 1, riporta tutti i dati informativi del cliente, la descrizione del servizio e richiede una firma mediante soluzione di FEA con effetto immediato.

7.5 Allegazione e conservazione della documentazione

In pieno rispetto di quanto previsto nell'articolo 56 comma 1 del DPCM 22/02/2013, al fine di darne evidenza, tuttia la documentazione raccolta per l'attivazione del servizio FEA viene conservata per un periodo minimo di 20 anni.

7.6 Caratteristiche del sistema di firma

Al fine di ottemperare alla normativa di cui articolo 56 comma 1 nel paragrafo 11, si descrivono le misure adottate a garanzia di quanto prescritto da parte di Intesi Group.

7.7 La tecnologia utilizzata

Nei paragrafi 12 e 13 si descrivono le caratteristiche hardware e software della soluzione di Intesi Group utilizzate al fine di ottemperare quanto richiesto dalle Regole Tecniche DPCM 22 febbraio 2013.

7.8 Aggiornamento del sito internet

Telepass S.p.A., in ottemperanza a quanto richiesto dalla normativa in essere, pubblica sul seguente link info-telepass.selecta.it il presente documento.

Il documento descrive anche le caratteristiche del sistema di firma e le caratteristiche delle tecnologie utilizzate.

7.9 Revoca del servizio

Il processo di FEA predisposto prevede che il consenso alla sottoscrizione in forma elettronica rilasciato dal firmatario si estenda a tutte le operazioni che:

- Siano effettuate da cliente o delegato che abbiano aderito al servizio;
- Comportino l'uso di un documento sottoscrivibile elettronicamente;

Pertanto, si prevede la possibilità di revoca di detto consenso attraverso la sottoscrizione di apposito modulo. L'aderente al servizio viene messo a conoscenza del suo diritto al momento della presa visione dell'Informativa.

Dal punto di vista operativo, il cliente può esercitare la revoca mediante la presentazione della stessa direttamente all'operatore, con il seguente processo:

a. Farsi identificare dall'Operatore, mediante esibizione di un documento di riconoscimento compreso nell'elenco di cui al precedente capitolo 7.1;
b. Compilare il modulo "Revoca del Servizio FEA", pubblicato sul link info-telepass.selecta.it
c. Consegnare il modulo firmato.

7.10 Tutela assicurativa

Le Regole Tecniche, di cui al DPCM 22 febbraio 2013, prevedono inoltre una copertura assicurativa a garanzia del firmatario.

In particolare, nelle Regole Tecniche art. 57 comma 2, si cita che: "Il soggetto che eroga soluzioni di Firma Elettronica Avanzata si impegna a stipulare una polizza assicurativa, con società abilitata ad esercitare nel campo dei rischi industriali, per la copertura dei rischi dell'attività svolta e dei danni a tutela delle parti (Firmatari ed i Terzi) per almeno Euro 500.000,00".

8 ADEMPIMENTI PER IL RISPETTO DELLE NORME SULLA PRIVACY

8.1 Informazione dell'utente firmatario

Telepass S.p.A., in qualità di Titolare del trattamento, deve informare l'utente firmatario, prima di attivare il servizio, circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la base giuridica del trattamento;
c) se la base giuridica del trattamento è il consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione dei dati;
e) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
f) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
g) l'esistenza dei diritti dell'interessato di chiedere al titolare l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al trattamento, oltre al diritto alla portabilità;
h) il diritto di proporre reclamo ad un'autorità di controllo;
i) gli estremi identificativi del titolare e, se designato, del rappresentante nel territorio dello Stato;
j) i dati di contatto del Responsabile della protezione dei dati.

A tal fine Telepass S.p.A. ha redatto un'apposita Informativa che, unitamente alle condizioni generali del servizio FEA, rende edotto l'utente di tutto quanto richiesto dalla citata normativa.

L'Informativa:

- È disponibile sul sito internet info-telepass.selecta.it

8.2 Diritti relativi ai dati personali e modalità di esercizio

Telepass S.p.A., in qualità di Titolare del trattamento, garantisce agli interessati (utenti firmatari) i diritti previsti dagli artt. 15 ss Regolamento UE 2016/679, in quanto applicabili.

Si tratta in particolare dei diritti di:

- **Accedere ai propri dati personali** e conoscerne l'origine, le finalità e gli scopi del trattamento, il periodo di conservazione, i dati del titolare del trattamento, del responsabile del trattamento e i soggetti a cui potranno essere divulgati.
- **Aggiornare, rettificare e integrare** i propri dati, in modo che siano sempre accurati.
- **Cancellare** i propri dati personali, qualora non siano più necessari per il perseguimento delle finalità indicate nell'informativa.
- **Limitare il trattamento** dei propri dati personali in talune circostanze, ad esempio laddove sia stata contestata l'esattezza, per il periodo necessario al Titolare per verificarne l'accuratezza.
- **Revocare il consenso** in qualunque momento, con la consapevolezza che la revoca non pregiudica la liceità del trattamento basato sul consenso prima della revoca stessa.

A tal fine Telepass S.p.A. si è dotata di un'apposita procedura "diritti dell'interessato" che permette l'evasione della richiesta nei tempi stabiliti dalla normativa, ovvero 30 giorni dal ricevimento della richiesta.

Per esercitare uno dei citati diritti, l'interessato deve presentare domanda all'indirizzo e-mail dpo@datlasgroup.com.

9 LA SOLUZIONE INTESI GROUP

Nel presente capitolo si descrivono le caratteristiche della soluzione fornita a Telepass S.p.A. da Intesi Group. Tale soluzione è composta dai seguenti moduli software:

- PkBox server sui server di Intesi Group e PkBox Remote sulla applicazione del CLIENTE
- App Valid per la generazione delle chiavi OTP

In particolare, i modulo Valid permettono al cliente/utente finale, previo conferimento dei propri dati personali, di:

- Accedere all'APP mobile VALID per la gestione delle proprie credenziali di sicurezza: inserimento e modifica del PIN di sblocco della visualizzazione del codice OTP. Questa operazione è consentita solo in fase di emissione delle credenziali;
- Accedere alla piattaforma PkBox per la modifica della password di accesso per le operazioni di firma;
- Solo per gli utenti che hanno preventivamente attivato il modulo "Valid", di generare i codici OTP per poter firmare i documenti che il proponente intende proporre in sottoscrizione.

Trattandosi, in tutti i casi, di funzionalità che comportano il trattamento di dati personali dell'utente, Intesi Group, in qualità di ideatore, sviluppatore e realizzatore dell'intera soluzione FEA, mette a disposizione delle società clienti specifici modelli di informativa relativi al trattamento di tali dati, redatti in conformità all'art. 13 Regolamento UE 679/2016. Si precisa che si tratta esclusivamente di modelli di supporto, rimanendo onere del Titolare la verifica della correttezza ed esaustività delle informazioni ivi inserite, oltre al completamento delle informazioni mancanti.

Per quanto concerne, poi, il modulo Valid, proponendo un servizio di sottoscrizione mediante FEA con OTP, la società che fruisce del servizio di FEA di Intesi Group (in qualità di soggetto che eroga la soluzione di firma), deve altresì:

- Informare il richiedente in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione d'uso (art. 57, comma 1, lett. a D.P.C.M. 22 febbraio 2013);

- Subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente (art. 57, comma 1, lett. a D.P.C.M. 22 febbraio 2013);
- Assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata (art. 57, comma 1, lett. h D.P.C.M. 22 febbraio 2013);

Anche in tal caso, Intesi Group mette a disposizione del proponente la modulistica di base richiesta dal citato Decreto, ferma restando l'esclusiva responsabilità in capo a quest'ultimo di verifica di adeguatezza e completezza delle informazioni contenute, rispetto alle peculiarità del servizio offerto.

In ogni caso, anche in vista di eventuali modifiche del testo proposto, si evidenziano in grassetto e corsivo le parti che, riferendosi al processo realizzato, devono in ogni caso essere presenti nel testo dei moduli che saranno adottati e resi pubblici, affinché sia conforme al dettato normativo relativo alla FEA.

NOTA

Le istruzioni di seguito riportate rappresentano una proposta di massima che Intesi Group fa ai propri prospect e clienti per agevolare l'attivazione di Valid ed il proprio processo FEA in cui verrà utilizzato.

Intesi Group non è comunque responsabile di eventuali applicazioni non corrette della normativa vigente e dei documenti che l'Azienda creerà per sé stessa.

9.1 Elaborazione della richiesta

Identificazione del richiedente.

- L'utente è identificato al momento di adesione al servizio Valid propedeutico e necessario alla sottoscrizione con FEA con OTP dei documenti, Ogni comunicazione avverrà tramite i mezzi di comunicazione (e-mail e numero di

telefono) indicati al momento di adesione al servizio e certificati dal personale espressamente incaricato al riconoscimento. L'accesso al portale avviene tramite inserimento di credenziali rilasciate all'utente, di cui la password è stata scelta e viene custodita con le adeguate norme di sicurezza, in completa autonomia da parte dell'utente. Si raccomanda all'utente di verificare frequentemente l'aggiornamento della propria anagrafica.

- Con l'adesione al servizio FEA, all'utente viene inviato un codice numerico e, in alternativa un QRcode, che permette di attivare sulla APP del dispositivo la creazione dei codici OTP per l'attivazione del processo di firma.
- Compilazione del documento in forma elettronica per firma FEA. AL termine della scelta del servizio, l'utente riceve tramite OTP link a landing page con informativa, modulo di adesione e contratto da sottoscrivere in formato digitale, ovvero la documentazione da firmare. Il Sistema, a questo punto, produce un nuovo documento contenente l'hash del documento da firmare.
- Creazione del certificato di firma FEA. Viene proposta la creazione di un certificato elettronico di tipo FEA (Firma Elettronica Avanzata) su una C.A. (Certification Authority) di tipo FEA, abbinato ad una coppia di chiavi di criptazione RSA. Il certificato conterrà i dati anagrafici dell'utente quali Nome e Cognome, Codice Fiscale, E-mail, numero di cellulare, e l'indicazione di Telepass S.p.A., quale propositore della soluzione di FEA, impiegando i dati anagrafici a lui mostrati sulla pagina. O nel caso ne fosse già dotato per precedenti operazioni, ne viene chiesto l'uso. L'utente è chiamato a confermare espressamente l'operazione o abbandonare. In caso di conferma, l'utente genera sulla APP Valid un codice OTP (One Time Password) da inserire nell'apposito campo firma. Su tale firma viene apposto un certificato abbinato all'utente, con coppia di chiavi RSA. In ogni caso sarà sempre possibile rifiutare il servizio e procedere in modalità analogica ovvero mediante firma digitale;

- Produzione del documento finale. Terminata la fase precedente, il sistema mette a disposizione dell'utente un documento informatico contenente i dati inseriti e la firma. Tale documento sarà sempre visualizzabile dall'utente nella propria area riservata.
- Conservazione. Il documento, sottoscritto e non più modificabile, sarà posto in Conservazione Digitale, a cura di Selecta Digital Services.

9.2 Il software di firma

Per la realizzazione del servizio di Firma Elettronica Avanzata per mezzo della applicazione PkBox Server disponibile dai server di Intesi Group, l'utente deve autenticarsi al portale di Intesi Group (raggiungibile alla URL https://user.time4mind.com) utilizzando le credenziali fornite dall'operatore durante la identificazione, o generate autonomamente attraverso la pagina di "Registrazione" sul modulo di autenticazione del portale Time4Mind.

In altri casi l'operazione di firma viene svolta a mezzo dell'app Telepass in dotazione ai gestori che invoca i servizi di Intesi Group attraverso chiamate web services.

Le sole credenziali di base non sono sufficienti per iniziare l'emissione di un certificato: per questo è necessario che l'utente inserisca il codice di sicurezza ricevuto al termine della registrazione ed il codice OTP indicato dalla app Valid installata sul dispositivo indicato al momento della registrazione dell'utente.

9.3 Integrità del documento sottoscritto

La verifica dell'integrità del documento può essere svolta da un qualsiasi software di verifica conforme al CA, come ad esempio Adobe Acrobat Reader o il verificatore proposto da Intesi Group e raggiungibile all'url https://va.time4mind.com.

10 IL PROCESSO DI FIRMA

Il processo in parola consente al cliente di visualizzare e leggere il documento sullo schermo del proprio dispositivo e di sottoscriverlo, utilizzando la modalità FEA con OTP e si sviluppa, in sintesi, nelle seguenti fasi:

- ***Identificazione del richiedente.*** L'utente viene identificato tramite documento di riconoscimento fornito al gestore del punto vendita al momento di adesione al servizio e tramite invio di OTP al momento della validazione del numero di telefono fornito, step propedeutico e necessario alla sottoscrizione con FEA con OTP del documento.
- ***Compilazione del documento in forma elettronica per firma FEA.*** il documento in forma elettronica viene compilato automaticamente dal sistema al termine della scelta dei prodotti desiderati. Il documento da sottoscrivere sarà visualizzabile dal cliente, tramite link inviato su SMS, prima di apporre la firma.
- ***Conferma della volontà di voler apporre le firme.*** Al termine del processo di selezione prodotti selezionando il button "invio SMS" viene avviato il processo di firma che si concretizza nei seguenti step:
    - Invio SMS con link a pagina web con il pdf del contratto compilato con la scelta del cliente, la presente informativa e il modulo di accettazione al servizio di FEA
    - Accettazione del documento da parte del cliente e invio di SMS con OTP per firma elettronica (modalità FEA con OTP)
    - Inserimento del codice OTP ricevuto all'interno dell'apposito box nella web page

- ***Scelta del certificato di firma FEA***. all'utente viene proposta la creazione di un certificato elettronico di tipo FEA (Firma Elettronica Avanzata) su una C.A. (Certification Authority) remota di tipo FEA, abbinato ad una coppia di chiavi di criptazione RSA. Il certificato conterrà i dati anagrafici dell'utente quali Nome e Cognome, Codice Fiscale, e-mail, numero di cellulare, e l'indicazione di Telepass S.p.A., quale propositore della soluzione di FEA, impiegando i dati anagrafici a lui mostrati sulla pagina. O nel caso ne fosse già dotato per precedenti operazioni, ne viene chiesto l'uso. L'utente è chiamato a confermare espressamente l'operazione o abbandonare. In caso di conferma, l'utente riceve sull'indirizzo telefonico indicato in sede di registrazione, un codice OTP (One Time Password) da inserire nell'apposito campo firma. Per maggiore sicurezza, su tale firma viene inserito un certificato digitale associato all'utente, contenente la chiave RSA pubblica
- ***Produzione del documento finale.*** Terminata la fase precedente, il sistema mette a disposizione

dell'utente un documento digitale contenente i dati inseriti e la firma. Tale documento verrà inviato via mail al cliente al termine del processo.

- ***Conservazione***. Il documento, sottoscritto e non più modificabile sarà posto in Conservazione Digitale, a cura di Selecta Digital Services.

11 COMPONENTI DI SICUREZZA

La soluzione di firma è garantita da Intesi Group sia per la componente server sia per la componente Device.

11.1 Server

La sicurezza dei server è garantita sia dalle procedure e sistemi di sicurezza di Intesi Group sia, per quanto concerne le misure di sicurezza fisiche, dal fornitore presso cui sono collocati i server.

L'accesso all'applicazione Web di gestione del server e ai Web Services avviene previa autenticazione dell'utente o tramite token di sicurezza, e con protocollo https.

12 ARCHIVIAZIONE E CONSERVAZIONE DOCUMENTI

Vedere manuale di conservazione pubblicato al seguente link info-telepass.selecta.it

13 LA GESTIONE DEL CONTENZIOSO

Il processo di gestione di un contenzioso, inizialmente, segue le politiche di gestione interne previste ma, qualora sia necessario l'intervento giudiziale, si deve obbligatoriamente prevedere un diverso approccio di perizia. In questo caso, in caso di richiesta di verifica da parte dell'organo giudiziario Telepass S.p.A. provvede, su indicazione della magistratura, a recuperare con le modalità richieste il documento oggetto del contezioso (chiedendo supporto eventualmente al conservatore) e da Intesi Group tutte le informazioni conservate e legate alla generazione del

certificato dell'utente firmatario del documento, oltre alle informazioni di registrazione dell'utente stesso.

Tutto ciò sarà messo a disposizione della magistratura.

L'onere probatorio, in caso di sottoscrizione con FEA, è a carico dell'erogatore del servizio FEA che deve poter dimostrare:

- La firma apposta (certificato FEA) è riferita al firmatario;
- Gli strumenti di firma erano in possesso del firmatario (se ha ceduto il telefono senza modificare le informazioni la responsabilità è del firmatario, se debitamente informato);
- Il documento non ha subito modifiche dopo la sottoscrizione;
- La registrazione deve poter dimostrare che i dati sono stati resi dal firmatario;
- L'identificazione per inserire la firma è stata eseguita in modo certo.