Manuale Operativo
Servizio di Firma Elettronica Avanzata (FEA) con One Time Password (OTP)

erogato da Banco di Credito P. Azzoaglio S.p.a. con certificati emessi da Intesi Group S.p.a.

11/10/2023

SOMMARIO

1. INTRODUZIONE

Il presente documento è stato realizzato dal Banco di Credito P. Azzoaglio 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.

Il Banco di Credito P. Azzoaglio 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.

1 DEFINIZIONI

1.1 Definizioni riguardanti i soggetti

Soggetto	Illustrazione
Soggetti che erogano servizi di Firma Elettronica Avanzata (Banco di Credito P. Azzoaglio 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 Banco di Credito P. Azzoaglio S.p.a., per usufruire di uno dei servizi offerti. Può essere: utente/cliente persona fisica utente/cliente persona giuridica

1.2 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

Sigle	Illustrazione
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

Sigle	Illustrazione
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,

Sigle	Illustrazione
	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 (FEA)

2 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 22.02.2013);

2. eventuale **Modulo di richiesta di copia della documentazione di accettazione FEA** (v. art. 57, c. 1 lett.c DPCM 22.02.2013);
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.**

3 GLI ATTORI

3.1 Soggetto che eroga la soluzione di FEA

Il Banco di Credito P. Azzoaglio 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.

Dati identificativi

Ragione Sociale	**Banco di Credito P. Azzoaglio S.p.a.**
Indirizzo sede	Via A. Doria, 17 - 12073 Ceva (CN)
Partita Iva	00166050047
Registro Imprese	Cuneo
REA	1368
Indirizzo E-Mail	posta@azzoaglio.it
Indirizzo PEC	direzione@pec.azzoaglio.it
Numero Telefonico	0174/7241
Indirizzo Sito Istituzionale	www.azzoaglio.it

3.2 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**.

3.3 Altri soggetti coinvolti

Nel processo sono coinvolti i seguenti ulteriori soggetti:

- **CRIF S.p.a.**: società che fornisce, anche per mezzo di altre società del gruppo ovvero di terzi sub-fornitori, il servizio di identificazione e verifica documenti d'identità degli utenti durante il processo di onboarding sul portale online del Banco di Credito P. Azzoaglio S.p.a.
- **CSE - Consorzio Servizi Bancari Soc. Cons. a r.l.:** società che fornisce il sistema informativo al Banco di Credito P. Azzoaglio S.p.a. con il quale viene realizzata la conservazione digitale dei documenti informatici sottoscritti con soluzione di FEA.

4 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 Banco di Credito P. Azzoaglio 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, Banco di Credito P. Azzoaglio 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	Il Banco di Credito P. Azzoaglio S.p.a. utilizza la seguente modalità di riconoscimento e identificazione sicura dell'utente a cui viene rilasciato un certificato di FEA: Conclusa la fase di onboarding e accettata la privacy, viene effettuata la verifica dell'identità tramite il servizio SELF ID di Inventia S.r.l. (azienda facente parte del gruppo CRIF S.p.a.) che permetterà di: 1. Effettuare il caricamento dei documenti dell'utente; 2. Estrarre con un OCR le informazioni dal documento per permetterne la validazione; 3. Acquisire le immagini dell'utente al fine di permettere una successiva fase di face matching tra le immagini acquisite e le foto del documento dell'utente. Si specifica che il servizio di SELF ID è integrato nel portale online del Banco di Credito P. Azzoaglio S.p.a. e, pertanto, non verrà effettuato un reindirizzamento all'esterno del portale stesso. Nel caso

	l'utente non abbia a disposizione un PC con telecamera potrà proseguire il flusso sullo smartphone. 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 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, 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	Il Banco di Credito P. Azzoaglio S.p.a. fornice sempre il documento completo tramite le proprie interfacce ed il documento completo di firma elettroniche dell'utente sarà disponibile per il download nell'area riservata del servizio del proponente la FEA.
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 il Banco di Credito P. Azzoaglio 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).

5 VALORE GIURIDICO DELLA FEA

La soluzione proposta dal Banco di Credito P. Azzoaglio 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.

5.1 Forma

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

5.2 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.

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, il Banco di Credito P. Azzoaglio S.p.a. ha deciso di proporre la soluzione di FEA ai propri utenti/clienti diretti persone fisiche e nuovi utenti/clienti persone fisiche per la sottoscrizione di una molteplicità di documenti per il tramite del proprio portale online.

6 ADEMPIMENTI PER IL RISPETTO DELLE NORME SULLA FEA

I soggetti che erogano soluzioni FEA 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 (Modulo per la richiesta di copia della dichiarazione di accettazione delle condizioni del servizio FEA e relativa documentazione – All. 2);
6) Rendere note le modalità con cui effettuare la richiesta di cui al punto 5, pubblicandole anche sul proprio sito internet;
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.

6.1 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.

Prima identificazione

L'identificazione del firmatario viene effettuata dagli operatori del Banco di Credito P. Azzoaglio S.p.a. 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.

Il Banco di Credito P. Azzoaglio 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 elettronica 3.0;
- Carta d'identità elettronica;
- Carta d'identità cartacea;
- Patente di guida;
- Passaporto.

In questa fase, si procede altresì con la richiesta e conseguente certificazione dei seguenti recapiti:

- 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.

Identificazioni successive

Le identificazioni successive alla prima sono temporalmente posticipate rispetto all'accettazione del servizio FEA.

In questo caso le modalità operative possono essere diverse, ma si riassumono in due classi operative:

- Presentazione di un documento di identificazione all'operatore (de visu);
- Utilizzo delle credenziali ottenute o ottenibili con gli strumenti registrati dopo la prima identificazione (ad esempio tramite il servizio di "Banca telefonica", etc.).

L'identificazione è, in ogni caso, a carico del Banco di Credito P. Azzoaglio S.p.a.

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 dal Banco di Credito P. Azzoaglio S.p.a. e poi comunicate a Intesi Group a mezzo di canali concordati.

6.2 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.

Il Banco di Credito P. Azzoaglio S.p.a. utilizza la seguente modalità di riconoscimento e identificazione sicura dell'utente a cui viene rilasciato un certificato di FEA:

Conclusa la fase di onboarding e accettata la privacy, viene effettuata la verifica dell'identità tramite il servizio SELF ID di Inventia S.r.l. (azienda facente parte del gruppo CRIF S.p.a.) che permetterà di:

1. Effettuare il caricamento dei documenti dell'utente;
2. Estrarre con un OCR le informazioni dal documento per permetterne la validazione;
3. Acquisire le immagini dell'utente al fine di permettere una successiva fase di face matching tra le immagini acquisite e le foto del documento dell'utente.

Si specifica che il servizio di SELF ID è integrato nel portale online del Banco di Credito P. Azzoaglio S.p.a. e, pertanto, non verrà effettuato un reindirizzamento all'esterno del portale stesso. Nel caso l'utente non abbia a disposizione un PC con telecamera potrà proseguire il flusso sullo smartphone.

Dopo aver selezionato il tipo di documento (tra quelli ritenuti idonei come precedentemente indicati) viene avviato il processo di video identificazione dell'utente, come di seguito descritto:

A questo punto partirà un countdown di 5 secondi in cui verranno date delle istruzioni all'utente al termine delle quali verrà effettuata la rilevazione del volto dell'utente. Si specifica che verrà chiesto all'utente di

sorridere, di girare lentamente la testa a destra e a sinistra: tutte queste azioni serviranno a verificare che si tratti di una persona reale e, ad esempio, non di una fotografia o un manichino. Una volta completata correttamente questa fase, verrà richiesto all'utente di proseguire con la fase di riconoscimento del documento. Come nel caso del rilevamento facciale, anche in questo caso dopo un breve countdown di 5 secondi verranno richiesti e rilevate le informazioni presenti sia sul fronte che sul retro del documento. Dopo aver raccolto tutte le schermate necessarie, il sistema procede con la comparazione tra volto e documento di identità. L'utente potrà quindi correggere eventuali errori e confermare i propri dati.

L'utente potrà modificarli o confermarli. Una volta completata questa fase l'utente verranno completati tutti gli step previsti sul servizio selfID di CRIF. Le informazioni saranno anonimizzate e dematerializzate sulla piattaforma di Inventia in seguito alla comunicazione con i sistemi di Banco Azzoaglio. Sui sistemi di Banco Azzoaglio, invece, le informazioni dovranno essere archiviate. Inventia fornirà a Banco Azzoaglio sia le informazioni estratte che le scansioni. L'intero flusso di riconoscimento, compreso il form di verifica dei dati al suo termine sono gestiti e implementati da Inventia.

Una volta completato e confermato l'inserimento da parte dell'utente, verrà effettuato il controllo incrociato dati anagrafici (dati inseriti dall'utente con dati del documento d'identità fotografato).
Il controllo sarà effettuato nella *blacklist* interna della banca e solo se non sarà presente verrà effettuata l'interrogazione al servizio *Idea* erogato da CRIF, che consentirà la rilevazione di eventuali incongruenze relative ai dati di:

a. Indirizzo (tramite la corrispondenza dello stesso sullo stradario);
b. Documento di riconoscimento;
c. Numero di telefono inserito dall'utente;
d. La tipologia del documento (in base all'individuazione dell'ente emittente);
e. Numero documento.

Se l'interrogazione avrà esito negativo il rapporto sarà dunque "congelato" sino a quando l'esito dei controlli sarà andato a buon fine e fino a che saranno espletate le fasi di adeguata verifica.
Se risulterà essere tutto a norma, il rapporto sarà caricato sul sistema informativo e sarà reso operativo a tutti gli effetti. In caso negativo, il rapporto non sarà aperto (rimarrà aperta e tracciata la pratica).
Una volta che l'utente avrà completato con successo la procedura di iscrizione, verrà effettuata una prima interrogazione al sistema interno bancario per verificare che l'utente non sia presente nella *black list* della banca. Questa sarà una prima fase di verifica.

6.3 Informazione del richiedente firmatario

Identificato il cliente, prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, il Banco di Credito P. Azzoaglio S.p.a. procede ad informare il richiedente firmatario sulle condizioni di uso del servizio, ivi comprese le limitazioni d'uso, presentandogli anche l'apposita Informativa, che verrà consegnata su richiesta dell'interessato e che in ogni caso è reperibile sul sito internet sito del Banco di Credito P. Azzoaglio S.p.a..

6.4 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.

6.5 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.

6.6 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.

6.7 La tecnologia utilizzata

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

I browser consigliati sia per la visualizzazione Web che Mobile (tutti gratuiti) del portale online del Banco di Credito P. Azzoaglio S.p.a. sia dei documenti da sottoscrivere, sono:

- Google Chrome (ultima versione disponibile - Windows e Mac OS);
- Mozilla Firefox (ultima versione disponibile - Windows e Mac OS);
- Safari (ultima versione disponibile - solo Mac OS) - obbligatorio per dispositivi Apple.

Tutti i documenti presenti sul sito sono visualizzabili con il supporto del programma Acrobat Reader (9 o successiva) o similari, scaricabili direttamente da Internet.

6.8 Aggiornamento del sito internet

Il Banco di Credito P. Azzoaglio S.p.a., in ottemperanza a quanto richiesto dalla normativa in essere, pubblica sul proprio sito internet il presente documento.

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

Unitamente al Manuale Operativo FEA, vengono pubblicati sul sito internet anche i moduli:

- Modulo per la richiesta di copia della dichiarazione di accettazione delle condizioni del servizio FEA e relativa documentazione;
- Adesione al servizio;
- Revoca del servizio;
- Dichiarazione polizza assicurativa;

6.9 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 al Banco di Credito P. Azzoaglio S.p.a., 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 sito internet;
c. Consegnare il modulo firmato.

6.10 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*".

Al riguardo, il Banco di Credito P. Azzoaglio S.p.a., in qualità di soggetto che eroga la soluzione di FEA, dichiara di avere stipulato adeguata polizza assicurativa, come da dichiarazione pubblicata sul sito internet.

7 ADEMPIMENTI PER IL RISPETTO DELLE NORME SULLA PRIVACY

7.1 Informazione dell'utente firmatario

Il Banco di Credito P. Azzoaglio 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 il Banco di Credito P. Azzoaglio 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 oltre che essere a disposizione durante l'onboarding sul portale online del Banco di Credito P. Azzoaglio S.p.a..

7.2 Diritti relativi ai dati personali e modalità di esercizio

Il Banco di Credito P. Azzoaglio 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 il Banco di Credito P. Azzoaglio 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@azzoaglio.it.

8 LA SOLUZIONE INTESI GROUP

Nel presente capitolo si descrivono le caratteristiche della soluzione fornita al Banco di Credito P. Azzoaglio 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 Banco di Credito P. Azzoaglio S.p.a.

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.

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).

8.1 Elaborazione della richiesta

Identificazione del richiedente.

- L'utente è già stato identificato al momento di adesione al servizio FEA, 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 e

certificati durante il processo di onboarding sul portale online del Banco di Credito P. Azzoaglio S.p.a..

- Con l'adesione al servizio FEA, all'utente viene data la possibilità di procedere con il processo e concludere la sottoscrizione della documentazione tramite FEA con OTP.
- Compilazione del documento in forma elettronica per firma FEA. Tramite apposita pagina del portale online del Banco di Credito P. Azzoaglio S.p.a., all'utente appare, in formato digitale, la documentazione da firmare che potrà essere visualizzata e/o scaricata dall'utente.
- 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 del Banco di Credito P. Azzoaglio S.p.a. quale propositore della soluzione di FEA, impiegando i dati anagrafici a lui mostrati sulla pagina. L'utente è chiamato a confermare espressamente l'operazione o abbandonare. In caso di conferma, la procedura genera un codice OTP (One Time Password) che viene inviato tramite SMS all'utente che deve provvedere ad inserirlo nell'apposito riqadro. Su tale firma viene apposto un certificato abbinato all'utente, con coppia di chiavi RSA.
- 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 reso disponibile all'utente.
- Conservazione. Il documento, sottoscritto e non più modificabile, sarà posto in Conservazione Digitale a cura del Banco di Credito P. Azzoaglio S.p.a. per il tramite del fornitore del proprio sistema informativo.

8.2 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 viene autenticato al portale di Intesi Group durante il processo di onboarding sul portale online del Banco di Credito P. Azzoaglio S.p.a. che invoca i servizi di Intesi Group attraverso chiamate web services.

8.3 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.

9 IL PROCESSO DI FIRMA

L'utente riceve una e-mail all'indirizzo certificato durante il processo di onboarding sul portale del Banco di Credito P. Azzoaglio S.p.a. con l'invito a sottoscrivere la documentazione contrattuale.

L'utente, come primo documento, provvede a visualizzare e sottoscrivere l'adesione alla firma elettronica avanzata (FEA).

Successivamente provvede a visualizzare e sottoscrivere i documenti contrattuali del rapporto.

Al termine del processo di firma, l'utente riceve tramite email la copia della documentazione firmata.

10 COMPONENTI DI SICUREZZA

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

10.1 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.

11 ARCHIVIAZIONE E CONSERVAZIONE DOCUMENTI

I documenti firmati tramite la soluzione di firma sopra descritta vengono acquisiti dal Banco di Credito P. Azzoaglio durante il processo di *onboarding* e, dopo l'apertura del rapporto, vengono archiviati nel proprio sistema informativo assoggettandoli a conservazione sostitutiva ai sensi della normativa vigente.

12 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, il Banco di Credito P. Azzoaglio 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.