



Firma Elettronica Avanzata (FEA)

Manuale operativo

Contenuti del documento

Introduzione	2
Scopo del documento	2
Proprietà intellettuale	2
Contesto	3
Attori	3
Contatti	3
Caratteristiche della soluzione FEA	4
Identificazione del firmatario	4
Adesione al servizio FEA	4
Firma del documento	4
Conservazione dei documenti	4
Tutela assicurativa	4
Processo di apposizione della FEA	5
Definizioni e riferimenti normativi	6
Definizioni	6
Acronimi	7
Normativa di riferimento	7

Introduzione

Scopo del documento

Questo manuale operativo, ai sensi dell'articolo 57, comma 1 del DPCM del 22/02/2013, descrive il processo di apposizione di una Firma Elettronica Avanzata (FEA) come alternativa alla firma autografa (di seguito denominato Servizio FEA), tramite cui il contraente aderisce ai prodotti intermediati da Yobi S.r.l. tramite le proprie piattaforme web. Il presente manuale operativo pertanto rende note:

- le modalità di richiesta della copia della dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
- le modalità di richiesta d'indicazione delle informazioni atte a dimostrare la sussistenza delle caratteristiche che deve avere una soluzione di firma elettronica avanzata;
- le caratteristiche della soluzione implementata necessarie a configurarla quale soluzione di firma elettronica avanzata;
- le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare alle norme in vigore;
- le modalità per revocare il consenso all'utilizzo della soluzione di firma elettronica avanzata;
- le modalità di contatto del servizio di assistenza.

Questo manuale operativo è redatto come *Documento informatico* ed è pubblicato, nella sua ultima versione, sul sito di Yobi.

Per facilitare la comprensione del testo, ogni elemento in corsivo rimanda ad una definizione o acronimo riportati nella sezione Definizioni di questo manuale.

Proprietà intellettuale

Questo manuale operativo è stato redatto da Yobi in qualità di *Erogatore del Servizio FEA*.

Le informazioni contenute nel presente documento sono strettamente confidenziali e riservate, di esclusiva proprietà di Yobi. Esse sono disponibili esclusivamente per i soggetti cui è stato direttamente consegnato il documento e per le finalità per cui è stato consegnato.

Contesto

Yobi ha deciso di implementare e mettere a disposizione dei propri clienti un *Servizio FEA* basato su *OTP* al fine di permettere la sottoscrizione digitale delle polizze assicurative da lei intermedate. Il *Servizio FEA* è sempre gratuito per i clienti Yobi.

Attori

Nella realizzazione del *Servizio FEA* descritto in questo manuale operativo sono coinvolte le seguenti società:

- Yobi S.r.l.: soggetto che eroga il servizio;
- Openwork S.r.l.: *Soggetto realizzatore del Servizio FEA* (di seguito *Openwork*);
- CompEd Software Design S.r.l.: soggetto erogatore dei servizi tecnici di *Firma Digitale* e dei *Certificati elettronici* (di seguito per brevità *Comped*).
- Unimatica-RGI S.p.A.: *Soggetto erogatore del Servizio di conservazione a norma*.

Contatti

Yobi, in qualità di erogatore del *Servizio FEA*, si mette a disposizione dei propri clienti in caso di richieste riguardanti:

- avere copia della dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
- avere indicazione delle informazioni atte a dimostrare la sussistenza delle caratteristiche che deve avere una soluzione di firma elettronica avanzata;
- comunicare la revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata.

I clienti di Yobi possono avanzare le proprie richieste presso support@helloyobi.com.

Caratteristiche della soluzione FEA

Identificazione del firmatario

La procedura di identificazione dell'*Utente firmatario* avviene durante la procedura di iscrizione alla *Piattaforma web* tramite la sottomissione in forma elettronica del proprio documento d'identità in corso di validità. La verifica della validità del documento di riconoscimento viene eseguita da *Yobi* tramite operazioni di back-office.

Durante la medesima procedura vengono validati indirizzo e-mail e numero di cellulare tramite l'invio e la validazione di un *OTP*.

Adesione al servizio FEA

L'adesione al *Servizio FEA* è facoltativa ma è necessaria per l'adesione ai prodotti intermediati da *Yobi*. Nel caso in cui il cliente non ne accettasse le condizioni per intero, non sarà possibile aderire ai prodotti intermediati da *Yobi*.

L' *Utente firmatario*, attraverso l'accettazione del *Modulo di adesione al Servizio FEA*:

- manifesta la volontà di aderire al *Servizio FEA*;
- accetta la modalità di trattamento dei dati personali;
- riceve indicazione circa la reperibilità della propria copia dei documenti sottoscritti a mezzo *FEA*.

L'adesione al *Servizio FEA* è limitata alla sottoscrizione di uno specifico *Documento informatico*, cessa pertanto dopo l'avvenuta sottoscrizione dello stesso.

Firma del documento

Il *Servizio FEA* certifica l'apposizione della firma su un determinato *Documento informatico* da parte dell'*Utente firmatario*, tramite *Firma digitale* in formato *PaDES* con un *Certificato digitale remoto*.

Il *Certificato digitale* può essere utilizzato univocamente per la sottoscrizione, da parte dell'*Utente firmatario*, dello specifico *Documento informatico* per cui è stato generato.

Il *Certificato digitale* oltre alle chiavi crittografiche contiene Nome, Cognome, Codice Fiscale, Numero del documento di riconoscimento, Numero di cellulare dell'*Utente firmatario*.

I dati che descrivono il processo di firma sono salvati in un report. Al fine di certificarne l'autenticità, al report viene apposta *Firma digitale* con *Certificato digitale qualificato* (Sigillo Elettronico) rilasciato ad *Openwork*. Il report non è rilasciato all'*Utente firmatario* ma resta disponibile per successive verifiche.

Conservazione dei documenti

I documenti firmati sono inviati al *Servizio di conservazione a norma* e conservati per almeno 20 anni, garantendo per tutto il periodo la disponibilità, integrità e leggibilità, secondo quanto previsto dall'articolo 56, comma 1 del DPCM 22/02/2013.

Tutela assicurativa

Yobi ha stipulato una idonea copertura assicurativa per la responsabilità civile in conformità all'articolo 57, comma 2 del DPCM 22/02/2013.

Processo di apposizione della FEA

Il processo di apposizione della *FEA* si articola in alcuni passaggi guidati sulla *Piattaforma web*. Il processo è vincolato e l'*Utente firmatario* è informato ad ogni passaggio su quali azioni compiere per portare a termine il processo.

I passaggi che definiscono il processo, per l'*Utente firmatario*, sono i seguenti:

- visualizzazione e accettazione del *Modulo di adesione al Servizio FEA*;
- visualizzazione e accettazione dei documenti da firmare;
- ricezione di un *OTP*, associato alla specifica operazione di firma, sul numero di cellulare indicato in fase di iscrizione alla *Piattaforma web*;
- inserimento del codice *OTP*;
- ricezione, sull'indirizzo e-mail indicato in fase di iscrizione alla *Piattaforma web*, del *Documento informatico* firmato.

Il *Documento informatico* firmato è ottenuto come unione dei documenti da firmare, del *Modulo di adesione al Servizio FEA* e del documento di identità dell'*Utente firmatario*.

Il codice *OTP* deve essere inserito entro un tempo limite, diversamente risulterà non più valido e dovrà essere richiesto nuovamente.

L'*Utente firmatario* ha facoltà di interrompere il processo in qualsiasi momento senza incorrere in qualsivoglia costo aggiuntivo.

Definizioni e riferimenti normativi

Definizioni

Agenzia per l'Italia Digitale o **AgID**: agenzia che, come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22, ha sostituito il Centro Nazionale per l'Informatica nella Pubblica Amministrazione e DigitPa.

Certification authority o **CA**: soggetto che rilascia Certificati elettronici consente la verifica di validità del Certificato digitale e nel caso di Certificato digitale remoto custodisce in maniera sicura la Chiave privata.

Certificato digitale: file contenente i dati identificativi dell'intestatario e la sua chiave pubblica firmato dalla Certification Authority.

Certificato digitale remoto: certificato digitale non custodito su dispositivi fisici forniti all'intestatario dello stesso (smart-card, token USB) ma su dispositivi remoti gestiti dalla CA.

Certificato qualificato: certificato digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da CA che rispondono ai requisiti di cui all'allegato II della medesima direttiva.

Codice dell'Amministrazione Digitale o **CAD**: normativa di cui al decreto legislativo 7 marzo 2005, n.82 e successive modificazioni.

Crittografia asimmetrica: conosciuta anche come Crittografia a doppia chiave o Crittografia a chiave pubblico/privata. È un algoritmo che consente di cifrare un'informazione con la prima chiave (Chiave privata) e di decifrarla con la seconda chiave (Chiave pubblica). In questo modo un soggetto che deve fornire una informazione ad un soggetto terzo non è obbligato nel fornire al ricevente la sua chiave privata ma solo quella pubblica; il ricevente è certo della identità del mittente dell'informazione in quanto l'unico che può averla cifrata con la chiave privata è proprio colui che ha reso disponibile la chiave pubblica.

Documento elettronico: rappresentazione informatica di qualsiasi contenuto informativo.

Documento informatico: Documento Elettronico contenente atti, fatti o dati giuridicamente rilevanti.

Firma digitale: particolare tipo di Firma elettronica che associa ad un Documento elettronico il Certificato digitale del firmatario e un Hash code cifrato con la chiave privata del firmatario. In fase di verifica della firma è sufficiente decifrare l'Hash code associato con la chiave pubblica del Certificato digitale e verificare che il valore ottenuto coincida con l'Hash code calcolato al momento della verifica.

Firma elettronica: insieme di dati informatici, allegati oppure connessi tramite associazione logica a un Documento Elettronico, utilizzati come metodo per indicare l'intenzione del firmatario di approvare o accettare il contenuto del Documento Elettronico.

Firma Elettronica Avanzata o **FEA**: insieme di dati informatici connessi a un Documento elettronico che consentono l'identificazione del firmatario del documento, garantiscono la connessione univoca del documento al firmatario, sono creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, sono collegati al contenuto del Documento elettronico ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati modificati successivamente all'operazione di firma.

Hash code: insieme di dati che identificano univocamente un insieme di altri dati, ottenuti applicando a questi ultimi l'algoritmo di hash.

Modulo di adesione al Servizio FEA: documento contrattuale elaborato da Yobi che raccoglie i consensi dell'Utente firmatario in merito all'utilizzo del servizio di Firma Elettronica Avanzata, stipulato dal cliente una tantum all'inizio del rapporto o in un momento successivo.

One Time Password o **OTP**: codice "usa e getta" utilizzato per una singola azione da parte di un utente di un servizio informatico inviato ad un dispositivo di cui è certificato il possesso da parte di quello specifico utente.

Piattaforma Web: applicazione web attraverso la quale Yobi consente l'adesione ai prodotti da lei intermediati.

PDF Advanced Electronic Signature o **PADES**: modalità di associazione dei dati di Firma elettronica ad un Documento elettronico in formato PDF, definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.

Portable Document Format o **PDF**: standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).

Servizio di conservazione a norma: servizio software strumentale alla conservazione dei Documenti informatici in osservanza alle direttive AgID espresse nel CAD.

Servizio FEA: servizio strumentale alla generazione e alla verifica della Firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis del DL 235/2010.

Soggetto erogatore del servizio di Conservazione a norma: soggetto giuridico accreditato all'Albo dei conservatori AgID per l'erogazione del Servizio di conservazione a norma.

Soggetto erogatore del Servizio FEA: soggetto giuridico che eroga Servizi FEA 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.

Soggetto realizzatore del Servizio FEA: soggetto giuridico che realizza tecnicamente Servizi FEA.

Utente: persona fisica registrata sulla Piattaforma Web e dotata delle credenziali per accedervi.

Utente firmatario: Utente che firma o ha intenzione di firmare un Documento informatico prodotto dalla Piattaforma Web.

Acronimi

AES – Advanced Encryption Standard: è un algoritmo di cifratura a blocchi e a chiave simmetrica operante su un gruppo di bit a lunghezza finita.

AgID – Agenzia per l'Italia Digitale: agenzia che, come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22, ha sostituito il Centro Nazionale per l'Informatica nella Pubblica Amministrazione e DigitPa.

CAD – Codice dell'Amministrazione Digitale: normativa di cui al decreto legislativo 7 marzo 2005, n.82 e successive modificazioni.

OTP – One-Time Password: codice “usa e getta” utilizzato per una singola azione da parte dell'utente.

PADES – PDF Advanced Electronic Signature: formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.

PDF – Portable Document Format: standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).

Normativa di riferimento

DPR n.445/2000: “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”.

Deliberazione CNIPA n.11 del 19 febbraio 2004: “Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali”.

D.Lgs. 82/2005: “Codice dell'amministrazione digitale”.

D.Lgs. 231/2007: “Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione”.

DPCM 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, lettera b) , 35, comma 2, 36, comma 2, e 71”.

DPCM 3 dicembre 2013: “Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”.

Regolamento UE 910/2014: Regolamento EU in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Regolamento UE 679/2016: Regolamento EU relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Determinazione AgID 121/2019: “Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate”.

Provvedimento di Banca d'Italia del 30 luglio 2019: “Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo”.