MANUALE OPERATIVO

PROGETTO FEA

FIRMA ELETTRONICA AVANZATA

Data Emissione:	10/2019	**Autore:**	HDI ASSICURAZIONI SPA
Data Approvazione:		**Eseguita da:**	
Data Riesame:		**Eseguita da:**	
Nome documento		**Revisione:**	

Mod. 06T

SOMMARIO

1 INTRODUZIONE

La firma elettronica è definita nel Regolamento UE 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (di seguito "*eIDAS*") come "*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*".

In merito al valore legale del documento informatico sottoscritto con firma elettronica, il quadro normativo vigente considera che l'idoneità a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.

Il documento informatico soddisfa invece il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore […] con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

In particolare, la firma elettronica avanzata (di seguito "*FEA*") è regolamentata nell'ambito d.P.C.M. 22 febbraio 2013 agli articoli 55 e seg. e costituisce una specifica tipologia di firma elettronica che:

- consente di garantire l'identificazione del firmatario del documento,
- garantisce la connessione univoca tra la persona e la firma,
- garantisce il controllo esclusivo del firmatario del sistema di generazione della firma,
- garantisce la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma.

La FEA, per essere correttamente implementata, deve consentire al firmatario di avere evidenza di ciò che ha sottoscritto, deve garantire una connessione univoca fra firma e documento sottoscritto e deve consentire l'individuazione dell'erogatore del servizio.

La soluzione di FEA, a differenza delle soluzioni di firma elettronica qualificata e digitale, non necessita né di un certificato qualificato né di un dispositivo sicuro per la sua valida apposizione. La definizione di cui all'art. 26 di eIDAS contiene solamente riferimento ai seguenti requisiti:

- connessione unicamente al firmatario;
- idoneità ad identificare il firmatario;
- creazione 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

- collegamento dei dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Il limite della soluzione FEA consiste nella sua utilizzabilità, secondo quanto al d.P.C.M. 22 febbraio 2013, esclusivamente nei rapporti giuridici intercorrenti tra il sottoscrittore ed il soggetto che ha realizzato per proprio conto la soluzione di firma, oppure si avvale di quelle di terzi, al fine di utilizzarle nel processo di dematerializzazione dei rapporti intrattenuti per motivi istituzionali, societari o commerciali. La soluzione FEA non è soggetta ad alcuna autorizzazione preventiva, la normativa indica solo le caratteristiche e garanzie che la firma elettronica avanzata deve avere perché abbia il valore di scrittura privata.

Una delle tecnologie più diffuse per sottoscrivere documenti con una firma elettronica che abbia il valore di firma elettronica avanzata consiste nell'impiego di soluzione firma mediante codice numerico mono uso (cd. One Time Password o OTP).

Nell'ambito della soluzione di firma con OTP l'erogatore del servizio (o suo fornitore tecnologico) attribuisce a una persona preventivamente identificata un certificato e, al momento di firmare un documento, invia a detta persona - mediante canale preventivamente concordato - un codice numerico che la stessa utilizza per dare disposizione all'erogatore di apporre il certificato assegnatoli sul documento che sta visualizzando, finalizzandone così la sottoscrizione.

La soluzione di FEA implementata da **HDI Assicurazioni S.p.A.** e descritta nel presente documento si basa su un sistema di firma mediante OTP.

L'articolo 57 comma 1 del d.P.C.M. 22 febbraio 2013, definisce gli obblighi a carico dei soggetti che erogano soluzioni di firma elettronica avanzata. Questi obblighi sono:

a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;

b) conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'art. 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità;

c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;

d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;

e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1;

f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;

g) pubblicare le caratteristiche di cui alle lettere e) ed f) sul proprio sito internet;

h)	*assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.*

1.1 OBIETTIVI DEL DOCUMENTO

Il presente documento ha l'obiettivo, come stabilito nell'articolo 57 comma 1 del d.P.C.M. 22 febbraio 2013, di rendere note:

- le modalità con cui effettuare la richiesta di avere copia della dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
- le modalità con cui effettuare la richiesta di avere indicazione delle informazioni atte a dimostrare la sussistenza delle caratteristiche che deve avere una soluzione di firma elettronica avanzata, accennate in premessa;
- 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 a quanto normativamente prescritto per la soluzione di firma elettronica avanzata;
- le modalità per revocare il consenso all'utilizzo della soluzione di firma elettronica avanzata;
- le modalità di contatto del servizio di assistenza.

Nel presente documento si illustrano i punti fondamentali del processo, il rispetto della normativa e gli attori coinvolti. Sono inoltre descritti i ruoli e le responsabilità.

Il presente documento, che in prima emissione esprime gli obiettivi e le caratteristiche del servizio, potrà essere oggetto di eventuali modifiche e/o integrazioni che verranno definite in corso di erogazione.

Il presente documento è pubblicato, nella sua ultima versione aggiornata, annualmente sul sito-web del Soggetto erogatore dei servizi di firma elettronica avanzata.

1.2 VERSIONE E REFERENTI

Versione:	Data:	Indicazioni:	Modifiche
1.0	10/2019		

1.3 PROPRIETÀ INTELLETTUALE

Il presente "Manuale Operativo", redatto in collaborazione con Plug-In S.r.l., è di proprietà di HDI Assicurazioni S.p.A.

2 DEFINIZIONI

2.1 DEFINIZIONI RIGUARDANTI I SOGGETTI

Soggetto	Illustrazione
Agente	La persona incaricata dal Soggetto erogatore dei servizi di Firma Elettronica Avanzata (agente assicurativo) che identifica l'utente / firmatario, lo informa in merito alle condizioni d'uso / modalità del servizio e partecipa al processo di acquisizione della firma elettronica avanzata da parte dell'utente.
Certificatore	Ente, pubblico o privato, abilitato a rilasciare certificati digitali previa specifica procedura di certificazione in conformità con gli standard nazionali ed europei.
Cliente	È il soggetto a favore del quale l'ente definito come "**Soggetto erogatore dei servizi di firma elettronica avanzata**" mette a disposizione una soluzione di firma elettronica avanzata al fine di sottoscrivere i documenti informatici.
Soggetti realizzatori dei servizi di firma elettronica avanzata	Soggetto giuridico (Plug-In S.r.l.) che, quale oggetto dell'attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore di Soggetti erogatori.
Soggetto erogatore dei servizi di firma elettronica avanzata	Soggetto giuridico (HDI Assicurazioni S.p.A.) che eroga la soluzione 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 sviluppate dai soggetti che le producono come attività di impresa.
Titolare	È la persona fisica identificata dal Certificatore, cui è stata attribuita la firma digitale (o remota) utilizzata per chiudere il documento sottoscritto con la soluzione di firma elettronica avanzata ed è stata consegnata la chiave privata del certificatore stesso.

2.2 DEFINIZIONE RIGUARDANTI GLI ACRONIMI E TERMINI UTILIZZATI

Sigle	Illustrazione
AES	Acronimo di Advanced Encryption Standard: è un algoritmo (utilizzato come standard dal governo degli Stati Uniti) di cifratura a blocchi e a chiave simmetrica operante su un gruppo di bit a lunghezza finita.
AgID	Agenzia per l'Italia Digitale (come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22): ha sostituito **CNIPA** e **DigitPa**.
Certificato digitale	Nella crittografia asimmetrica è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, ecc.), il quale dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.
Certificato qualificato	Certificato digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Chiave Privata del PAdes	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 del PAdes	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.
CNIPA (DigitPA)	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. È l'organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri. È stato sostituito da **AgID**.
Copia informatica di documento informatico	Documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza dei valori binari
Dispositivi sicuri per la generazione della firma Digitale	Mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 13 del DPCM 22/02/2013.
Dispositivi sicuri per la generazione della firma elettronica	Mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 12 del DPCM 22/02/2013.
Dispositivo sicuro per creazione della Firma	Dispositivo hardware in grado di proteggere in modo efficace la segretezza della chiave privata.
Documento analogico	Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Documento Informatico	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.

Firma digitale	Particolare tipo di firma elettronica basata su un certificato qualificato e su un sistema di chiavi crittografiche, pubblica e privata, correlate tra loro, consentendo al titolare, tramite chiave privata, e al destinatario, tramite chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di uno o un insieme di documenti informatici.
Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma Elettronica Avanzata (FEA)	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma Elettronica Qualificata	È un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata tramite un dispositivo sicuro per la creazione della firma.
Gestione informatica di documenti	Insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuato mediante sistemi informatici.
HASH	Funzione matematica che genera, a partire da un'evidenza informatica, un'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.
PAdes	Formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.
PDF	Standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).
RSA	Algoritmo di crittografia asimmetrica. Questo algoritmo si basa su utilizzo di chiavi pubblica e privata, serve a cifrare i dati biometrici e la chiave privata non è in possesso del Soggetto erogatore dei servizi di firma elettronica avanzata.
SHA-1	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 160 bit.
SHA-256	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 256 bit.
SHA-512	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 512 bit.
Signature Tablet	Dispositivo elettronico che si connette ad un computer ed è in grado di acquisire dati biometrici comportamentali e grafici di una firma autografa. I valori acquisiti sono coordinate x-y; tempo; pressione.
Soluzioni di firma elettronica avanzata	Soluzioni strumentali alla generazione e alla verifica della firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis del DL 235/2010.
Tablet	Dispositivo mobile in grado di acquisire i dati biometrici di una firma autografa, eventualmente per mezzo di specifiche penne elettroniche.

2.3 RIFERIMENTI NORMATIVI

Riferimenti	Descrizioni
1999/93/CE	Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa a una comune visione comunitaria in tema di firme elettroniche.
DPR 445/2000	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*".
D.Lgs. 196/2003	Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" o "**Codice**".
D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005 n. 82 "*Codice dell'amministrazione Digitale*".
D.Lgs. 159/2006	Decreto Legislativo 4 aprile 2006 n. 159 "*Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale*".
DPCM 12 ottobre 2007	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007 "*Differimento del termine che autorizza l'autodichiarazione circa a rispondenza ai requisiti di sicurezza a cui all'art. 13, comma4, del DPCM, pubblicato sulla Gazzetta Ufficiale del 30 ottobre 2003, n. 13*".
DPCM 30 marzo 2009	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 che abroga il DCPM del 13 gennaio 2004 "*Regole Tecniche*" in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
D.Lgs. 235/2010	Decreto Legislativo 30 dicembre 2010 n. 235 "*Modifiche ed integrazioni al D.Lgs. 7 marzo 2005 n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge n. 69 del 18 giugno 2009*".

D.Lgs. 83/2012	Decreto Legislativo 22 giugno 2012 n. 83 recante la sospensione di CNIPA e DigitPA che confluiscono nell'**Ag**enzia per l'**I**talia **D**igitale (AgID).
D.Lgs. 221/2012	Decreto Legislativo n. 221 del 17 dicembre 2012 "*Misure Urgenti per la crescita del Paese*". Il CAD, modificato nell'articolo 21, afferma il principio secondo cui "*l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria*".
DPCM 22 febbraio 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, lettera b), 35, comma 2, 36, comma 2, 3 e 71*".
Provvedimento 26 novembre 2014 del Garante per la protezione dei dati personali	Provvedimento "Provvedimento generale prescrittivo in tema di biometria" del 12 novembre 2014 Registro dei provvedimenti n. 513 del 12 novembre 2014 pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014 o "**Provvedimento**".

3 CONTESTO

HDI Assicurazioni S.p.A. ha deciso di implementare una soluzione di FEA mediante OTP al fine di acquisire in modalità digitale la sottoscrizione dei propri contratti.

3.1 GLI ATTORI

Nella realizzazione della soluzione FEA (nei due scenari contemplati) sono coinvolte le seguenti società:

- Plug-In S.r.l., che cura la realizzazione della soluzione applicativa integrata con la firma OTP (o anche "*Soluzione FEA*");
- Andxor Soluzioni Informatiche S.r.l., fornitore del servizio di certification authority interna necessario per il funzionamento della Soluzione FEA e soggetto che si occupa di apporre il certificato sui documenti da firmare previo ricevimento dell'OTP;
- Archiva S.r.l., che svolge l'attività di archiviazione e conservazione a norma dei documenti informatici sottoscritti con la Soluzione FEA.

3.2 I CONTATTI

HDI Assicurazioni S.p.A., soggetto erogatore del servizio FEA, mette a disposizione dei clienti i propri dati societari che saranno riportati nella loro completezza sia sul proprio sito-web che nell'informativa relativa al servizio.

Ragione Sociale	HDI Assicurazioni S.p.A.
Indirizzo sede	Via Abruzzi 10 – 00187 Roma
Legale Rappresentante	Sig. Roberto Mosca
Codice Fiscale	04349061004
Partita IVA	04349061004
Registro Imprese	04349061004 del Registro imprese di Roma
REA	RM-757172
Capitale Sociale (in Euro)	96.000.000€ I.V
Indirizzo E-Mail	hdi.assicurazioni@pec.hdia.it
Numero Telefonico	+39 06 421031
Numero FAX	+39 06 4120 3500
Indirizzo Sito istituzionale	https://www.hdiassicurazioni.it/home

Il Soggetto erogatore della Soluzione FEA può essere contattato ai seguenti recapiti per:

- 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;
- per revocare il consenso all'utilizzo della soluzione di firma elettronica avanzata.

Via postale	Via Abruzzi 10 – 00187 Roma
Via e-mail	hdi.assicurazioni@pec.hdia.it
Via telefonica	+39 06 421031
Via Fax	+39 06 4120 3500

4 LA SOLUZIONE FEA

La Soluzione FEA è stata progettata al fine di garantire l'ottemperanza rispetto ai requisiti fondamentali di garanzia per il firmatario, in particolare:

- identificabilità dell'autore della firma;
- integrità del documento;
- l'immodificabilità del documento informatico firmato.

Tutti questi requisiti vengono garantiti, oltre che dalle procedure operative di **HDI Assicurazioni S.p.A.** dalle soluzioni implementate per gestire il processo qui descritto.
I requisiti per definire una Firma Elettronica come Firma Elettronica Avanzata (FEA) e assumere quindi la valenza legale definita per questa tipologia di firma, sono elencati nelle Regole Tecniche Art. 56 comma l del d.P.C.M. 22 febbraio 2013. In questo capitolo si riassumono questi requisiti e si descrive come la soluzione implementata risponda positivamente a questi requisiti.

Caratteristiche ex art. 56 comma 1 d.P.C.M. 22 febbraio 2013	Adempimento
a) Identificazione del firmatario del documento	Il backoffice identifica il firmatario mediante un documento di riconoscimento in corso di validità che viene esibito e acquisito. Vedi par. 4.1.
b) Connessione univoca della firma con il firmatario	La firma OTP permette di stabilire una connessione univoca tra firmatario e documento firmato. Vedi par. 4.2.
c) Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima	La firma è apposta mediante OTP che viene rilasciato dal fornitore in ogni singola occasione di firma. Vedi par. 4.2.
d) Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma	Esiste sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Presso il sito dell'Agenzia per l'Italia Digitale (URL http://www.agid.gov.it/identitadigitali/firme-elettroniche/software-verifica) sono disponibili gratuitamente software per la verifica dell'integrità del documento in conformità alla delibera CNIPA del 21 maggio 2009 n. 45. Vedi par. 4.3.
e) Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	Il firmatario ha la visione completa del documento sottoposto alla firma e può scorrerlo. Oltre a ciò è previsto che il firmatario possa scaricare dal portale i documenti già sottoscritti (oltre che quelli in attesa di sottoscrizione. Vedi par. 4.4.
f) Individuazione del soggetto di cui all'art. 55, comma 2, lettera (a)	HDI Assicurazioni S.p.A. è identificabile come soggetto che eroga soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con i propri clienti.
g) Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati	Il documento generato nel processo di firma è nel formato PDF/A. Vedi par. 4.3.
h) Connessione univoca della firma al documento sottoscritto	Il servizio del fornitore di rilascio di un OTP e l'utilizzo da parte del firmatario del detto OTP rispetto a uno specifico documento garantiscono la connessione tra documento e firma. Vedi par. 4.2.

4.1 IDENTIFICAZIONE DEL FIRMATARIO

Il processo di adesione alla Soluzione FEA per la sottoscrizione dei documenti indicati sopra avviene previa esibizione e acquisizione del documento di riconoscimento in corso di validità del cliente ed espressa accettazione della Soluzione FEA da parte di quest'ultimo.

A seguito della verifica di completezza dei dati in possesso, dopo aver fornito informazioni esaustive dal punto di vista funzionale e normativo, il dipendente / collaboratore di **HDI Assicurazioni S.p.A.** autorizza il cliente all'utilizzo della Soluzione FEA.

Nell'ambito della sottoscrizione del contratto e di altri documenti mediante Soluzione FEA il cliente è chiamato ad accettare i termini e le condizioni della soluzione FEA mediante OTP.

La corretta identificazione del cliente e l'espletamento degli obblighi informativi sono compiti a carico del backoffice.

Al fine di dare evidenza di quanto previsto, viene conservata copia del documento di riconoscimento, in allegato al documento di accettazione del servizio, per almeno 20 anni.

Il cliente può sempre rifiutare la soluzione FEA e optare per la sottoscrizione olografa dei contratti e documenti che gli sono presentati da **HDI Assicurazioni S.p.A..**

4.2 FIRMA DEL DOCUMENTO

Per la sottoscrizione di documenti digitali da parte del cliente, è necessario che il dipendente / collaboratore di **HDI Assicurazioni S.p.A.** metta a disposizione il documento mediante la soluzione di firma, mostrandolo sullo schermo.

Il cliente può attivare il servizio di firma con il comando "firma". All'utilizzo di tale comando il portale richiede al fornitore presso cui è creata la certification authority interna (e quindi presso cui è presente un certificato riconducibile al cliente) il rilascio di un OTP. Il fornitore invia l'OTP al cliente mediante il canale concordato in fase di adesione al servizio. Il cliente, ricevuto l'OTP, lo inserisce in un apposito spazio proposto dalla soluzione di firma. La soluzione finalizza il processo di firma inviando il certificato rispetto al quale è stato digitato l'OTP e il documento stesso in modo che il fornitore del servizio provveda alla apposizione della firma, ovvero del certificato.

Il documento, su cui il fornitore del servizio ha apposto il certificato del cliente, viene instradato al sistema di conservazione sostitutiva gestito da Archiva S.r.l..

4.3 INTEGRITÀ E AUTENTICITÀ DEL DOCUMENTO

La verifica dell'integrità ed autenticità del documento può essere svolta da un qualsiasi software di verifica conforme al CAD. Mediante tale software è possibile accertare che il documento non sia stato alterato successivamente alla apposizione della firma.

Il documento è sempre in disponibilità del cliente (come indicato al punto seguente) e può verificare la conformità del documento firmato con OTP a quanto presentatogli.

4.4 DISPONIBILITÀ DEI DOCUMENTI

HDI Assicurazioni S.p.A. rende disponibile al cliente tutta la documentazione da questi firmata alla mail conferita in fase di adesione al servizio. Il cliente potrà contattare **HDI Assicurazioni S.p.A.** per ricevere assistenza.

5 IL PROCESSO DI CONSERVAZIONE

Il servizio di conservazione sostitutiva è gestito da Archiva S.r.l.. I documenti prodotti dalla soluzione FEA sono trasmessi, secondo politiche stabilite di intesa con il fornitore, al fornitore stesso, perché provveda alla conservazione sostitutiva in osservanza di quanto descritto nel manuale della conservazione sostitutiva.

6 TUTELA ASSICURATIVA

Le Regole Tecniche di cui al d.P.C.M. 22 febbraio 2013, prevedono che sia stipulata una copertura assicurativa a garanzia del firmatario. Il soggetto che eroga soluzioni di Firma Elettronica Avanzata si deve impegnare 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.

HDI Assicurazioni S.p.A. si è dotata di una adeguata copertura assicurativa per la responsabilità civile avente massimali non inferiori a quelli richiesti dalla normativa vigente.

7 SERVIZIO DI REVOCA

Il processo di FEA adottato da **HDI Assicurazioni S.p.A.** permette la revoca del consenso all'utilizzo della Soluzione FEA tramite apposita richiesta scritta da parte del cliente. In caso di revoca la soluzione FEA non potrà più essere utilizzata. Il cliente potrà contattare il **HDI Assicurazioni S.p.A.** per ricevere assistenza in merito alle richieste di revoca del consenso.

Il *form* da compilare è allegato al presente documento quale Allegato 1.
Al ricevimento di una richiesta di revoca viene modificato lo stato di abilitazione alla firma del singolo utente con la conseguenza che è inibita ogni ulteriore sottoscrizione di documenti mediante la Soluzione FEA.

ALLEGATO 1: RECESSO DALLA FEA

Oggetto: esercizio del diritto di revoca del consenso all'utilizzo dalla firma elettronica avanzata

Il/la sottoscritto/a, ……., C.F. ....., nato a .....(....) il ..../..../....., residente in .....(....) alla via ..... n. ....., con la presente intende comunicare la propria revoca del consenso all'utilizzo della firma elettronica avanzata dallo stesso precedentemente rilasciato.

La presente richiesta di revoca non ha alcun effetto sulla validità dei documenti già da me sottoscritti, fino alla data della presente comunicazione, mediante firma elettronica avanzata.

Allega a tal fine copia di un documento di riconoscimento in corso di validità.

_____

Luogo Data

_____

Firma

Allegato: documento di riconoscimento in corso di validità