Cap. soc. 10.000 € i.v.
Reg. Imp. Palermo
P.iva 06640050826
REA 405032
RUI B000587008
Lloyd's OMC 191394

Plurima
Servizi Assicurativi s.r.l.

Via Enrico Albanese, 114
90139 Palermo

Tel. +39 091 8486320
Fax. +39 091 6195495
Cel. +39 338 5372085

Mail: info@plurima.net
Pec: plurima.net@pec.it

Informativa sulla soluzione di

Firma Elettronica Avanzata

erogata da Plurima srl

SOMMARIO

Scopo

Il presente documento illustra le caratteristiche della firma elettronica erogata da Plurima tramite la piattaforma eSignAnywhere (eSAW) del Qualified Trust Service Provider Namirial e descrive la relativa efficacia probatoria ai sensi del Decreto Legislativo n.82 del 7 marzo 2005 recante "Codice dell'Amministrazione Digitale" e s.m.i. e del Regolamento (UE) n. 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.

Riferimenti tecnici e normativi

Plurima, nell'erogazione dei suoi servizi, è conforme alle normative e regolamenti europei e nazionali applicabili. Tutti i regolamenti e le leggi applicabili sono riportati nella seguente tabella ed al personale del Certificatore, e a chi collabora a vario titolo con lo stesso, vengono fornite adeguate policy per il rispetto di tali norme e regolamenti.

NUM	NORMATIVA	DESCRIZIONE
[01]	D.Lgs. 4/4/2006 n. 159	Decreto Legislativo 4 aprile 2006 n. 159 *Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.*
[02]	DPCM 12/10/2007	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007 *Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'art. 13, comma 4, del DPCM", pubblicato sulla GU 30 ottobre 2003, n. 13*
[03]	D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005, n. 82 *Codice dell'Amministrazione Digitale (CAD)*, con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.
[04]	CNIPA/CR/48	Circolare CNIPA 6 settembre 2005 *Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.*
[05]	DPCM 22/02/2013	Decreto del Presidente del Consiglio dei Ministri 22 Febbraio 2013. *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.*
[06]	D.Lgs. 196/2003	Decreto Legislativo 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali.*
[07]	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*
[08]	CNIPA 45/2009	CNIPA Deliberazione n. 45 del 21 maggio 2009 e successive modificazioni. *La presente deliberazione ha abrogato: Deliberazione CNIPA 17 febbraio 2005 n. 4 Deliberazione CNIPA 18 maggio 2006 n. 34 Regole per il riconoscimento*

		e la verifica del documento informatico.
[09]	CNIPA Limiti d'uso nei CQ	Limiti d'uso garantiti agli utenti ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 21 maggio 2009, n. 45
[10]	RFC 3647	Certificate Policy and Certification Practices Framework
[11]	RFC 5280	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[12]	ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates
[13]	ETSI TS 101 862	Qualified Certificate profile
[14]	ETSI TS 102 023	Policy requirements for time-stamping authorities
[15]	ITU-T X.509 ISO/IEC 9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
[16]	DigitPA DC 69/2010	DigitPA - Determinazione Commissariale n. 69/2010 Modifica della Deliberazione 21 maggio2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica amministrazione, recante "Regole per il riconoscimento e la verifica del documento informatico", pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana – serie generale – n. 282.
[17]	CAD 30/12/2010 n.235	Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
[18]	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 attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione".
[19]	D. Lgs. 22 giugno 2012, n. 83	Misure urgenti per le infrastrutture l'edilizia ed i trasporti. art. 22 DigitPA e l'Agenzia per la diffusione delle tecnologie per l'innovazione sono soppressi. I due enti confluiscono nell' Agenzia per l'Italia Digitale.
[20]	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[21]	RFC 3161	Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF - Agosto 2001.
[22]	DM 9/12/2004	Decreto del Ministero dell'Interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze 9 Dicembre 2004. *Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale*

		dei Servizi" pubblicato nella Gazzetta Ufficiale n.296, 18 dicembre 2004.
[23]	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[24]	ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[25]	ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[26]	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[27]	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[28]	ETSI EN 319 411-3	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
[29]	ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[30]	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[31]	ETSI EN 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[32]	ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[33]	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[34]	eIDAS n. 910/2014	Regolamento eIDAS (electronic IDentification Authentication and Signature) UE n° 910/2014 sull'identità digitale.
[35]	eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[36]	QSCD	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
		COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications

[37]	TSL	and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[38]	Electronic Signature Formats	COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Definizioni ed acronimi

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

TERMINE O ACRONIMO	SIGNIFICATO
AgID	Agenzia per Italia Digitale [19].
Autorità per la marcatura temporale [Time-stamping authority]	È il sistema software/hardware, gestito dal Certificatore, che eroga il servizio di marcatura temporale.
Certificato digitale, Certificato qualificato	È un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica). Vedi [01] Art.28
Certificatore [Certification Authority]	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiave privata	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso dal Titolare che la utilizza per firmare digitalmente i documenti.
Chiave pubblica	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata, ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.
CIE	Carta d'Identità Elettronica, è il documento di identificazione destinato a sostituire la carta d'identità cartacea sul territorio italiano.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, l'Organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
CNS	Carta Nazionale dei Servizi
CRL – Lista di revoca e sospensione dei certificati	È una lista di certificati che sono stati resi "non validi" dal certificatore prima della loro naturale scadenza. La revoca rende i certificati "non validi" definitivamente. La sospensione rende i certificati "non validi" per un tempo determinato.
CRS	Carta regionale dei servizi
CUC	È il Codice Univoco Certificato ed è indicato sulla Richiesta di Registrazione ed inserito nel certificato. Identifica in modo

	univoco il certificato emesso dal Certificatore.
CUT	È il Codice Univoco Titolare ed è indicato sulla Richiesta di Registrazione
Destinatario	È il soggetto a cui è destinato il documento e/o di una evidenza informatica firmata digitalmente.
Dispositivo Sicuro per la Creazione della Firma	Dispositivo hardware capace di proteggere efficacemente la segretezza della chiave privata.
Giornale di controllo	Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di base.
Hash (o funzione di hash)	una 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
Impronta (o impronta hash)	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
IUT	Identificativo Univoco del Titolare, diverso per ogni certificato emesso.
LDAP [Lightweight Directory Access Protocol]	È un protocollo standard per l'interrogazione e la modifica dei servizi di directory (segue gli standard X.500).
LRA	È la persona fisica o giuridica delegata dal Certificatore allo svolgimento delle operazioni di emissione dei Certificati, secondo le modalità individuate e descritte nel presente Manuale. L'ente deve aver preventivamente stipulato accordi di servizio con il Certificatore. L'LRA può avvalersi di RAO per le operazioni identificazione, registrazione ed emissione.
Marca temporale [Timestamp]	È il riferimento temporale che consente la validazione temporale.
Manuale Operativo	È il documento pubblico depositato presso AgID che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
OID [Object Identifier]	È una sequenza di numeri, registrata secondo lo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
OCSP [Online Certificate Status Protocol]	È un protocollo che consente di verificare la validità di un certificato in tempo reale.
Organizzazione	Società o altro soggetto giuridico che gestisce l'applicazione in cui viene integrata la piattaforma di firma elettronica Namirial (eSAW) ai fini dell'erogazione delle firme elettroniche per la dematerializzazione dei flussi documentali.
OTP	One-Time-Password. Codice numerico generato da un dispositivo fisico utilizzato per effettuare un'autenticazione a due fattori.
PIN [Personal Identification Number]	Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso
PUK	Codice personalizzato utilizzato dal Titolare per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.
RA	Registration Authority, soggetto che esegue l'identificazione dei Richiedenti dei certificati qualificati applicando le procedure definite dal Certificatore.

RAO	È soggetto espressamente delegato da Namirial allo svolgimento, per conto di quest'ultima, delle Operazioni di identificazione e registrazione del Titolare, nonché l'emissione dei Certificati. Tale soggetto deve appartenere ad una LRA.
Referente	È la persona fisica incaricata alla predisposizione di ogni documento necessario per il ciclo di vita della firma e che mantiene i contatti con il Certificatore.
Registro dei certificati	È la lista dei certificati emessi dal Certificatore, nella lista sono inclusi i certificati revocati e sospesi, accessibile telematicamente.
Revoca del certificato	È l'operazione con cui il Certificatore annulla la validità del certificato, prima della sua naturale scadenza, da un dato momento, non retroattivo, in poi.
Richiedente	È il soggetto che richiede al Certificatore il rilascio di certificati qualificati. Se il Soggetto è diverso dal Titolare del Certificato l'identità del Richiedente verrà inserito nel campo Organization del certificato X.509.
RSA	Algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SHA-1 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una impronta digitale di 160 bit.
SHA-256 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una impronta digitale di 256 bit.
Sospensione del certificato	È l'operazione con cui il Certificatore sospende la validità del certificato, prima della sua naturale scadenza, per un periodo di tempo definito, non retroattivo.
Terzo Interessato	È la persona fisica o giuridica che dà il consenso, in conformità alle norme, al rilascio di certificati qualificati nei quali sia riportata l'appartenenza ad una organizzazione ovvero eventuali poteri di rappresentanza o titoli e cariche rivestite. Ha il diritto/dovere di richiedere la revoca o sospensione del certificato nel caso risultano modificati i requisiti in base ai quali lo stesso è stato rilasciato
Titolare	È la persona fisica, identificata dal Certificatore, cui è attribuita la firma digitale.
Token	È il dispositivo fisico (smart card, o chiave USB) che contiene la chiave privata del Titolare.
X.509	È uno standard ITU-T per le infrastrutture a chiave pubblica (PKI)

Local Registration Autority

Plurima è una società di intermediazione assicurativa che eroga soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali; Plurima agisce in qualità di Local Registration autority delegata dall'Ente Certificatore allo svolgimento delle operazioni di emissione dei Certificati, secondo le modalità individuate e descritte nel presente Manuale.

Certification Authority

Namirial è una società IT di software e servizi ed è un Qualified Trust Service Provider che fornisce Trust Services come Firme Elettroniche, Firme Elettroniche Avanzate (Grafometriche e con Strong Authentication), Firme Elettroniche Qualificate (anche Digitali), Posta Elettronica Certificata, Fatturazione Elettronica e Conservazione Sostitutiva a più di 500.000 utenti.

I gruppi di utenti serviti da Namirial si articolano in diversi settori, tra cui: Ordini Professionali di cui fanno parte Medici, Avvocati, Ingegneri, Consulenti del Lavoro, Dottori Commercialisti, Strutture Cooperative e Imprenditoriali tra cui la Media e Piccola Impresa, la Pubblica Amministrazione, i Trasporti, le Banche e le Assicurazioni e le aziende di classe enterprise.
La sede principale è a Senigallia con ulteriori uffici in Italia e sedi in Austria e Romania, da cui vengono serviti utenti situati in tutta l'Europa, gli Stati Uniti, il Medio Oriente e l'Africa.

Tipologia di Firma Elettronica

Firma Elettronica Avanzata

La soluzione di firma implementata da Plurima all'interno dei propri sistemi informatici è una Firma Elettronica Avanzata, avente le seguenti caratteristiche:

- E' possibile firmare i documenti utilizzando meccanismi di autenticazione tramite **codice OTP inviato al numero di cellulare** dell'utente;
- All'interno della firma, e quindi protette da quest'ultima, vengono raccolte tutte le informazioni collegate al firmatario (**nome, mail, indirizzo IP, timestamp**);
- Le operazioni eseguite sono irrobustite nel fattore di autenticazione inviato al numero di cellullare dell'utente;
- Per la firma viene utilizzato un **certificato elettronico di servizio**, integrato nella piattaforma e rilasciato dalla CA Qualificata Namirial. Il certificato è presente all'interno degli store Europei e del software di gestione dei PDF, Adobe, e serve a garantire **l'integrità e immodificabilità del documento**
- La firma viene effettuata **dinnanzi ad un incaricato** (operatore che procede all'identificazione del soggetto sottoscrittore) il che rende il processo ancora più robusto da un punto di vista della non ripudiabilità del documento sottoscritto.

La Firma Elettronica Avanzata è definita dalla norma (Art 3, comma 11 dell'eIDAS) come "una firma elettronica che soddisfi i seguenti requisiti:

a) È connessa unicamente al firmatario
b) è idonea a identificare il firmatario
c) è creata 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
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati."

Questo tipo di firma risulta essere quindi un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica ad un documento informatico, garantisce integrità (consentendo di rilevare se i dati sono stati successivamente modificati) e autenticità del documento sottoscritto. La sua creazione presuppone l'utilizzo di dati per la creazione di una firma, sui quali il firmatario mantiene il controllo esclusivo. Quest'ultimo elemento assicura la connessione univoca con il firmatario e quindi la paternità giuridica del documento.
La firma elettronica avanzata presenta dei caratteri peculiari che la differenziano marcatamente rispetto alle altre tipologie di firma. In primo luogo, la normativa non vincola la firma elettronica avanzata a particolari standard tecnici o determinati software. Conseguentemente non esiste uno standard di firma elettronica avanzata, ma sono

ipoteticamente possibili soluzioni di firma anche molto diverse tra loro, purché rispettino i requisiti richiesti dalla legge:

1) capacità di assicurare integrità ed autenticità del documento sottoscritto;
2) controllo esclusivo dei dati per la creazione della firma da parte del firmatario.

Gli strumenti più diffusi sono quelli che utilizzano nei processi di sottoscrizione le password temporanee (OTP) o i dati biometrici, tra cui assumono un posto di rilievo le soluzioni di firma grafometrica. La FEA è pertanto una tipologia di firma tecnologicamente neutra: non si fa riferimento alla tecnologia utilizzata, ma deve soddisfare determinati requisiti previsti dal Regolamento eIDAS e disciplinati nelle Regole Tecniche di cui al DPCM 22 febbraio 2013, Titolo V.

Valore legale dei documenti generati

La firma elettronica avanzata SMS generata è realizzata tramite un processo articolato secondo alcuni step funzionali di seguito elencati; in questo processo il requisito di riconducibilità della firma al titolare viene garantita dal possesso del cellulare e dall'invio di un codice OTP su tale numero.

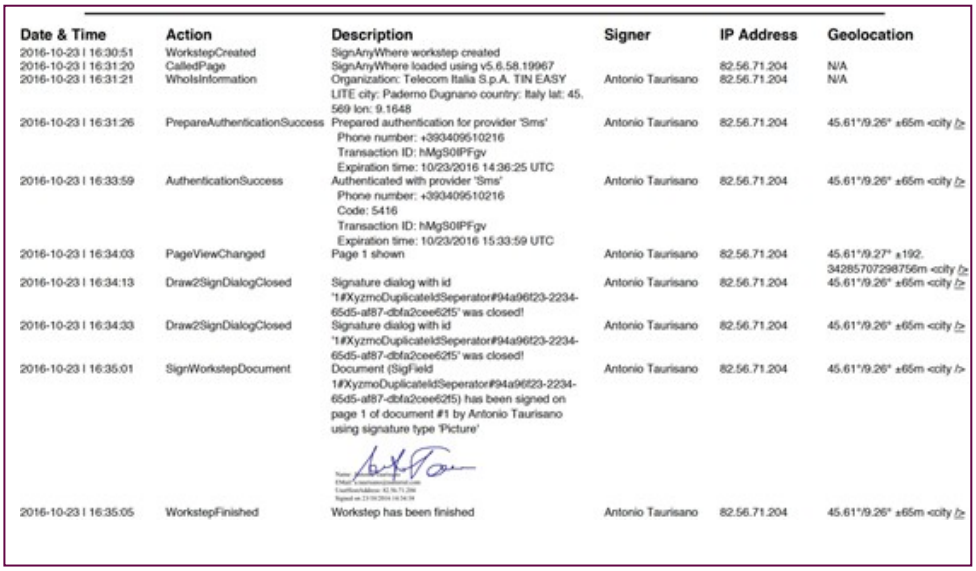
Entrando nel dettaglio, il meccanismo si sviluppa secondo le seguenti macro-fasi:

a) Identificazione dell'utente sottoscrittore da parte di un operatore
b) Acquisizione del documento da firmare
c) Invio di un codice OTP al numero di cellullare del Titolare
d) Login dell'utente sulla piattaforma eSAW tramite l'inserimento del codice OTP ricevuto nel cellulare
e) Registrazione dell'avvenuto login all'interno dell'audit log della piattaforma eSAW
f) Visualizzazione del documento
g) Firma del Titolare tramite click su campo firma
h) Calcolo dell'impronta HASH SHA-256 del documento da sottoscrivere
i) Creazione di una firma elettronica avanzata in formato PAdES basata su un certificato di firma elettronica avanzata di servizio installato all'interno della piattaforma eSAW.

Grazie al processo sopradescritto, l'utente può apporre la propria firma solo se prima è riuscito ad autenticarsi tramite il codice OTP inviato sul suo cellullare.

L'informazione del login, in combinazione delle restanti informazioni collezionate dalla piattaforma eSAW, sono inserite all'interno dell'Audit Trail (Log) che viene regolarmente firmato a garanzia dell'integrità

Le informazioni contenute nell'Audit Trail possono essere successivamente prodotti in tribunale in caso di disconoscimento della firma da parte dell'utente.



Date & Time	Action	Description	Signer	IP Address	Geolocation
2016-10-23 I 16:30:51	WorkstepCreated	SignAnyWhere workstep created			
2016-10-23 I 16:31:20	CalledPage	SignAnyWhere loaded using v5.6.58.19967		82.56.71.204	N/A
2016-10-23 I 16:31:21	WhoIsInformation	Organization: Telecom Italia S.p.A. TIN EASY LITE city: Paderno Dugnano country: Italy lat: 45.569 lon: 9.1648	Antonio Taurisano	82.56.71.204	N/A
2016-10-23 I 16:31:26	PrepareAuthenticationSuccess	Prepared authentication for provider 'Sms' Phone number: +393409510216 Transaction ID: hMgS0IPFgv Expiration time: 10/23/2016 14:36:25 UTC	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:33:59	AuthenticationSuccess	Authenticated with provider 'Sms' Phone number: +393409510216 Code: 5416 Transaction ID: hMgS0IPFgv Expiration time: 10/23/2016 15:33:59 UTC	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:34:03	PageViewChanged	Page 1 shown	Antonio Taurisano	82.56.71.204	45.61°/9.27° ±192.34285707298756m <city />
2016-10-23 I 16:34:13	Draw2SignDialogClosed	Signature dialog with id '1#XyzmoDuplicateIdSeperator#94a96f23-2234-65d5-af87-dbfa2cee62f5' was closed!	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:34:33	Draw2SignDialogClosed	Signature dialog with id '1#XyzmoDuplicateIdSeperator#94a96f23-2234-65d5-af87-dbfa2cee62f5' was closed!	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:35:01	SignWorkstepDocument	Document (SigField 1#XyzmoDuplicateIdSeperator#94a96f23-2234-65d5-af87-dbfa2cee62f5) has been signed on page 1 of document #1 by Antonio Taurisano using signature type 'Picture'	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />
2016-10-23 I 16:35:05	WorkstepFinished	Workstep has been finished	Antonio Taurisano	82.56.71.204	45.61°/9.26° ±65m <city />

Efficacia probatoria della firma elettronica avanzata

L'utilizzo di un codice OTP inviato tramite SMS al numero personale del titolare e l'utilizzo di una firma elettronica avanzata basata su un certificate emesso e gestito da CA Accreditata (c.d. terza parte fidata), permette di soddisfare pienamente i requisiti richiesti dalla normativa per la FEA, ovvero:

a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
h) la connessione univoca della firma al documento sottoscritto.

Manuale Operativo

Plurima offre la modalità per realizzare la firma elettronica avanzata FEA online da remoto, cioè sfruttando il canale internet. Nella sezione seguente viene descritta la soluzione.

Descrizione sistema FEA online da remoto

Il sistema di Firma è basato sulla piattaforma eSAW utilizzata come sistema centrale trustato, utilizzato per l'erogazione di firme elettroniche semplici, avanzate e qualificate.
Il sistema eSAW è progettato per garantire massimi livelli di sicurezza nonché per rispettare pienamente i requisiti previsti per la Firma Elettronica ai sensi eIDAS.
Attraverso il protocollo HTTPS ogni comunicazione dal Sistema di Firma e verso il Sistema di Firma è autenticata e protetta.

Il Sistema eSAW genera un Log di tutti i passi effettuati e gli eventi registrati, includendo anche gli indirizzi IP e la eventuale geolocalizzazione del firmatario.
L'integrità del log è protetta da sistemi di crittografia basati su firme elettroniche e marche temporali. L'infrastruttura è quindi completata da un front end securizzato di gestione del servizio di firma.

Sistema di autenticazione

La sicurezza del sistema di autenticazione per la FEA online da remoto è basata su:

a. L'accesso ad un account personale protetto da password, ed in particolare l'indirizzo email a cui vengono inviati i link necessari per accedere alla procedura di firma sulla piattaforma eSaw;
b. Una One Time Password (OTP) inviata nel numero di cellullare personale dell'utente.

La chiave privata ed il certificato di firma sono utilizzati esclusivamente per l'apposizione della firma elettronica avanzata. La firma viene valorizzata con dati peculiari dell'utente (username dell'account, codice OTP inviato nel numero di cellulare del cliente) che, nel loro complesso ed in virtù del processo implementato dalla piattaforma, risultano collegati biunivocamente al legittimo utente e al documento sottoscritto.

Attivazione del servizio

Il servizio di firma elettronica avanzata viene attivato dal personale e dagli intermediari assicurativi partner di Plurima presso cui il Titolare risulta essere cliente.

In fase di attivazione del servizio, il soggetto incaricato provvederà ad:

a. Identificare il Titolare;
b. A farsi rilasciare dal Titolare un documento di identità in corso di validità;
c. A rendere disponibile al Titolare la documentazione per attivare il servizio di firma elettronica avanzata;
d. A far accettare al Titolare l'informativa per attivare il servizio di firma elettronica avanzata.

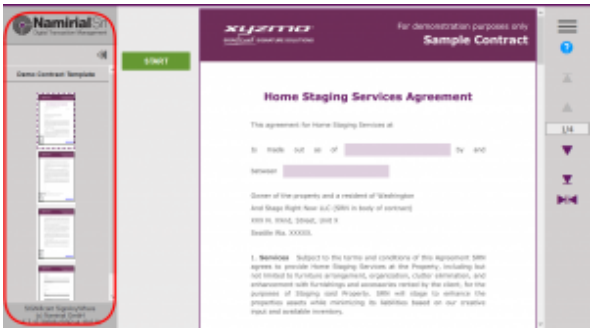
Processo di attivazione

Ultimata la fase di attivazione/registrazione, al Titolare verrà:

a. Reso disponibile il documento da firmare con FEA attraverso l'account previsto al punto 3;
b. Equipaggiato di una password personale, solo nel caso di portale con area riservata dal personale della Filiale di <Organizzazione>;
c. Inviata una One Time Password (OTP) al numero di cellulare indicato.

Come procedere alla firma

Per eseguire la firma on line è necessario che il Titolare acceda all'account, recuperi il link al documento da firmare ed inserisca l'OTP nella sezione di firma.



Conservazione dei documenti

Il documento informatico sottoscritto viene inviato tramite canali protetti al "Sistema documentale" e all'Archivio di conservazione a norma di Plurima per la relativa conservazione.

Adesione al servizio di FEA

L'adesione al servizio sarà manifestata dal Titolare mediante la firma del seguente modulo di adesione, a cui andrà allegato il documento di identità del Titolare:

Modulo di adesione

Il sottoscritto Nome, Cognome (Titolare), richiede di poter sottoscrivere con Firma Elettronica Avanzata ("FEA") tutta la documentazione per la quale Plurima renderà possibile la sottoscrizione con detta modalità di firma, tramite infrastruttura tecnologica e software forniti dalle società incaricate da Plurima del servizio.
Il/la sottoscritto/a (Titolare) prende atto che la FEA e il suo utilizzo sono disciplinati dalle norme e dai principi di seguito riportati, che dichiara di conoscere e che sottoscrive ed approva integralmente.

1. Per FEA si intende la Firma Elettronica Avanzata apposta dal Titolare con identificazione tramite OTP inviata al cellulare del Titolare;
2. Il Titolare autorizza Plurima ad acquisire i dati relativi al proprio numero di cellulare ed eventuali altri dati disponibili (indirizzo IP, caratteristiche del software o hardware in uso, geolocalizzazione, etc…) e conservarli in un tracciato denominato dell'Audit Trail; i codici e le procedure di sicurezza per l'accesso ai dati completi della sottoscrizione sono conservate da uno o più soggetti terzi appositamente incaricati che forniscono i dati di firma esclusivamente nei casi in cui ciò sia indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e/o su richiesta delle Autorità competenti e/o su richiesta del titolare dei dati stessi. Il trattamento dei dati sensibili del Titolare che Plurima acquisisce, in relazione a specifiche operazioni, prodotti e servizi dallo stesso richiesti, avviene nel rispetto degli obblighi di riservatezza e nell'osservanza del Codice in materia di Protezione dei Dati Personali (D.Lgs 30 giugno 2003, n. 196).

3. Il documento informatico sottoscritto con FEA garantisce l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ed ha l'efficacia prevista dal Codice dell'Amministrazione Digitale (D.lgs 7 marzo 2005 n. 82, cd. CAD).
4. La FEA è sottoposta alla norme in materia di Firma Elettronica Avanzata stabilite dal Codice dell'Amministrazione Digitale (D.lgs 7 marzo 2005 n. 82, cd. CAD), cosi come modificato dal D.lgs 30 dicembre 2010 n. 235, dalle Regole Tecniche dettate ai sensi dell'art. 71 del CAD e successive modificazioni.
5. Il documento informatico sottoscritto con FEA viene archiviato digitalmente nel sistema informatico di Plurima e/o delle società incaricate da Plurima del Servizio e il Titolare può richiederne in ogni momento un duplicato informatico per il periodo in cui Plurima è tenuta a conservare per legge la documentazione cosi sottoscritta. Plurima fornirà al Titolare il documento informatico nei modi volta per volta concordati con il Titolare.
6. Il Titolare può richiedere in ogni momento il rilascio di copia cartacea dei documenti informatici da lui sottoscritti.
7. Plurima per motivi tecnici, di sicurezza o di forza maggiore può in ogni momento sospendere o interrompere la possibilità per il Titolare di utilizzo della FEA
8. Plurima, per ragioni operative e di sicurezza, potrà chiedere la sottoscrizione di una nuova richiesta di utilizzo della Firma Elettronica Avanzata alla accensione/apertura di ogni nuovo rapporto contrattuale.
9. In caso di documenti che prevedano firme congiunte (a qualsiasi titolo), i Titolari possono utilizzare la Firma Elettronica Avanzata solo se tutti hanno accettato detta modalità di firma.
10. In ogni momento il Titolare, se lo desidera, può ottenere copia della presente richiesta da Plurima.
11. Il Titolare conserva la facoltà di sottoscrivere la documentazione su supporto cartaceo apponendo la propria tradizionale firma non elettronica.
12. Plurima si riserva di rendere disponibile la Firma Elettronica Avanzata per la sottoscrizione di contratti relativi a prodotti e servizi offerti – tramite Plurima stessa - da Società e/o Imprese di assicurazione terze che abbiano conferito specifico incarico in tal senso a Plurima.
13. In ogni momento il Titolare può revocare il consenso all'utilizzo della Firma Elettronica Avanzata mediante richiesta da presentarsi periscritto con raccomandata A.R. a Plurima srl, Via E. Albanese 114, 90139 Palermo o mediante Posta Elettronica Certificata a plurima.net@pec.it, avendo cura di specificare il proprio codice fiscale ed il rapporto contrattuale di riferimento. Le comunicazioni fatte con altre modalità ed in assenza dell'indicazione dei dati sopra specificati, non produrranno l'effetto richiesto. Plurima provvederà a disattivare la modalità di Firma Elettronica Avanzata entro i sette giorni lavorativi successivi a quello in cui ha ricevuto la comunicazione di revoca. Detto termine è posto ad esclusiva tutela di Plurima, che vi provvederà pertanto in base alle proprie modalità organizzative.
14. Plurima ha stipulato, in conformità alla normativa vigente, una polizza assicurativa con una Compagnia assicuratrice a tutela dei danni eventualmente derivanti da problemi tecnici riconducibili all'utilizzo della Firma Elettronica Avanzata, con massimale pari ad 1.500.000 euro.
15. Per quanto qui non espressamente previsto si applicano le disposizioni contrattuali e le condizioni economiche previste per i rapporti e le operazioni per i quali Plurima renderà possibile l'utilizzo della FEA.