Manuale Operativo

Manuale Operativo
Firma Elettronica Avanzata FEA
Per D.A.S.

Data	21/04/2020
Versione	2
Stato	Prima stesura
Numero del documento	MOFEA_RG-Aprile 2020
Nome del documento	Manuale operativo FEA

Indice generale

INTRODUZIONE

Nel corso del 2018, D.A.S. S.p.A., ha deciso di dotarsi di una soluzione di firma dei contratti assicurativi proposti al mercato che rispecchi la normativa vigente CAD e sia indipendente dai device utilizzati per la firma.

Si precisa che il processo di firma sarà un processo FEA (Firma Elettronica Avanzata).

Nel rispetto di quanto previsto dalle "Regole Tecniche" viene redatto questo documento "Manuale Operativo FEA per D.A.S." limitatamente al progetto e utilizzatore D.A.S..

Il "Manuale Operativo" è il documento pubblicato sul proprio sito internet che:

- ✓ definisce le procedure applicate;
- ✓ le caratteristiche del sistema e della soluzione;
- ✓ le tecnologie utilizzate.

Il tutto al fine di rispondere a quanto espresso nel "Decreto del Presidente del Consiglio dei Ministri" (DPCM) in emanazione delle Regole Tecniche approvato in data 22 febbraio 2013.

Nel proseguo si illustrano i punti fondamentali del processo, il rispetto della normativa, gli attori coinvolti descrivendone ruoli e responsabilità.

VERSIONI

VERSIONE DEL DOCUMENTO

Versione:	000 – 2019
Data:	15 Dicembre 2019
Indicazioni:	Seconda stesura
Modifiche:	Adeguamento a firma OTP

REFERENTI

Versione:	000-2019	
Redatto da:	Romano Garavaglia	
Verificato da:	Silvia Nuvolini	
Approvato da:	Paola Sandri	
Responsabile del documento:	D.A.S. Difesa Automobilistica Sinistri S.p.A. di Assicurazione Tel. +39 045 8372611 PEC: dasdifesalegale@pec.das.it	

RIFERIMENTI NORMATIVI

Item	Riferimenti	Descrizioni
(1)	**Testo Unico -DPR 445/2000 e successive modificazioni ed integrazioni**	Decreto del Presidente della Repubblica 28 dicembre 2000, n.445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
(2)	**CAD - D.Lgs. 82/2005 e successive modificazioni ed integrazioni**	Decreto Legislativo 7 marzo 2005 N. 82 "Codice dell'amministrazione Digitale".
(3)	**DPCM 22/02/2013 Nuove regole Tecniche e successive modificazioni e integrazioni**	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, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 coma 3, 32 comma 3 lettera b, 5 comma 2, 36 comma 2 e 71" (del CAD ndr).
(4)	**Deliberazione CNIPA n° 45 e successive modificazioni e integrazioni**	Deliberazione CNIPA 21 maggio 2009, n° 45 "Regole per il riconoscimento e la verifica del documento informatico"
(5)	**DPCM 19/07/2012 e successive modificazioni e integrazioni**	Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012 "Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del presidente del consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma".
(6)	**Regolamneto (UE) n° 910/2014 (eIDAS) e successive modificazioni e integrazioni**	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.
(7)	**Regolamento (UE) n° 679/2016 (GDPR) e successive modifiche e integrazioni**	Regolamento (UE) n° 679/2016 del del Parlamento e del Consiglio Europeo del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

GLOSSARIO DI ACRONIMI E TERMINI

Termine o Acronimo	Significato
AgID	Agenzia per l'Italia Digitale (già CNIPA e DigiPA): www.agid.gov.it. D'ora in avanti solo *Agenzia*
Audit Log	La piattaforma eSAW genera un Log di tutti i passi effettuati con inclusi gli indirizzi IP e l'eventuale geolocalizzazione del firmatario. L'integrità dei Log è protetta da sistemi di crittografia basati su firme elettroniche e marche temporali. L'infrastruttura è poi completata da un front enf securizzato di gestione del servizio di firma.
TSP	Trust Service Provider – Prestatore di servizi fiduciari (già *Certificatore*). Persona fisica o giuridica abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Certificato re Accreditato	TSP presente nell'elenco pubblico dei Certificatori Accreditato tenuto da AgID (nelle more del regolamento (UE) n° 910/2014
Documento Informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento Analogico	Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
eSAW (Piattaforma)	eSignAnyWhere (eSAW) è una piattaforma integrata per l'apposizione di firme elettroniche su varie tipologie di documenti e contratti. Lo strumento consente di progettare in maniera molto semplice una pratica (vale a dire uno o più documenti PDF) da far sottoscrivere ad uno o più destinatari. I destinatari possono visulaizzare e firmare i documenti su qualsiasi dispositivo utilizzando diverse tipologie di firma.
ETSI	European Telecommunications Standards Institure
FEA	Firma Elettronica Avanzata – ex Art. 26 Reg. UE 910/2014 (eIDAS), la FEA soddisfa 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 d) È collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni succesiva modifica di tali dati
HASh (o funzioni di Hash)	Una funzione matematica che genra, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a paryire da questa,

	ricostruire l'evidenza informatica originaria e genera 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 di una opportuna funzione di Hash
HSM (Dispositivo Sicuro per la creazione della Firma)	Hardware Security Module – Insieme di Hardware e Software che realizza dispositivi sicuri per la generazione delle firme, in grado di gestire in modo sicuro una o più copie di chiave crittografiche
CA	Certification Authority: Entità del PKI che rilascia i certificati
Autorità per la marcatura temporale (Time Stamping Authority)	È il sistema Hardware/Software gestito dal certificatore che eroga il servizio di marcatura temporale.
Validità Temporale o Marca Temporale	Informazione Elettronica contenente la data e l'ora che viene associata ad un documento informatico, al fine di provare che quest'ultimo esisteva in quel preciso momento
TSA	Time Stamping Authority – Autorità che rilascia marche temporali
Utente	Agente fruitore del servizio D.A.S.
Cliente	È il soggetto a favore del quale D.A.S. mette a disposizione la soluzione di Firma Elettronica Avanzata al fine di sottoscrivere i documenti informatici

GLI ATTORI

Nell'ambito del progetto FEA per D.A.S. si vedono coinvolti una serie di attori che hanno permesso la realizzazione in rispetto della normativa vigente:

- D.A.S.: Compagnia assicurativa che vende i propri prodotti direttamente e/o per il tramite dei propri intermediari utilizzando servizi di firma elettronica avanzata;
- Namirial S.p.A.: Certification Authority accredita per l'emissione dei certificati asimmetrici e conservazione della chiave pubblica di crittografia e società tecnologica che ha realizzato e fornisce il servizio di Digital Transaction Management (DTM) che permette di firmare i documenti in modalità elettronica;
- Microdata Group: società qualificata per archiviazione e conservazione a norma di legge dei documenti informatici.

LE SOCIETÀ

D.A.S.

D.A.S. è la più antica ed esperta organizzazione internazionale specializzata nella Tutela Legale. Le sue origini risalgono allo straordinario intuito di Georges Durand, padre della leggendaria 24 Ore di Le Mans, città in cui nel 1917 venne fondata la D.A.S. "Defense Automobile et Sportive" con lo scopo di offrire una copertura assicurativa agli automobilisti delle prime competizioni sportive dell'epoca.

Da allora D.A.S. è diventata una società affermata nel panorama internazionale, detenendo in Europa la leadership di settore, con 12 milioni di clienti in 18 Paesi e una raccolta premi di 1,1 miliardi di euro.

D.A.S. Italia, compagnia fondata nel 1959, ha la propria sede a Verona e una struttura decentrata nella città di Bolzano, con un organico complessivo di 88 persone. Gli oltre cinquant'anni di esperienza hanno reso la società il punto di riferimento per il mercato dell'assicurazione di tutela legale.

Attualmente i principali azionisti sono: Generali Italia S.p.A. e ERGO Versucherungs AG (Gruppo Munich RE)

Mettono a disposizione dei clienti una rete estesa di intermediari articolata su tutto il territorio nazionale, formata da oltre 1.100 agenzie, per lo più plurimandatarie, tra cui l'intera rete distributiva Toro. Hanno inoltre scelto D.A.S. come loro partner circa 350 Broker di assicurazione.

Inoltre prestano i loro servizi a favore di 15 Compagnie di assicurazione, attraverso accordi di riassicurazione in ottica di servizio tecnico e di assistenza legale.

In relazione a questo progetto, D.A.S., si pone come Compagnia che utilizza il servizio di Firma Elettronica Avanzata per i propri clienti. È responsabile della redazione dei documenti di riferimento per la definizione dei processi, dello sviluppo software necessario a richiamare il processo di firma di Namirial S.p.A. e per la realizzazione di applicazioni con utilizzo della firma in ambito FEA.

NAMIRIAL S.P.A.

Namirial è una società IT di software e servizi ed è una **Certification Authority** che fornisce Trust Services come **Firme Elettroniche, Grafometriche e Digitali, Posta Elettronica Certificata, Fatturazione Elettronica e Conservazione Sostitutiva**.

- **Autorità di Certificazione accreditata** presso AgID ed autorizzata all'emissione di certificati qualificati conformi alla Direttiva europea 1999/93/CE, certificati CNS e Marche Temporali.
- **Qualified Trust Service Provider eIDAS** per l'emissione di validazioni temporali e certificati qualificati. In particolare Namirial ha conseguito il certificato n. IT269191 rilasciato da Bureu Veritas Italia SpA per l'emissione di validazioni temporali qualificate (marche temporali)
- **Gestore di PEC**, accreditato presso AGID ed autorizzato alla gestione di caselle e domini di Posta Elettronica Certificata.
- **Conservatore accreditato presso AgID** per attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Certificata UNI EN ISO 9001:2008** Namirial ha conseguito il certificato n. 223776 rilasciato da Bureau Veritas Italia S.p.A.
- **Certificata ISO/IEC 27001:2013**. Namirial ha conseguito il certificato n. IND15.0059U rilasciato da Bureau Veritas Italia S.p.A. e il certificato n.38271 rilasciato da CSQA
- **Certificata da Adobe.** Da Giugno 2013 Namirial è membro dell'AATL (Adobe Approved Trust List).

CERTIFICAZIONE ISO 9001

Namirial ha ottenuto la certificazione UNI EN ISO 9001:2000 in data 28.11.2007. Namirial ha conseguito il certificato n. 223776 presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO 9001:2008 con il seguente scopo:

"Progettazione, elaborazione ed assistenza post vendita di software, piattaforme gestionali e siti internet. Erogazione di servizi di hosting e co-location. Erogazione del servizio di posta elettronica certificata. Certification Authority, time stamping, firma automatica, firma remota, firma elettronica semplice e avanzata e personalizzazione di smart card. Progettazione ed erogazione di servizi gestiti in modalità Saas, Paas e on premise in ambito Enterprise Content Management e paperless business (Business Process Management, acquisizione e trasmissione dei documenti, fatturazione elettronica, formazione documenti, gestione archiviazione e conservazione a norma di documenti informatici)."

CERTIFICAZIONI ISO/IEC 27001:2013

Namirial ha ottenuto la certificazione UNI EN ISO 27001:2013 in data 19.03.2012. Namirial ha conseguito il certificato n. IND15.0059U presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO/IEC 27001:2013 con il seguente scopo:

"Consulting, design, development, delivery, support, provisioning of it services and solutions for electronc signature, advanced electronic signature, advanced electronic signature based on biometrics, trust mail, certification authority and trust services in accordance with eIDAS European regulation".

Namirial ha conseguito il certificato n. 38271 presso la CSQA che l'ha giudicata conforme ai requisiti della norma ISO/IEC 27001:2013 con il seguente scopo:

"Progettazione di soluzioni ed erogazione di servizi gestiti in modalità SaaS, PaaS e On Premise in ambito Enterprise Content Management e Paperless Business (Business Process Management, Acquisizione e Trasmissione dei documenti, Fatturazione Elettronica, Formazione Documenti, Gestione Archiviazione e Conservazione a Norma di documenti informatici)."

CERTIFICAZIONE AATL

La Certification Authority Namirial, da Giugno 2013, è inserita nell'elenco AATL (Adobe Approved Trust List).

MICRODATA

Microdata nasce nel 1990 per offrire soluzioni di gestione dei processi documentali dei propri clienti. In quegli anni la gestione documentale era ancora agli albori e la trasformazione dell'immagine in informazione era uno dei principali obiettivi a cui le aziende tendevano.

Nel corso del tempo Microdata ha sempre investito nel miglioramento e nella crescita della propria struttura e la sua offerta si è evoluta insieme alle esigenze dei suoi clienti.

Oggi Microdata Group rappresenta una delle principali realtà italiane nel mercato dell'outsourcing documentale e dei servizi di back-office. Attraverso le controllate Microdata Service, Microdataweb e Prosint è in grado di offrire in outsourcing un servizio globale dei processi documentali.

In questo contesto, Microdata svolge la funzione di archiviazione e conservazione a norma dei documenti firmati in modalità FEA.

SCOPO DEL DOCUMENTO

Questo documento si pone lo scopo di descrivere le procedure operative e le regole predisposte e utilizzate al fine di gestire i servizi di Firma Elettronica Avanzata in relazione al progetto D.A.S. Il documento recepisce quanto richiesto dalle Regole Tecniche, con riferimento a quanto espresso nel Titolo V.

In particolare sono descritte, nel documento, le procedure atte a soddisfare quanto richiesto in tema di generazione, apposizione e verifica della Firma Elettronica Avanzata, Firma Digitale Remota e Validazione Temporale dei documenti informatici. Sono recepite le indicazioni espresse dal D.Lgs. del 7 marzo 2005 e successive modifiche riportate nel D.Lgs. del 30 dicembre 2010.

CONTESTO NORMATIVO DI RIFERIMENTO

PREMESSA

All'interno del nostro ordinamento la firma digitale e, più in generale, le restanti tipologie di firme elettroniche, sono regolamentate dal Decreto Legislativo 7 marzo 2005, n. 82, recante "**Codice dell'amministrazione digitale" (CAD)**.

Con l'emanazione e successiva entrata in vigore del Regolamento europeo 910/2014, noto come **eIDAS**, dallo scorso primo luglio 2016 sono intervenute rilevanti modifiche che riguardano la disciplina, anche tecnica, delle firme elettroniche.

Con il chiaro obbiettivo di armonizzare le previsioni del CAD con eIDAS, il legislatore ha emanato il Decreto Legislativo 26 agosto 2016 n. 179, entrato in vigore il 14 settembre 2016, che ha abrogato le definizioni di firma elettronica contenute nel precedente testo di legge, allineandole "tout court" a quelle descritte nel Regolamento Europeo.

Le modifiche introdotte dal Dlgs 179/2016 non si sono limitate ad un mero aggiornamento delle definizioni ma, con l'intento di rispettare il principio di non discriminazione dettato da eIDAS, hanno innalzato la valenza probatoria delle firme elettroniche "semplici" (non avanzate e non qualificate) elevandole al soddisfacimento della forma scritta e, nel contempo, hanno anche esteso il raggio di mutua riconoscibilità delle firme elettroniche a livello Europeo.

Attualmente, nel nostro quadro normativo sono contemplate le seguenti tipologie di firme:

FIRMA ELETTRONICA (FES)

La Firma Elettronica è definita dalla norma (Art 3, comma 10 dell'eIDAS) come *"dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare"*.

La firma elettronica "semplice" quindi, più che a una vera e propria firma, dà vita ad un processo di autenticazione cui sono riferibili minori requisiti di sicurezza rispetto alle altre tipologie di firma (avanzata e qualificata).

La normativa riconosce alla firma elettronica il valore probatorio dettato dall'Art 21, comma 1 del CAD: *"Il documento informatico, cui è apposta una firma elettronica, soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità"*.

Inoltre, ai sensi del principio di non discriminazione del Regolamento eIDAS, è previsto che:

"A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate."

"A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica."

FIRMA ELETTRONICA AVANZATA (FEA)

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;*
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.

E' essenziale comprendere che la FEA non si «riduce» al prodotto che viene utilizzato (tablet, OTP, ecc..), ma è qualificata come tale solo dal processo che viene adottato.

FIRMA ELETTRONICA QUALIFICATA (FEQ)

La Firma Elettronica Qualificata è definita dalla norma (Art 3, comma 12 dell'eIDAS) come *"una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;"*

È un particolare tipo di firma elettronica avanzata basato su un certificato "qualificato" (che garantisce l'identificazione univoca del titolare, rilasciato da certificatori qualificati) e realizzato mediante un dispositivo per la creazione di una firma elettronica qualificata che soddisfa particolari requisiti di sicurezza; il certificato può contenere limitazioni relative alla tipologia di atti da sottoscrivere o a tetti di spesa. Si abbandona quindi la neutralità tecnologica e si fa riferimento a una tecnologia specifica che prevede l'uso di un certificato qualificato e l'utilizzo di un dispositivo sicuro per la creazione della firma.

FIRMA DIGITALE (FD)

La Firma Digitale è definita dalla norma (Art 1, comma 1, let s del CAD) come *"un 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*

In altri termini, la Firma Digitale è una firma elettronica qualificata con doppia chiave, una privata (per firmare) ed una pubblica, esposta nel certificato, per la verifica della firma stessa.

Va pure ricordato che l'art. 25, comma 3 del Regolamento 910/2014 stabilisce che "*Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri"*: quindi la firma digitale italiana è, nel contesto europeo, a tutti gli effetti una firma elettronica qualificata.

LA SOLUZIONE DI FIRMA

La società D.A.S. offre all'interno della propria piattaforma, accessibile via Web, la tecnologia della firma elettronica (Vedasi DPCM 22 febbraio 2013 " Regole Tecniche in materia di generazione, apposizione e verifica delle Firme Elettroniche Avanzate, Qualificate e Digitali", DLG 82/05 e successive modificazioni e integrazioni "Codice dell'Amministrazione Digitale" nonché Regolamento (EU) n° 910/2014 (eIDAS) e successive modificazioni e integrazioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno) e si rivolge agli agenti assicurativi, essendo un utile e innovativo strumento per avere sempre a disposizione la numerosa contrattualistica che un Agente Assicurativo si trova ogni giorno ad utilizzare.

La piattaforma, per il tramite del proprio Certificatore Accreditato, concede la possibilità di redigere contratti e moduli in formato elettronico, sottoscrivendoli con Firma Elettronica Avanzata, che offre i vantaggi della semplicità di utilizzo, dell'immediatezza oltre a garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore, previa identificazione informatica, attraverso un processo stabilito dalla normativa vigente.

I contratti e tutta la modulistica che con tale modalità vengono sottoscritti sono documenti informatici che sul piano giuridico hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa.

Gli hash dei documenti (o i file integrali se richiesto) ed i relativi log vengono conservati nella piattaforma sviluppata da D.A.S. e portati in conservazione a norma da parte di Microdata sulla base di regole successivamente descritte.

AMBITO DI UTILIZZO

La piattaforma D.A.S., tramite il servizio di Firma Elettronica Avanzata, consente all'utente ed al proprio Cliente di sottoscrivere i seguenti contratti e/o Moduli:

- ✓ polizza;
- ✓ questionario adeguatezza polizza;
- ✓ consenso privacy.

L'utilizzo della FEA per la sottoscrizione degli elencati contratti e/o moduli deriva dalla lettura dei combinati disposti degli art. 21 comma 2bis del CAD il quale fa un esplicito richiamo all'art 1350 c.c. (gli atti di cui all'art 1350 del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena nullità, con Firma Elettronica Avanzata, Qualificata o Digitale ovvero sono formati con le ulteriori modalità di cui all'art 20 comma 1bis primo periodo), che permette, appunto, di sottoscrivere tramite FEA tutti i contratti che l'ordinamento italiano preveda possano essere sottoscritti per scrittura privata (rimangono pertanto esclusi solo gli atti pubblici e le scritture private Autenticate)

TIPOLOGIE DI FEA FRUIBILI ATTRAVERSO LA PIATTAFORMA

La piattaforma di D.A.S., per il tramite del proprio partner TSU prevede due tipologie di Firma Elettronica Avanzata, di seguito meglio specificate:

- **Firma Elettronica Avanzata Grafometrica**

La Firma Elettronica Avanzata Grafometrica generata da eSAW è realizzata secondo un processo che prevede un meccanismo di Document-binding estremamente robusto che si articola nelle seguenti macro-fasi:

a) Identificazione del cliente da parte dell'Agente
b) Acquisizione del documento da firmare grafometricamente da parte di eSAW
c) Caricamento del certificato di cifratura fornito dal TSP integrato in eSAW
d) Acquisizione protetta dei vettori grafometrici dal dispositivo di acquisizione grafometrica (Pad, Tablet)
e) Calcolo dell'impronta HASH-SHA-256 del documento da sottoscrivere
f) Creazione di una struttura dati contenente i vettori grafometrici in formato strutturato secondo le previsioni della normativa di settore
g) Creazione di una busta crittografica con algoritmo AES e contenente la struttura dati predisposta allo step precedente. La cifratura avviene con il certificato del TSP
h) Inserimento dei vettori grafometrici cifrati all'interno del documento
i) Creazione di una FEA in formato PAdES sul documento contenente i vettori grafometrici cifrati. La firma PAdES è basata su un certificato di FEA di servizio installato all'interno della piattaforma eSAW.
j) Invio copia documento firmato al cliente ed all'Agente DAS

Grazie al meccanismo software sopradescritto, mentre il firmatario appone la propria firma su un dispositivo, vengono rilevati tutti i dati biometrici della firma (Coordinata, tempo, pressione, tratti in aria etc).
Tutte queste informazioni, in combinazione con il tratto grafico della firma, sono inserite all'interno di documenti PDF contemporaneamente alla creazione di impronte HASH-SHA-256 per assicurarne l'integrità.
I dati comportamentali non sono conservati all'interno di archivi separati per dei successivi confronti, ma vengono criptati ed "inglobati" nel documento stesso; solo nel caso in cui il documento dovesse essere disconosciuto, i dati grafometrici contenuti nel documento verranno decifrati per confrontarli con quelli presenti in altri documenti già verificati o con quelli raccolti al momento stesso dal perito "grafometrico" nominato dal giudice.
L'utilizzo di dati comportamentali legati al documento (mediante opportuni algoritmi di HASH) e l'utilizzo di una Firma Elettronica Avanzata basata su un certificato emesso e gestito da CA Accreditate (c.d. terza parte fidata) permette di soddisfare pienamente i requisiti richiesti dalla normativa per la FEA, ovvero:

1) Identificazione del firmatario
2) Connessione univoca della firma al firmatario
3) Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima
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 di cui all'art. 55, comma 2, lettera A
7) Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatto o dati nello stesso rappresentati
8) Connessione univoca della firma al documento elettronico sottoscritto.

- **Firma Elettronica Avanzata con SMS (OTP)**

La Firma Elettronica Avanzata con SMS generata da eSAW è realizzata secondo un processo articolato secondo degli steps funzionali simili a quelli descritti nel punto precedente (Firma Elettronica Avanzata Grafometrica)
L'autenticazione del firmatario è convalidata mediante l'immissione di un codice di sicurezza univoco (One Time Password) da parte del firmatario. Il codice viene ricevuto sul proprio numero telefonico verificato. Questa

operazione può avvenire in presenza degli intermediari incaricati da D.A.S. oppure può essere eseguita dal firmatario in autonomia attraverso un Link ricevuto sulla propria mail.
Rispetto alla soluzione basata sulla grafometria, in questo processo il requisito di riconducibilità della firma del titolare viene garantita dal possesso del cellulare e dall'invio di un codice OTP (One Time Password) su tale numero.
Entrando nel dettaglio, il meccanismo si sviluppa secondo le seguenti macro-Fasi:

Firma in Agenzia

A. Identificazione del cliente da parte dell'agente
B. Acquisizione del documento da firmare da parte di eSAW
C. Visualizzazione del documento
D. Firma del Cliente tramite Click o Write sul campo firma
E. Invio di un codice OTP al numero di cellulare del firmatario
F. Inserimento del codice OTP ricevuto sul cellulare nel campo preposto
G. Calcolo dell'impronta HASH-SHA-256 del documento da sottoscrivere
H. Creazione di una FEA in formato PAdES basata su un certificato di Firma Elettronica Avanzata di servizio Installato all'interno della piattaforma eSAW.
I. Invio copia documento firmato al cliente ed all'Agente DAS

Firma da remoto

L'utilizzo della metodologia di firma OPT da remoto prevede che il cliente sia formalmente riconosciuto prima della stipula del contratto. Questa attività, nel processo di firma di DAS, è demandata all'agente che in quel momento sta emettendo la nuova polizza. Il nuovo processo OTP a distanza prevede però un passaggio in più rispetto la classica firma digitale o emissione OTP in agenzia che è la possibilità di convalidare i dati email e cellulare del futuro cliente.

La procedura di convalida invierà una mail all'assicurato contenente la richiesta per la convalida dei propri dati. Il cliente, cliccando sul link, confermerà la correttezza dei dati abilitando, per l'agenzia, l'opportunità di utilizzare il metodo di firma OTP a distanza. Se non avviene questa procedura non sarà possibile procedere con la firma da remoto

A. Invio di una mail al cliente contenente i link per effettuare la firma della polizza oppure per cancellare la richiesta, che avrà una validità di 48 ore. In caso di accettazione, il cliente verrà indirizzato sulla pagina web del portale operativo DAS che recupererà i dati e documento di polizza
B. Acquisizione del documento da firmare da parte di eSAW
C. Visualizzazione del documento
D. Firma del Cliente tramite Click o Write sul campo firma
E. Invio di un codice OTP al numero di cellulare del firmatario
F. Inserimento del codice OTP ricevuto sul cellulare
G. Calcolo dell'impronta HASH-SHA-256 del documento da sottoscrivere
H. Creazione di una FEA in formato PAdES basata su un certificato di Firma Elettronica Avanzata di servizio Installato all'interno della piattaforma eSAW.
I. Invio copia del documento firmato al cliente e all'Agente DAS

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

- Identificazione del firmatario del documento
- Connessione univoca della firma al firmatario
- Controllo esclusivo del firmatario del sistema di generazione della firma
- Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma
- Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto
- Individuazione del soggetto di cui all'art. 55, comma 2, lettera A
- Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatto o dati nello stesso rappresentati
- Connessione univoca della firma al documento elettronico sottoscritto.

CONSIDERAZIONI SULLE TIPOLOGIE DI FEA

Entrambe le tipologie di FEA (Grafometrica e con SMS-OTP) rispondono alla normativa eIDAS che prevede, ad esempio, nel caso della firma OTP, che le operazioni eseguite vengano rafforzate nel fattore di autenticazione dell'invio della password al numero di cellulare univocamente collegabile al firmatario, in quanto allo stesso riconducibile.

Nel caso di firma biometrica, la firma viene effettuata tramite appositi dispositivi di ultima generazione in grado di catturare un set strutturato di informazioni comportamentali relative allo stile di scrittura e alla grafia del sottoscrittore. Questi device, oltre a garantire una precisione molto elevata nella fase di acquisizione, realizzano anche canali di comunicazione per evitare che i dati sensibili possano essere manomessi o intercettati.

Cliccando sul campo firma, viene attivato il device di acquisizione del tratto utilizzato dal firmatario (PAD, Tablet o smartphone) e, in fase di firma, vengono registrate le informazioni sull'habitus di scrittura del sottoscrittore (Aspetto, Tempo, Velocità, Accellerazione, Ritmo, etc). Queste informazioni vengono quindi connesse all'impronta del documento e l'intera struttura viene salvata in un contenitore cifrato congelato all'interno del documento.

In entrambi i casi (Biometria e autenticazione tramite OTP) si dovrà procedere preliminarmente all'identificazione del firmatario in modo da rendere il processo ancora più robusto da un punto di vista della non ripudiabilità del documento sottoscritto.

Con la Firma Elettronica Avanzata, per concludere il processo, viene utilizzato un certificato elettronico di servizio, integrato in piattaforma e rilasciato dal Certificatore Qualificato Namirial S.p.A.

Il certificato è presente all'interno degli store Europei e del software di gestione dei PDF, Adobe e serve a garantire l'integrità e l'immodificabilità del documento

LA SOLUZIONE D.A.S.

La soluzione realizzata da D.A.S. garantisce i requisiti fondamentali di garanzia per il firmatario, in particolare:

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

Il completamento dei documenti sopraindicati avviene previa esibizione e acquisizione del documento d'identità e del codice fiscale.

A seguito della verifica di completezza dei dati in possesso, in caso di esito positivo, l'agente vaglierà la disponibilità del cliente all'utilizzo della FEA, fornendo informazioni esaustive dal punto di vista funzionale e normativo.

Nel caso in cui il cliente non fosse interessato all'utilizzo della FEA, tutta la documentazione verrà stampata e sottoposta a firma autografa seguendo l'iter standard attualmente in uso.

Invece, qualora il cliente scegliesse l'opzione proposta, verrà attivato il processo di firma che vede coinvolta l'applicazione sviluppata da D.A.S.

Tale applicazione predispone i file in formato PDF e attiva il processo di firma governato dal servizio eSAW secondo i parametri attivati dall'applicazione sviluppata da D.A.S.. In caso di Grafometrica, la firma viene raccolta da tavolette sicure (Wacom) o da tablet sicuri (con sistemi operativi Windows; iOS e Android) e vengono acquisiti i dati biometrici di identificazione univoca (coordinate, pressione, tempo) e il tratto grafico. Nel caso di firma OTP la firma sarà messa utilizzando il codice ricevuto al numero di cellulare univocamente collegabile al firmatario, in quanto deve essere intestato a quest'ultimo. La sicurezza è garantita dal servizio eSAW che provvede a inglobare i parametri nel file PDF. La sottoscrizione viene completata con la generazione del file impronta (Hash) da utilizzare poi in verifica e controllo. I documenti soggetti a sottoscrizione saranno:

- ✓ accettazione utilizzo FEA

- ✓ polizza;
- ✓ questionario adeguatezza polizza;
- ✓ consenso privacy;

Il cliente sarà invitato ad inserire la propria firma in ogni spazio preposto e, ad ogni inserimento, avrà la possibilità di cancellare e ripetere l'inserimento, annullare il processo o proseguire con le firme successive. La firma, in caso di grafometria, riproduce esattamente la firma con la grafia personale del firmatario e non è un insieme di dati alfanumerici. Per questo motivo ogni firma ha una sua validità legale: è una firma personale e mantiene le caratteristiche di integrità e di qualità, incide minimamente sulla dimensione del file e viene apposta, nel sistema, è trattata in vettoriale. Nel caso di firma OTP il cliente sarà invitato ad inserire il codice di sicurezza ricevuto sul proprio cellulare confermando a questo punto la sua identità.

In ultima istanza, l'agente dovrà inserire le propria firme.

La fase di acquisizione firma termina e la polizza viene chiusa. Il documento di polizza sarà disponibile nel documentale aziendale, ed il fascicolo precedentemente chiuso sarà depositato in una directory che mensilmente il sistema di Microdata provvederà a svuotare e a sottoporre ai sistemi di archiviazione e conservazione secondo le indicazioni normative.

COMPONENTI

La soluzione implementata si compone di processi strutturati, di soluzioni hardware e software per il processo di acquisizione della firma e per la gestione del documento.

SOFTWARE GESTIONE FIRMA

Il software di gestione del processo di firma è fornito in SaaS da Namirial e viene richiamato dalle componenti software sviluppate da D.A.S., prende in carico il documento da firmare e ne gestisce l'operatività in sicurezza e senza possibilità di iterazioni, interventi da parte di software esterni. Alla conclusione rilascia un documento di tipologia PDF/A con le firme acquisite e cifrate e chiuso con certificato di servizio rilasciato dal Certificatore Qualificato Namirial S.p.A

HARDWARE

L'hardware utilizzabile è una vasta gamma di apparati, dalle tavolette Wacom collegate ai PC, ai Tablet e/o Smartphone con sistemi operativi Android, iOS e Microsoft. I documenti sono visibili sui diversi monitor di rappresentazione del cliente (tablet, pad, smartphone).

LIMITE D'USO

La FEA ha l'efficacia prevista dall'articolo 2702 del Codice Civile e integra il requisito della forma scritta.

Nei documenti normativi citati nel capitolo 2 e con particolare riferimento alle Regole Tecniche, approvate con Decreto del Presidente del Consiglio in data 22 febbraio 2013, si pongono alcune limitazioni all'operatività della Firma Elettronica Avanzata e di seguito riassumiamo:

- La FEA non consente il libero scambio di documenti informatici: il suo uso è limitato al contesto;
- La FEA è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore (Cliente) e il soggetto che eroga soluzioni di FEA (D.A.S.) al fine di trattarle nel processo di dematerializzazione per motivi istituzionali, societari o commerciali;

- La FEA pur avendo l'efficacia prevista dall'articolo 2702 del Codice Civile presenta alcune eccezioni e in particolare atti di cui l'art. 1350 punti 1-12 del Codice Civile. In questi casi si deve utilizzare la Firma Digitale.

Di conseguenza la soluzione di FEA può gestire tutti i documenti ad eccezione di quanto previsto dall'articolo 21 comma 2-bis del D.Lgs 235/2010 che cita testualmente "Salvo quanto previsto dall'articolo 25. Le scritture private di cui all'articolo 1350, primo comma, numero da 1 a 12, del Codice Civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale". Il contratto in esame risponde all'articolo 1350 primo comma numero 13.

OBBLIGHI

I soggetti che erogano soluzioni FEA (D.A.S. nel nostro caso) hanno una serie di obblighi al fine di mantenere tutti i requisiti richiesti dal CAD.

1) Identificare in modo certo l'utente tramite un valido documento di riconoscimento;
2) Informare l'utente ed il Cliente in relazione agli esatti termini e condizioni d'uso del servizio, compresa ogni eventuale limitazione d'uso;
3) Subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte del Cliente;
4) Conservare per almeno **20 anni** copia del documento di riconoscimento e la dichiarazione del punto 3;
5) Garantire la disponibilità, integrità, leggibilità e autenticità del documento di accettazione del servizio (punto 3);
6) Fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui al punto 3) al firmatario su sua richiesta;
7) Rendere note le modalità con cui effettuare la richiesta di cui al punto 6), pubblicandole anche sul proprio sito internet;
8) Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dalle Regole Tecniche articolo 56, comma 1;
9) Specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;
10) Pubblicare le caratteristiche di cui alle lettere 8) e 9) sul proprio sito internet.

Ciò premesso si precisa che **è esclusiva responsabilità dell'Utente (Agente) identificare correttamente il Cliente** secondo le modalità di acquisizione del documento di riconoscimento e del relativo numero di cellulare e dell'indirizzo di e-mail, manlevando in tal senso D.A.S. da qualsiasi responsabilità in caso di inidonea identificazione

TUTELA ASSICURATIVA

Ulteriore richiesta espressamente citata nelle Regole Tecniche, prevede una copertura assicurativa a garanzia del firmatario. In particolare, nelle Regole Tecniche art. 57 comma 2, si cita che:

Ai sensi dell'art. 57 comma 2 delle Regole Tecniche 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.

D.A.S. ha stipulato, in conformità alla normativa vigente, polizza assicurativa con primaria Compagnia Assicuratrice a tutela dei danni eventualmente derivanti/causati da problemi tecnici riconducibili all'utilizzo della FEA

INFORMATIVA E ARCHIVIAZIONE DOCUMENTI

In pieno rispetto delle regole tecniche, su sito istituzionale di D.A.S. (http://www.das.it/) è possibile reperire l'informativa relativa alle modalità di erogazione del servizio di Firma Elettronica Avanzata.

L'utilizzo della firma elettronica con valore di FEA avviene solo dopo che il Cliente, opportunamente e preliminarmente riconosciuto, in conformità a quanto prescritto dalla normativa, abbia manifestato la sua volontà di accettare, con una apposita dichiarazione di autorizzazione, l'utilizzo di tale strumento.

Il Cliente, una volta sottoscritto il contratto e/o modulo, riceverà una copia o in formato cartaceo o attraverso l'indirizzo di posta elettronica indicato, e D.A.S. archivierà tale documento presso il suo conservatore.

Si precisa che i documenti sottoscritti e gli allegati, che costituiscono il dossier della pratica, sono a disposizione del firmatario e degli agenti di D.A.S. in forma diversa, in particolare:

- Il cliente riceve copia della documentazione del dossier o in cartaceo all'atto della sottoscrizione o via e-mail se ha scelto queste modalità. In ogni caso potrà sempre richiederne una copia.
- Il documento di Polizza per consultazione su documentale aziendale.

In estrema sintesi i dati presenti nel dossier riguarderanno:

- Data e ora della sottoscrizione
- Geolocalizzazione se consentita dal cliente in fase di firma
- L'attestazione che il documento e/o modulo non è stato modificato dopo l'apposizione delle firme
- La validazione delle firme apposte
- I dettagli del certificato accreditato

Il dossier comprensivo dei documenti firmati con FEA e dei Log della piattaforma eSAW, viene archiviato in una directory che mensilmente Microdata provvede a svuotare avviando il processo di conservazione sostitutiva a norma dei documenti in oggetto.

La conservazione a Norma è un processo che permette di archiviare in modo sicuro i contratti e/o moduli sottoscritti dal Cliente tramite FEA, affinché restino integri e risultino immodificabili e leggibili nel tempo.

Tale metodo di archiviazione permette, nel lungo termine, ovvero dall'inizio della conservazione e per tutto il tempo di custodia previsto e richiesto, il mantenimento continuo ed ininterrotto delle caratteristiche di validità originarie di ciascun oggetto messo in conservazione assicurandone, insieme alla reperibilità e possibilità di esibizione per tutta la durata del periodo di archiviazione/conservazione, anche il rispetto delle norme sul trattamento dei dati.

D.A.S., attraverso Microdata, conserverà i documenti per i tempi previsti della legge e, in particolare, le copie del documento di riconoscimento e l'accettazione del servizio saranno conservati per 20 anni così come previsto dalle Regole Tecniche.

Periodiche verifiche sull'integrità e la leggibilità dei Documenti vengono svolte al fine di garantire un alto livello di affidabilità e di qualità del servizio nel tempo

Si precisa che tutto il processo di apposizione di marche temporali su tutti i documenti sottoscritti con FEA tramite D.A.S. e la relativa conservazione ed archiviazione seguono un processo totalmente automatizzato e non è richiesta nessuna attività specifica da parte dell'utente o del cliente.

Periodiche verifiche sull'integrità e la leggibilità dei Documenti vengono svolte al fine di garantire un alto livello di affidabilità e di qualità del servizio nel tempo.

LA GESTIONE DEL CONTENZIOSO FEA GRAFOMETRICA

Il processo di gestione di un contenzioso, inizialmente segue le classiche politiche di gestione previste dalla società ma, in ipotesi che il contenzioso prosegua in giudizio, si deve obbligatoriamente prevedere un diverso approccio di perizia.

In particolare è necessario procedere a una perizia dei dati informatici e biometrici delle firme in contenzioso.

I dati comportamentali non sono conservati all'interno di archivi separati per successivi confronti ma vengono criptati ed "inglobati" nel documento stesso.

Nel caso in cui il documento dovesse essere disconosciuto, i dati grafometrici saranno decifrati per confrontarli con quelli presenti in altri documenti già verificati o con quelli raccolti al momento dallo stesso perito calligrafo nominato dal giudice.

Ovviamente per poter effettuare questo controllo è indispensabile poter accedere ai dati crittografati della firma.

In sintesi il processo prevede:

a) la nomina da parte del Giudice del perito incaricato di effettuare la perizia;

b) La definizione da parte del Giudice della sede dove si svolgerà la perizia (tribunale; ufficio del perito o altra sede) ed i tempi di effettuazione della stessa;

c) la richiesta, alla società di conservazione, del documento originale elettronico;

d) L'apposizione, a richiesta del perito, di una nuova firma al cliente che ne ha contestato l'autenticità l'analisi comparata di quest'ultima con altre firme (presenti su altri documenti elettronici e/o cartacei) firmati entro un periodo di un anno.