# Firma Elettroniche eSAW

Valenza giuridica

**Sommario**

# 1 Introduzione

## 1.1 Scopo

Il presente documento illustra le caratteristiche delle firme elettroniche disponibili all'interno della 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.

## 1.2 Riferimenti tecnici e normativi

Namirial, 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<br>*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<br>*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<br>*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<br>*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.<br>*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<br>*Codice in materia di protezione dei dati personali.* |
| [07] | DPR 445/2000 | Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445<br>*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.<br>*La presente deliberazione ha abrogato: Deliberazione CNIPA 17 febbraio 2005 n. 4*<br>*Deliberazione CNIPA 18 maggio 2006 n. 34*<br>*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<br>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.<br>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.<br>*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);<br>Time-stamping protocol and time-stamp token profiles |
| [26] | ETSI EN 319 411-1 | Electronic Signatures and Infrastructures (ESI);<br>Policy and security requirements for<br>Trust Service Providers issuing certificates;<br>Part 1: General requirements |
| [27] | ETSI EN 319 411-2 | Electronic Signatures and Infrastructures (ESI);<br>Policy and security requirements for<br>Trust Service Providers issuing certificates;<br>Part 2: Requirements for trust service providers issuing<br>EU qualified certificates |

| | | |
|---|---|---|
| [28] | ETSI EN 319 411-3 | Electronic Signatures and Infrastructures (ESI);<br>Policy and security requirements for<br>Trust Service Providers issuing certificates;<br>Part 3: Policy requirements for<br>Certification Authorities issuing public key certificates |
| [29] | ETSI EN 319 412-1 | Electronic Signatures and Infrastructures (ESI);<br>Certificate Profiles;<br>Part 1: Overview and common data structures |
| [30] | ETSI EN 319 412-2 | Electronic Signatures and Infrastructures (ESI);<br>Certificate Profiles;<br>Part 2: Certificate profile for certificates issued<br>to natural persons |
| **NUM** | **NORMATIVA** | **DESCRIZIONE** |
| [31] | ETSI EN 319 412-3 | Electronic Signatures and Infrastructures (ESI);<br>Certificate Profiles;<br>Part 3: Certificate profile for certificates issued<br>to legal persons |
| [32] | ETSI EN 319 412-4 | Electronic Signatures and Infrastructures (ESI);<br>Certificate Profiles;<br>Part 4: Certificate profile for web site certificates |
| [33] | ETSI EN 319 412-5 | Electronic Signatures and Infrastructures (ESI);<br>Certificate Profiles;<br>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 |
| [37] | TSL | COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications 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 |

*Tabella 1: Riferimenti tecnici e normativi*

## 1.3 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. |

| TERMINE O ACRONIMO | SIGNIFICATO |
|---|---|
| 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.<br>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. |

| TERMINE O ACRONIMO | SIGNIFICATO |
|---|---|
| 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. |

| TERMINE O ACRONIMO | SIGNIFICATO |
|---|---|
| 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) |

*Tabella 1: Definizioni e Acronimi*

# 2 Convenzioni di lettura

Per comodità di lettura si precisa che nel corso del testo, i punti di forza del sistema proposto verranno indicati con il seguente simbolo  .

# 3 Namirial

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 Stron 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.

---

- **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).

---

# 4 Caratteristiche generali della piattaforma per la firma elettronica

## 4.1 Descrizione generale della piattaforma

Il sistema di firma elettronica centralizzato sviluppato da Namirial è basato sull'architettura **eSAW** (eSignAnyWhere).

eSAW è una piattaforma integrata per l'esecuzione di transazioni di business attraverso l'apposizione di firme elettroniche. 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 visualizzare e firmare i documenti su qualsiasi dispositivo utilizzando diverse tipologie di firma.

La creazione e gestione delle pratiche di firma può avvenire in due modalità:

1. **interattiva**, tramite l'uso di una GUI (Graphical User Interface - Figura 1).

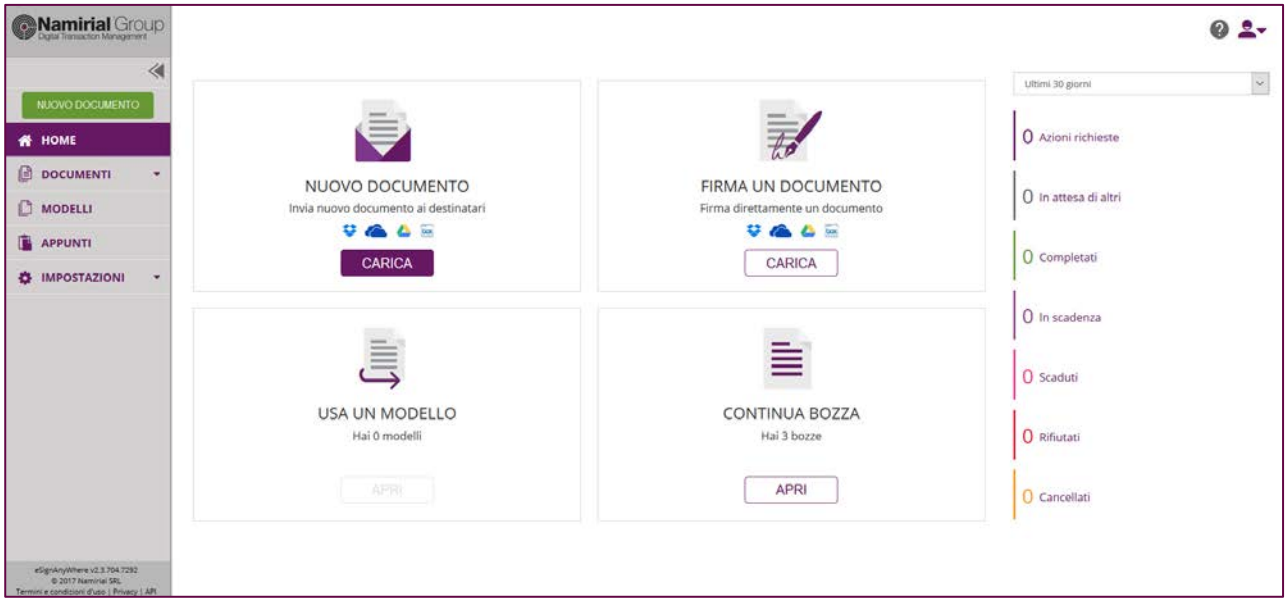


**Figura 1 - GUI eSAW**

2. **programmatica**, attraverso l'invocazione di web-service SOAP o REST (Figura 2) da parte di un'applicazione di gestione documentale già in esercizio presso l'Organizzazione.

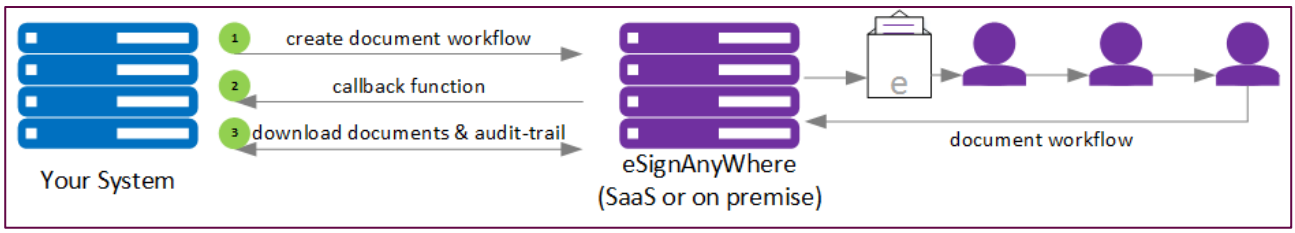


**Figura 2 – Integrazione applicativa eSAW**

I livelli di qualità e sicurezza offerti dal processo implementato dal sistema unitamente alla garanzia dell'integrità del documento raggiunta con l'utilizzo di firme elettroniche in formato PAdES,

conformi alla Decisione di Esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015 (ETSI TS 103172 v.2.2.2), contribuiscono a attribuire il valore legale della firma, anche nel caso venga apposta una firma elettronica semplice.

Le Impronte dei documenti (o gli interi file) ed i relativi log sono conservati nella piattaforma eSAW e, qualora lo specifico caso d'uso lo richieda, possono essere portati in conservazione a norma per estenderne la validità sul lungo periodo.

### 4.1.1 Tipologie Firme Elettroniche

Con eSignAnyWhere è possibile eseguire le seguenti tipologie di firma:

- **Firma Elettronica Semplice (FES)**
    - E' possibile firmare i documenti utilizzando i meccanismi di **Click to Sign**, **Type to Sign** e **Draw to Sign**.
    - All'interno della firma, e quindi protette da quest'ultima, vengono raccolte tutte le informazioni collegate al firmatario (nome, mail, indirizzo IP, timestamp).
    - Nel caso Type to Sign, il destinatario firma inoltre digitando il proprio nome che viene reso in corsivo sul campo firma, mentre nel caso Draw to Sign: Il firmatario disegna la propria firma con un dito, una penna o il mouse.
    - Per ciascuna delle firme sopracitate 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
- **Firma Elettronica Avanzata**
    - E' possibile firmare i documenti utilizzando **meccanismi grafometrici** (biometria) ovvero di **autenticazione tramite codice OTP** inviato al numero di cellulare dell'utente.
    - Nel caso di **firma OTP** le operazioni eseguite sono le stesse previste per le precedenti tipologie di firma, irrobustite nel fattore di autenticazione inviato al numero di cellullare dell'utente.
    - 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 ed alla grafia del sottoscrittore. Questi device, oltre a garantire una precisione molto elevata nella fase di acquisizione, realizzando anche canali di comunicazione sicuri per evitare che i dati sensibili in transito 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, velocità, tempo, accelerazione, 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 OTP, 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.

  Anche con la firma elettronica avanzata il file viene utilizzato un certificato elettronico di servizio, integrato in 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

- **Firma Elettronica Qualificata** (FEQ)
  - E' possibile firmare un documento utilizzando un certificato digitale remoto rilasciato dal Certificatore Namirial. Per firmare basta inserire un nome utente, una password ed una One Time Password (ad esempio ricevuta per SMS o generata da un dispositivo eventualmente già in possesso del sottoscrittore).

    Nel caso di integrazioni con workflow preesistenti è possibile utilizzare la stessa username e password impostante nel sistema ERP/CMS dell'Organizzazione/Ente
  - E' possibile utilizzare un qualsiasi certificato di firma digitale su supporto fisico, quali Token o Smart Card.
  - Nell'ambito della firma qualificata è importante rimarcare il concetto di sottoscrizione di N documenti con un solo OTP. Nel caso siano presenti anche clausole vessatorie all'interno dello stesso documento, eSAW permette, dietro specifica indicazione del Organizzazione/Ente, di consentire o meno l'inserimento di un solo OTP.

- **Firma Digitale Remota**
  - Trattasi, come meglio descritto nel prosieguo (§ 6.1), di caso particolare di firma elettronica qualificata.

# 5 Contesto normativo di riferimento

## 5.1 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 sono state quindi aggiornate dalle modifiche introdotte Decreto Legislativo 13 dicembre 2017 , n. 217, pubblicato in Gazzetta Ufficiale in data 12 gennaio 2018 ed in vigore dal 27 gennaio 2018.

Le modifiche introdotte al CAD dal D.lgs 179/2016 e dal 217/2017 hanno 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 (SEMPLICE)**

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 20, comma 1-bis del CAD (Validità ed efficacia probatoria dei documenti informatici) : *"Il documento informatico soddisfa 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, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di qualità, sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se appostein conformità alle Linee guida."*.

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**

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.

E' essenziale comprendere che la FEA non si «riduce» al prodotto o soluzione tecnologica che vengono utilizzati (tablet, OTP, librerie, app, ecc..), ma è considerata tale solo in virtù dal processo che viene adottato.

**FIRMA ELETTRONICA QUALIFICATA**

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**

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.

## 5.2 Valore legale documenti generati

La piattaforma eSAW, come anticipato nel paragrafo § 5, permette di generare documenti informatici sottoscritti con diverse tipologie di firma, ciascuna calzante per il particolare flusso, documento o use-case di atterraggio:

- Firma Elettronica "Semplice" (Click-to-Sign, Draw-to-Sign, Type-to-Sign)
- Firma Elettronica Avanzata (Grafometrica o OTP)
- Firma Elettronica Qualificata (sia remota che locale)

- Firma Digitale (sia remota che locale)

Soprassedendo momentaneamente ai dettagli tecnici ed operativi propri dei diversi flussi all'interno dei quali è possibile integrare le funzionalità di firma elettronica di eSAW, nel prosieguo verrà descritto il focus sulle caratteristiche oggettive di qualità e sicurezza possedute dai documenti sottoscritti con ciascuna delle tipologie di firma sopraindicate.

### 5.2.1 Firma elettronica semplice in eSignAnyWhere

Ricordiamo che per Firma Elettronica Semplice s'intende un insieme di *dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*.

La normativa riconosce alla firma elettronica un valore probatorio minimo attribuendo al documento informatico, cui è apposta una firma elettronica, il diritto a poter essere accettata e poter essere liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Al fine di garantire le caratteristiche di cui sopra, la piattaforma eSAW utilizza i seguenti meccanismi:

a) Il documento da firmare può essere acceduto direttamente all'interno di un'area riservata del portale su cui il sottoscrittore si è autenticato tramite credenziali in suo possesso.

   ➡ Qualora richiesto dal particolare flusso, al fine di innalzare il livello di sicurezza, è possibile inviare il link per l'accesso al documento da firmare anche all'email indicata dal firmatario ed a cui egli ha accesso con credenziali, diverse da quelle utilizzate nei portali integrati con eSAW.

   Questo meccanismo consente di verificare le credenziali di tipo **SYK** (something you know) in possesso del sottoscrittore

b) Prima di accedere al documento da firmare può essere richiesto l'inserimento di una One Time Password (OTP) inviata via SMS al numero di cellulare indicato dal firmatario.

   Questo meccanismo risulta particolarmente utile in tutti quei casi in cui si renda necessario inserire un secondo fattore di autenticazione per l'utente di tipo **SYH** (something you have) oltre che per garantire la non disclosure del documento da firmare (es. documenti per finanziamento contenenti dati sensibili e relativi all'importo richiesto)

   In generale i documenti da firmare possono essere protetti da un meccanismo di autenticazione per assicurarsi che solamente il firmatario designato possa accedervi. I meccanismi di autenticazione disponibili sono:

   - Un PIN comunicato al firmatario designato "out-of-band";
   - Un OTP inviato sul numero di cellulare del firmatario (dispositivo personale);
   - Windows Live Authentication.
   - Third-Party plugin authenticator (OAuth 2.0 compliant)

c) Assieme ad ogni firma vengono allegati al documento un set di metadati (inseriti graficamente come un timbro) in cui sono indicati il nome e cognome del firmatario, la sua mail, l'indirizzo IP dal quale ha effettuato la connessione e la data/ora UTC.

   Tali informazioni sono inserite centralmente dal sistema eSAW e, pertanto, non sono modificabili dall'utente sottoscrittore. Inoltre, in paradigmi di erogazione SaaS (Software as a Service), il servizio di firma eSAW può essere erogato direttamente dal Prestatore Qualificato di Servizi Fiduciari e ciò estende di fatto il perimetro di sicurezza sull'integrità dei metadati anche al soggetto cofirmatario, tipicamente l'Organizzazione o l'Ente che gestisce l'applicazione ed i flussi documentali all'interno dei quali viene integrata la firma elettronica di eSAW.

   Il meccanismo consente di arricchire il documento e la firma con le informazioni che contestualizzano luogo e data della sottoscrizione. Queste informazioni rappresentano elementi di prova che prodotti in sede di contenzioso, assieme ad altri elementi di prova, possono fondare il convincimento del giudice

d) L'integrità del documento viene garantita attraverso l'apposizione di una firma tecnica effettuata attraverso un certificato di firma qualificato per ogni firma apposta.

e) Viene generato un Audit Trail o Log di tutti i passi effettuati con inclusi gli indirizzi IP e la eventuale geolocalizzazione del firmatario.

   L'Audit Trail è estraibile dal sistema e producibile in sede di contenzioso.

| 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: hMgS0fPFgv 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: hMgS0fPFgv 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-a887-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-a887-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-a887-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 /> |

**Figura 3 - Esempio di Audit Trail**

#### *5.2.1.1 Efficacia probatoria della firma elettronica semplice*

Nonostante la normativa vigente non riconosca al documento cui è apposta una firma elettronica semplice il requisito della forma scritta, ne garantisce però l'ammissibilità in sede giudiziaria. Affinché il giudice ne possa valutare l'idoneità al soddisfacimento della forma scritta ed il suo valore probatorio, è facilmente comprensibile come una firma elettronica generata tramite il processo sopraindicato, riesca a produrre una collezione di elementi probatori in grado di dimostrare oggettivamente alti livelli di qualità, sicurezza, integrità e immodificabilità atti a permetterne l'accettazione quale piena prova dei fatti.

### 5.2.2 Firma Elettronica Avanzata in eSAW (Grafometrica)

La firma elettronica avanzata grafometrica generata da eSAW è realizzata secondo un processo che, oltre a ricalcare pienamente le caratteristiche descritte in § 5.2.1 prevede un meccanismo di document -binding estremamente robusto che si articola nei seguenti macro-fasi:

a) Identificazione dell'utente sottoscrittore da parte di un operatore
b) acquisizione del documento da firmare grafometricamente da parte di eSAW
c) Caricamento del certificato di cifratura fornito dalla CA Namirial, integrato in eSAW
d) Acquisizione protetta dei vettori grafometrici dal dispositivo di acquisizione grafometrica (tavoletta desktop o 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 di cui al punto 3 e l'impronta del documento di cui al punto 4.
g) Creazione di una busta crittografica cifrata con algoritmo AES e contenente la struttura dati predisposta allo step precedente. La cifratura avviene con il certificato Namirial descritto allo step 2.
h) Inserimento dei vettori grafometrici cifrati all'interno del documento
i) Creazione di una firma elettronica avanzata in formato PAdES sul documento contenente I vettori grafometrici cifrati. La firma PAdES è basata su un certificato di firma elettronica avanzata di servizio installato all'interno della piattaforma eSAW.

Grazie al meccanismo software sopradescritto, mentre il cliente appone la propria firma su un dispositivo, vengono rilevati tutti i dati biometrici della firma (coordinate, tempo, pressione, tratto in aria ecc).

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.

#### *5.2.2.1 Efficacia probatoria della firma elettronica avanzata eSAW*

L'utilizzo di dati comportamentali legati al documento (mediante opportuni algoritmi di HASH) 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.

### 5.2.3 Firma Elettronica Avanzata in eSAW (SMS)

La firma elettronica avanzata SMS generata da eSAW è realizzata tramite un processo articolato secondo degli steps funzionali simili a quelli descritti in § 5.2.2. Rispetto alla soluzione basata su grafometria, 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 da parte di eSAW
c) Invio di un codice OTP al numero di cellullare del Titolare
d) Login dell'utente su 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 (§ 5.2.1), 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.

#### *5.2.3.1 Efficacia probatoria della firma elettronica avanzata eSAW*

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:

i) l'identificazione del firmatario del documento;

j) la connessione univoca della firma al firmatario;

k) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;

l) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;

m) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

n) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);

o) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;

p) la connessione univoca della firma al documento sottoscritto.