SÜDTIROL BANK

Firma Elettronica Avanzata

Caratteristiche tecnologiche

FIRMA ELETTRONICA AVANZATA

CARATTERISTICHE TECNOLOGICHE DEL SISTEMA REALIZZATO DALLA ALTO ADIGE BANCA SPA / SÜDTIROL BANK AG PER L'USO DELLA FIRMA ELETTRONICA AVANZATA

[ai sensi dell'art. 57, lett. e) delle "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali," pubblicate nella Gazzetta Ufficiale n. 117 del 21 maggio 2013, attuative del Codice dell'Amministrazione Digitale di cui al Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni].

Premessa

Il processo associato al sistema di *firma elettronica avanzata* garantisce:

- l'identificazione del firmatario;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma;
- la possibilità di verificare che il documento sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione dell'intermediario (Alto Adige Banca SpA / Südtirol Bank AG) che realizza la soluzione di *firma elettronica avanzata;*
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
- la connessione univoca della firma al documento sottoscritto.

1.

Descrizione delle caratteristiche del sistema che garantiscono l'identificazione del firmatario

La Alto Adige Banca SpA / Südtirol Bank AG (di seguito, anche solo, la "Banca") identifica preliminarmente il firmatario dei documenti (l'"utente") richiedendo il relativo documento d'identità in corso di validità.

2.

Descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al firmatario

Prima di procedere con l'apposizione delle proprie firme, il firmatario può consultare interamente il documento informatico, controllandone e validandone i contenuti direttamente a video. Tale documento informatico ripropone le medesime caratteristiche delle precedenti versioni cartacee, ma è di più semplice ed efficace gestione.

Il sistema registra le caratteristiche dinamiche della firma autografa che il firmatario appone di suo pugno con penna elettronica sull'apposito dispositivo di firma ("signature PAD" o "tablet"). Le caratteristiche registrate corrispondono alla scansione temporale di posizione, vale a dire il ritmo, la velocità e la pressione della penna, quali acquisite con opportuna risoluzione.

La rappresentazione informatica della firma racchiude informazioni superiori alla raccolta della firma autografa su carta.

L'univocità della connessione viene garantita dalla sottoscrizione effettuata davanti all'operatore bancario ovvero, in caso di offerta fuori sede, al Promotore Finanziario, previa identificazione del firmatario, e alla possibilità di effettuare un'eventuale perizia grafica, in modo del tutto equivalente a quanto previsto per una firma autografa su carta.

Il processo consente di visualizzare, anche a distanza di tempo, la firma apposta sul documento informatico e di confrontarla visivamente con le altre presenti sullo stesso documento o su altri documenti, apposte dallo stesso soggetto, evidenziando oltre alla grafia anche ulteriori informazioni quali la data, l'ora nonché, eventualmente, il luogo di apposizione.

L'utente, utilizzando il signature PAD collegato al PC via USB ovvero il tablet, firma con la penna in dotazione, esattamente come farebbe su carta. Il sistema è in grado di rilevare le caratteristiche comportamentali del firmatario, quali la posizione (coordinate), la velocità, il ritmo e la pressione.
Terminata l'operazione, il sistema visualizzerà la firma grafica apposta dall'utente, provvedendo a cifrare i dati biometrici e l'hash del documento, in modo da garantire l'assoluta indissolubilità dei dati rispetto al documento PDF visualizzato e sottoscritto.
Non è pertanto consentita l'estrazione dei dati biometrici né la loro associazione ad un altro documento, diverso da quello sottoscritto. Una volta inseriti nel documento PDF, i dati biometrici vengono peraltro distrutti e cancellati sia dalla memoria applicativa che dalla memoria del sistema su cui opera l'applicazione.
Ciascun documento firmato in modalità grafometrica può essere concluso ed approvato dalla Banca con una propria firma digitale, applicabile con la stessa piattaforma Web2Sign, utilizzando tuttavia un Certificato Digitale Qualificato ottenuto da un Certification Authority ("CA") a norma, attivato tramite uno dei meccanismi di Autenticazione Strong previsti dalla nostra piattaforma, previa una validazione visiva tra l'immagine raccolta grafometricamente e quella depositata su carta (specimen) presso la Banca stessa.
Durante la sottoscrizione con firma grafometrica, viene generato per ogni firma un nuovo Certificato intestato al firmatario. Tale Certificato permette di effettuare, a tutti gli effetti, una firma PDF del documento, in modo da renderla visibile e verificabile con gli strumenti più diffusi (Client Adobe, ecc.).
Il processo di firma prevede la creazione di una busta Cades, tipicamente utilizzata per le firme PDF, all'interno della quale sono inseriti la firma dell'hash del documento originale e, come ulteriori attributi della firma, una sorta di blob cifrato, costituito dall'hash stesso e dai dati biometrici. Tale blob viene a sua volta firmato ed inserito nella busta Cades.

3.
Descrizione delle caratteristiche del sistema che garantiscono il controllo esclusivo del firmatario sul sistema di generazione della firma
Durante la fase di firma, il sistema è sotto il controllo esclusivo del firmatario. Lo schermo del dispositivo di firma (o "tablet") mostra il documento completo, consentendo al firmatario di verificare personalmente i propri dati anagrafici ed ogni dettaglio contrattuale mediante scorrimento. Durante l'apposizione della firma, lo schermo del tablet rappresenta in tempo reale il segno grafico tracciato ed apposite funzioni consentono al firmatario di cancellare in caso di errori. L'operatore bancario ovvero, in caso di offerta fuori sede, il Promotore Finanziario non possono in alcun modo interferire sino alla conclusione dell'operazione o sino all'annullamento del processo. L'applicazione di firma registra i parametri comportamentali del firmatario senza che nessun altro interlocutore – sia esso una persona o un processo – possa agire sul documento, nel momento in cui il firmatario appone la firma il tratto grafico viene visualizzato e direttamente cifrate le informazioni nello spazio dedicato alla firma, le informazioni al termine dell'apposizione della firma vengono immediatamente rimosse dal sistema utilizzato, memoria ram e fisica, in questo modo non possono essere oggetto di altro utilizzo ma ogni firma successiva sarà costituita da altri nuovi parametri che subiranno comunque il medesimo trattamento. Oltre alla cancellazione immediata di tutte le informazioni grafometriche, i livelli di sicurezza degli strumenti utilizzati ("devices") e il collegamento cifrato permettono di garantire l'assoluta impossibilità di catturare detti dati da altre figure o processi.

4.
Descrizione delle caratteristiche del sistema che garantiscono di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma
Le tecnologie di firma elettronica utilizzate – sia per la firma grafometrica che per le "firme tecniche", cfr. n. 8, *infra)* includono le impronte informatiche (c. d. "hash") del contenuto soggetto a sottoscrizione. Il controllo della corrispondenza tra un'impronta ricalcolata e quella "sigillata" all'interno delle firme permette di verificare che il documento informatico sottoscritto non abbia

subito modifiche dopo l'apposizione della firma. Generalmente, al termine delle operazioni di firma (dei clienti e dei promotori finanziari), la Banca verifica visivamente le firme grafiche apposte dai firmatari e "chiude" il documento informatico con l'apposizione sul documento di una propria firma digitale, utilizzando la rappresentazione di tipo PDF/A, portandolo successivamente in conservazione sostitutiva.

5.
La descrizione delle caratteristiche del sistema che garantiscono la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto
All'atto della presentazione del documento per la firma, il firmatario può visualizzare il contenuto in tutte le sue parti, con apposite funzioni di posizionamento e ingrandimento. Le caratteristiche del dispositivo di *firma elettronica avanzata* sono opportunamente scelte per garantire la miglior leggibilità.
Successivamente il firmatario potrà, nelle forme eventualmente convenute con la Banca, visualizzare il documento elettronico per mezzo di uno strumento informatico standard, di cui avrà piena disponibilità, su supporto duraturo che permetterà la conservazione e la stampa del documento in ogni momento (es. software gratuito PDF Reader).

6.
Descrizione delle caratteristiche del sistema che garantiscono l'individuazione del soggetto erogatore della soluzione di firma elettronica avanzata.
Il certificato di firma della *firma elettronica avanzata* individua il soggetto erogatore del servizio ed è emesso da un'autorità di certificazione tecnica, riconducibile alla Banca, con visualizzazione della dicitura "Sudtirol Bank AG / Alto Adige Banca SpA" ("Dettagli certificato").

7.
Descrizione delle caratteristiche del sistema che garantiscono l'assenza nell'oggetto della sottoscrizione di qualunque elemento idoneo a modificarne gli atti, i fatti e i dati in esso rappresentati
I documenti prodotti dal sistema utilizzano esclusivamente formati atti a garantire l'assenza, nell'oggetto della sottoscrizione, di qualunque elemento idoneo a modificare gli atti, i fatti e i dati in essi rappresentati (formato standard ISO PDF/A).

8.
Descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al documento sottoscritto
I dati della firma vengono inseriti nel documento in una struttura, detta "vettore grafometrico", che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. L'unica chiave crittografica in grado di estrare le informazioni è in esclusivo possesso di una Certification Authority ("Namirial S.p.a."), la quale custodisce presso apparecchiature certificate la chiave in oggetto ed eventualmente porzioni di essa anche presso Notai. Il sistema appone, per ogni firma eseguita, una corrispondente "firma tecnica" in formato standard PADES. A differenza del "vettore grafometrico" queste firme tecniche sono visibili e verificabili con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).

9.
Descrizione delle caratteristiche delle tecnologie utilizzate nel servizio di Firma Elettronica Avanzata che consentono di garantire i requisiti previsti ai precedenti punti da 1. a 8.
Il trasferimento dei dati e la loro memorizzazione nel "vettore grafometrico" è protetto con le seguenti tecnologie crittografiche:

- crittografia simmetrica standard AES con chiave a 256 bit segreta e IV condiviso per la

protezione dei dati;
Lo scambio delle informazioni biometriche tra i devices che le rilevano, siano essi signature PAD (Es: Wacom STU-520) o tablet (Es: Samsung Android o Samsung Ativ Win8), e il sistema computer/server sul quale gira l'applicazione Web2Sign viene così garantito:

- signature PAD, i devices sono collegati tramite porta USB al computer che mostra il documento da firmare; viene generata ogni volta (per ogni firma che l'utente deve apporre) una differente chiave di sessione AES 256 per cifrare i dati che, tramite cavo USB, transitano dal PAD al computer; una volta ricevuti dal computer, questi dati subiscono una nuova cifratura asimmetrica insieme all'hash del documento, come già sopra descritto,
- tablet (con monitor Wacom Digitizer), l'applicazione Web2Sign viene istanziata direttamente dai browser, esclusivamente su canale sicuro e cifrato https. Una volta ricevuti sul computer, questi dati subiscono una nuova cifratura asimmetrica insieme all'hash del documento, come già descritto.

- RSA 2048 bit con chiave privata detenuta da una terza parte per la cifratura della chiave AES. La cifratura è di tipo asimmetrico e perciò effettuata utilizzando una coppia di Chiavi/Certificato RSA 2048 rilasciati da una CA iscritta presso AGID. In particolare, per la Cifratura dei dati viene utilizzata la parte pubblica (Certificato), mentre, la decifratura degli stessi, potrà essere effettuata solo avendo diritto di accesso alla corrispettiva chiave privata, solitamente custodita in un apparato sicuro a norma, HSM o su di una Smart Card, custodita presso una cassetta di sicurezza dell'Ente stesso, di un Notaio o di una CA, garantendo così l'accesso esclusivo ad utenti che ne abbiano il diritto (Pubblico Ufficiale/Magistratura) in caso di contenzioso;
- durante la fase di firma grafometrica, viene generato per ogni firma un nuovo Certificato intestato all'utente che appone la propria firma grafometrica, il quale permette di effettuare, a tutti gli effetti, una firma PDF del documento in modo tale che sia visibile e verificabile con tutti gli strumenti di verifica più diffusi (per esempio, Client Adobe); viene dunque creata una PKI/CA apposita per lo scopo sopra descritto. Il processo di firma avviene con le seguenti modalità:
  - viene creata una busta Cades tipicamente utilizzata per le firme PDF,
  - all'interno di essa vengono inseriti i) la firma dell'hash del documento originale e, come ulteriori attributi della firma e ii) una sorta di blob cifrato costituito dall'hash del documento e dai dati biometrici,
  - detto blob viene anch'esso firmato ed inserito nella busta Cades, terminando così l'attività di firma dell'utente grafometrico;
- firma digitale della Banca del documento PDF con firma PADES (opzionale).

10.
Descrizione delle modalità attraverso cui i clienti possono richiedere copia gratuita del modulo di adesione, da questi sottoscritto, al servizio di firma elettronica avanzata.
I clienti possono richiedere gratuitamente alla Banca una copia cartacea del modulo di adesione al servizio di *firma elettronica avanzata* nonché degli atti e dei documenti bancari e finanziari così sottoscritti.

11.
Descrizione delle modalità attraverso cui i clienti possono richiedere le informazioni di cui ai precedenti punti da 1. a 8.
Il presente documento, contenente le informazioni relative alle caratteristiche del servizio di *firma elettronica avanzata* ed alle tecnologie su cui questo si basa, è pubblicato in evidenza nella home page del sito internet della Banca *(www.suedtirolbank.eu),* risultando in tal modo sempre disponibile per i clienti e il pubblico in generale.
Per ogni ulteriore informazione, è comunque possibile rivolgersi alla Banca.

12.
Descrizione della copertura assicurativa che la Banca è tenuta a stipulare per la responsabilità civile da danno a terzi per un ammontare non inferiore a euro cinquecentomila.
La Alto Adige Banca SpA / Südtirol Bank AG, conformemente alla normativa vigente, ha stipulato una polizza assicurativa rilasciata da Generali Italia spa (polizza numero 350201084) con copertura assicurativa a partire dal 24/12/2015, per la responsabilità civile da danno a terzi eventualmente derivante dalla fornitura del servizio di firma elettronica avanzata.

GLOSSARIO

Piattaforma Web2Sign	Piattaforma realizzata dall'outsourcer per la fornitura in modalità fidata e sicura di servizi interoperabili con i dispositivi utilizzati dagli utenti, che garantisce l'integrità, l'immodificabilità e la sicurezza dei documenti pdf dalla stessa gestiti.
Certificato Digitale Qualificato	Certificato utilizzato per l'apposizione di firma digitale qualificata rilasciato esclusivamente da enti preposti e certificati per questa attività (CA)
CA	Autorità certificata accreditata presso AGID per il rilascio di certificati qualificati di firma digitale e/o crittografia
Meccanismi di Autenticazione Strong	Generalmente basati su due fattori, un PIN statico a cui associare un PIN dinamico o OTP (password usa e getta) generato tramite appositi token ovvero altri strumenti, oppure ricevuto via SMS.
Busta Cades	Busta crittografica che contiene le informazioni relative ad un processo di firma elettronica, avanzata o digitale.
Hash	Funzione matematica che genera, a partire da un'evidenza informatica, un'impronta in modo tale che risulti impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Blob cifrato	Campo di database Oracle che contiene un file
Formato standard PADES (firma PADES)	PAdES è l'acronimo di "PDF Advanced Electronic Signature". Si tratta di una firma elettronica che, basando sul formato PDF le modalità e le tecnologie per l'identificazione dell'autore del documento e per le informazioni contenute nel documento originale (secondo la norma ETSI TS 102 778 e lo standard ISO 32000-1), garantisce le qualità necessarie per essere definita "firma elettronica avanzata" (avente valore legale).
Vettore grafometrico	Record contenente le informazioni grafometriche registrate durante l'apposizione di una firma grafometrica e cifrate
AGID	Agenzia per l'Italia Digitale, istituita ai sensi dell'articolo 19 del decreto legge 22 giugno 2012, n. 83, convertito in legge, con modificazioni, dall'art. 1 della legge 7 agosto 2012, n. 134, e successive modifiche e integrazioni, ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria e persegue, nella sua attività, gli obiettivi di efficacia, efficienza, imparzialità, semplificazione e partecipazione dei cittadini e delle imprese.
PKI/CA	Infrastruttura di sicurezza basata sull'utilizzo di chiavi pubbliche e private (RSA) che ne gestisce il ciclo di vita, dalla registrazione, rilascio eventuale sospensione o revoca sino alla regolare scadenza.