CARATTERISTICHE TECNOLOGICHE DEL SISTEMA DI FIRMA ELETTRONICA AVANZATA UTILIZZATO IN AVEPA

Nota introduttiva

Questo documento descrive le caratteristiche funzionali e tecnologiche del servizio di firma elettronica avanzata reso disponibile dall'AVEPA per la sottoscrizione di alcuni documenti informatici da parte degli utenti. Il documento è redatto ai sensi dell'articolo 57, lettera e) del decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" (pubblicato in Gazzetta Ufficiale n. 117 del 21.05.2013) ed è pubblicato nel sito web istituzionale dell'AVEPA (*www.avepa.it/fea*), risultando in tal modo sempre aggiornato e disponibile.

Descrizione della soluzione di firma elettronica avanzata

Il processo di firma elettronica avanzata (di seguito "FEA") utilizzato dall'Agenzia veneta per i pagamenti in agricoltura (di seguito "AVEPA") è basato sull'utilizzo della **firma grafometrica** e prevede l'apposizione della firma da parte dell'utente su una tavoletta grafica attraverso un'apposita penna elettronica ad essa collegata. La tavoletta rileva alcuni dati biometrici di tipo comportamentale dell'utente (velocità, accelerazione, pressione, ritmo e movimento con cui viene eseguita la firma) e li utilizza per attribuire univocamente la firma apposta al soggetto che l'ha eseguita. A tal fine, la tavoletta utilizza appositi software che hanno il compito di governare le periferiche ed acquisire i dati di biometria comportamentale.

L'utilizzo congiunto della tavoletta grafica, dello specifico software e delle soluzioni di certificazione consente di creare un documento informatico che contiene al suo interno tutti gli elementi necessari a stabilirne l'autenticità, essendo formato dal contenuto del documento sottoscritto e dai **dati biometrici cifrati** relativi alla sottoscrizione dell'utente. Tali dati non sono memorizzati, organizzati e conservati in un database, ma rimangono esclusivamente all'interno del documento informatico sottoscritto in **forma criptata**.

Caratteristiche tecnologiche del sistema di firma elettronica avanzata

Identificazione del firmatario del documento

Prima di raccogliere l'adesione dell'utente al servizio di firma elettronica avanzata, il personale dell'AVEPA (o di un suo organismo delegato) identifica l'utente attraverso un documento di identità originale in corso di validità.

Connessione univoca della firma al firmatario

La connessione univoca della firma al firmatario è garantita dall'identificazione dell'utente effettuata da parte del personale dell'AVEPA (o di un suo organismo delegato) che, secondo quanto previsto dalla normativa vigente, è sempre tenuto a verificare l'identità del soggetto che sta mettendo in atto la sottoscrizione. La connessione univoca è inoltre garantita dal fatto che la firma è apposta dall'utente, di suo pugno ed in presenza di personale dell'AVEPA (o di un suo organismo delegato), tracciandola con una penna elettronica su un'apposita tavoletta grafica in grado di rilevare, acquisire e registrare le caratteristiche dinamiche della firma autografa in forma di dati biometrici di tipo comportamentale quali la velocità, l'accelerazione, la pressione, il ritmo e il movimento con cui viene eseguita la firma.

Garanzia del controllo esclusivo del firmatario del sistema di generazione della firma

Durante la fase di firma, il sistema è sotto il controllo esclusivo dell'utente. Lo schermo del personal computer collegato alla tavoletta grafica consente all'utente di visualizzare il documento integrale e di verificare personalmente i propri dati e il contenuto del documento da sottoscrivere. Durante l'apposizione della firma, lo schermo del personal computer collegato alla tavoletta grafica rappresenta in tempo reale il segno grafico tracciato dall'utente sulla tavoletta e apposite funzioni consentono al firmatario, in caso di errori, di cancellare la propria firma.

Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma

L'integrità del documento informatico è garantita dalla procedura di inserimento dei dati biometrici (criptati) del firmatario nel documento PDF e dalla successiva marcatura temporale digitale apposta alla chiusura del processo. Le tecnologie di firma elettronica utilizzate includono le impronte informatiche (*hash*) del contenuto del documento sottoscritto. Il controllo della corrispondenza tra un'impronta ricalcolata e quella criptata all'interno del documento informatico permette di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Il sistema appone inoltre su ciascun documento sottoscritto la firma digitale del gestore del servizio di firma elettronica avanzata (si tratta di una firma digitale "tecnica" che funge da "sigillo" ad ulteriore garanzia dell'integrità del documento sottoscritto).

Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto

Prima di apporre la propria firma sul documento informatico da sottoscrivere, l'utente può visualizzare il suo contenuto in tutte le sue parti, con apposite funzioni di posizionamento e ingrandimento tramite il personal computer al quale è collegata la tavoletta grafica. Al termine del processo, il documento informatico viene inviato alla casella di posta elettronica certificata (PEC) dichiarata dall'utente e registrata nel rispettivo fascicolo aziendale. Una copia del documento sottoscritto viene inoltre archiviata nel sistema informativo dell'AVEPA, dove rimane a disposizione dell'utente per l'eventuale successiva consultazione.

Individuazione del soggetto che eroga la soluzione di firma elettronica avanzata

La soluzione di firma elettronica avanzata utilizzata in AVEPA è erogata da Postel spa (*www.postel.it*).

Assenza nell'oggetto della sottoscrizione di qualunque elemento idoneo a modificarne gli atti, i fatti e i dati in esso rappresentati

La soluzione di firma elettronica avanzata resa disponibile dall'AVEPA utilizza esclusivamente formati di file conformi alla normativa vigente e idonei a garantire l'assenza, nel documento oggetto di sottoscrizione, di qualunque elemento che possa modificare gli atti, i fatti e i dati in esso rappresentati. Attualmente, i documenti sottoscritti con firma elettronica avanzata sono registrati in formato standard PDF.

Connessione univoca della firma al documento sottoscritto

I dati della firma elettronica avanzata vengono inseriti nel documento in una struttura detta "vettore biometrico" che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta tramite un sistema di crittografia, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. L'unica chiave crittografica in grado di estrarre le informazioni è in esclusivo possesso di Postel spa e potrà essere usata in sede di perizia per attestare l'autenticità del documento e della sottoscrizione apposta, o comunque quando previsto dalla normativa vigente. I dati biometrici associati alla firma grafometrica sono pertanto cifrati e criptati direttamente mediante un certificato digitale, la cui chiave non è in diretto possesso dell'AVEPA, e sono legati indissolubilmente al documento informatico sottoscritto, che viene inoltre "sigillato" con la firma digitale apposta dal gestore del servizio di firma elettronica avanzata (Postel spa).

Tecnologie utilizzate dal sistema di firma elettronica avanzata

La soluzione tecnologica utilizzata dall'AVEPA per il servizio di firma elettronica avanzata si compone di:

- una postazione d'ufficio dotata di personal computer al quale è collegata un'apposita tavoletta grafica collegata e un monitor per la visualizzazione del documento informatico da sottoscrivere;
- le applicazioni informatiche che generano il documento da sottoscrivere;
- la piattaforma di firma grafometrica integrata con i servizi gestionali, di certificazione digitale e per la conservazione del documento informatico.

Il trasferimento dei dati e la loro memorizzazione nel “vettore biometrico” sono protetti con le seguenti tecnologie crittografiche:

- i dati biometrici vengono rilevati tramite dispositivo WACOM STU 500, che li codifica all’origine con algoritmo AES a 128bit; la comunicazione con i server avviene su canale HTTPS.
- i dati biometrici vengono cifrati con algoritmo RSA con chiave a 2048bit unitamente all’hash del documento da firmare, calcolato con algoritmo SHA-256.