COS'é
Il Sistema denominato Sigillo è un sistema che consentirà agli utenti che interagiscono con l'Amministrazione (personale supplente, aspiranti docenti, docenti, ATA, studenti, famiglie) di appore la firma elettronica sui documenti prodotti dall'amministrazione e dalle scuole senza la necessità di utilizzare un sistema di firma elettronica qualificata che necessita di certificato di firma digitale emesso da una CA.

Tale sistema potrà essere utilizzato nei rapporti intrattenuti tra i cittadini ed il MI, soggetto erogatore della soluzione tecnologica ai sensi della normativa vigente, e nei rapporti intrattenuti tra i cittadini e le istituzioni scolastiche che per il tramite del MI, offriranno i propri servizi utilizzando la Firma Elettronica Avanzata (FEA).

La FEA è equivalente informatico della firma autografa apposta su un documento cartaceo; consente di ridurre i tempi e costi di redazione di un documento e riduce i rischi falsificazione rispetto alla firma autografa.
Poiché rientra nel piano di dematerializzazione dei processi a supporto dei procedimenti amministrativi, il servizio di FEA del Ministero dell'Istruzione (di seguito: servizio di Firma Elettronica Avanzata) è in linea con il programma pluriennale di digitalizzazione della Pubblica Amministrazione.

Il servizio di Firma Elettronica Avanzata consente che la firma presenti le seguenti caratteristiche:

- è connessa unicamente al firmatario
- è idonea a identificare il firmatario
- 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
- è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati

AUTENTICAZIONE TRAMITE SPID
La soluzione individuata, attraverso particolari accorgimenti, sfrutta il processo di autenticazione con identità digitale SPID e fornisce pertanto un elevato grado di sicurezza e non ripudio delle firme apposte.

Nel caso specifico i cittadini che devono sottoscrivere un documento devono dotarsi di una identità digitale SPID di livello 2 senza avere la necessità di dotarsi di un certificato digitale e di dover seguire il lungo processo di *enrollment* che l'assegnazione di quest'ultimo comporta. Il riconoscimento forte del soggetto è demandato al processo di assegnazione dell'identità digitale SPID effettuata dagli Identity Provider e la possibilità di legare la firma elettronica ad una autenticazione SPID aggiunge le caratteristiche di non ripudiabilità al documento firmato con questo strumento.

Il sistema SPID si basa sul protocollo di identità federata SAML v.2.0. Tale protocollo prevede che la richiesta di autenticazione da parte del Service Provider verso l'Identity Provider, avvenga attraverso una struttura XML firmata elettronicamente con il certificato del Service Provider. Allo stesso modo la risposta da parte dell'Identity Provider viene anch'essa firmata elettronicamente con il certificato dell'Identity Provider.

La soluzione individuata lega in modo indissolubile il firmatario ai documenti firmati attraverso elementi certificati da entità esterne trusted e opponibili a terzi. Nella fattispecie la soluzione lega l'hash del documento con le asserzioni SAML del processo di autenticazione SPID.

PROCESSO DI FIRMA ELETTRONICA AVANZATA

L'applicazione che produce il documento da firmare, lo invia a Sigillo per permettere all'utente di apporre la propria firma, e indica se al momento della firma è necessario applicare una marca temporale.

Il processo di firma prevede i seguenti passi:

- l'utente accede al servizio di FEA utilizzando le proprie credenziali SPID (il servizio FEA sarà un servizio SPID Only e non sarà accessibile tramite le credenziali IAM, se l'utente ha già effettuato un accesso al sistema di SSO tramite la propria identità SPID non verrà richiesta una nuova autenticazione). In caso di primo accesso al sistema FEA l'utente accetta i termini e condizioni per l'utilizzo dello strumento di firma elettronica come previsto dalla normativa
- l'utente tramite una apposita *dashboard* prende visione del documento e della/delle firme che l'applicazione ha richiesto che vengano apposte su di esso
- l'utente seleziona esplicitamente le firme che intende apporre sul documento (potendo gestire casi particolari come la sottoscrizione di clausole vessatorie o il consenso al trattamento dati personali)e richiede di apporre la propria Firma Elettronica Avanzata
- il sistema calcola l'hash del documento da firmare e genera una richiesta di autenticazione verso l'IdP utilizzato per accedere alla piattaforma FEA inserendo l'hash del documento nel campo ID (hash + stringa random) della Authentication Request
- l'Authentication Request viene firmata con il certificato di federazione del MI e viene inviata all'Identity Provider tramite il browser dell'utente
- l'utente viene reindirizzato sulla pagina di login dell'Identity Provider ed effettua un accesso utilizzando le proprie credenziali SPID di Livello2
- al termine del processo di autenticazione l'IdP produce una Response firmata elettronicamente contenente le informazioni dell'utente che ha effettuato la firma (Codice Fiscale e SPIDCode) ed il campo ID dell'Authentication Request all'interno del campo InResponseTO
- il sistema, verifica che l'identità autenticata con SPID sia corrispondente a quella del firmatario tramite il Codice fiscale
- a garanzia del processo di sottoscrizione viene apposto sul documento il Sigillo Digitale del MI, il sigillo oltre che in formato digitale viene apposto anche in forma grafica in tutti i punti in cui è prevista la firma dell'utente, l'immagine inserita conterrà i dati di riferimento dell'utente che ha posto la propria Firma Elettronica Avanzata; se richiesto dall'applicazione che ha caricato il documento, per garantire la validità temporale contestualmente al sigillo viene apposta anche una marcatura temporale
- sul sistema di FEA si memorizza il documento firmato e tutte le asserzioni SPID che legano l'hash del documento firmato all'identità SPID dell'utente che ha apposto la firma per permettere successive verifiche; inoltre i documenti vengono memorizzati su file system all'interno di una struttura gerarchica di cartelle, in modo da rendere efficienti le operazioni di ricerca
- l'utente ha la possibilità di effettuare il download del documento firmato, la cui integrità e autenticità saranno garantite dal sigillo digitale del MI mentre la marca temporale, se apposta, garantirà la validità nel tempo associando data e ora di quando è stato apposto il sigillo

PERIMETRO DI UTILIZZO DEL SERVIZIO DI FIRMA ELETTRONICA AVANZATA

La FEA è utilizzata nell'ambito delle sottoscrizioni documentali all'interno dei procedimenti amministrativi del Ministero dell'Istruzione e per la fruizione dei servizi da Esso offerti; la FEA integra il requisito di garanzia di opponibilità a terzi della c.d. firma in forma scritta, avendone lo stesso valore legale ai sensi del codice civile.

GARANZIA DEL PROCESSO DI SOTTOSCRIZIONE TRAMITE IL SERVIZIO DI FIRMA ELETTRONICA AVANZATA

A garanzia del processo di sottoscrizione tramite FEA potrebbe essere apposto sul documento sottoscritto dall'utente un Sigillo digitale del Ministero dell'Istruzione; il sigillo oltre che in formato digitale viene apposto anche in forma grafica in tutti i punti in cui è prevista la firma dell'utente, l'immagine inserita conterrà i dati di riferimento dell'utente che ha posto la propria Firma Elettronica Avanzata; qualora previsto dal procedimento amministrativo per il quale si sta firmando il documento, è apposta una marca temporale associata alla sottoscrizione.

Il sigillo elettronico per il Ministero dell'Istruzione è omologo della firma elettronica rilasciata alle persone fisiche, con la quale condivide la definizione fino allo scopo operativo finale e serve a garantire l'origine e l'integrità del documento sigillato.

L'apposizione del sigillo sul documento firmato con il sistema di FEA permette di garantire la possibilità di verificare che il documento elettronicamente sottoscritto non abbia subito modifiche dopo l'apposizione della firma; durante l'apposizione del Sigillo, sono inseriti in forma grafica i dati dell'utente che ha apposto la propria Firma Elettronica Avanzata: i dati sono visualizzati sul documento firmato nei punti in cui è prevista l'apposizione della firma.

Il sigillo è applicato tante volte quante sono le firme da apporre sul documento.

LIMITAZIONI D'USO DEL SERVIZIO DI FIRMA ELETTRONICA AVANZATA

L'utente può utilizzare il servizio di FEA esclusivamente per sottoscrivere documenti afferenti a servizi e procedimenti amministrativi del Ministero dell'Istruzione.

FUNZIONALITÀ UTENTE DI SIGILLO

Il servizio di FEA mette a disposizione le seguenti funzionalità per l'utente:

- richiesta di firma asincrona di un documento
- richiesta di firma sincrona di un documento
- verifica dello stato della firma di un documento
- download di un documento firmato
- revoca della richiesta di firma di un documento
- notifica dell'avvenuta firma di un documento

RISERVATEZZA E INTEGRITÀ

Sigillo abbina indissolubilmente l'oggetto della sottoscrizione (attraverso l'hash del documento) con il processo di autenticazione SPID e dunque l'identità del firmatario; tale garanzia è ancora più forte in quanto viene coinvolto un soggetto esterno 'trusted', l'Identity Provider, che è indipendente dal gestore del servizio di FEA (Ministero dell'Istruzione), a vantaggio del conseguimento della non ripudiabilità.

CONNESSIONE UNIVOCA DELLA FIRMA AL FIRMATARIO TRAMITE FEA

L'identificazione del firmatario del documento è garantita dall'identità SPID; lo SPID Manager garantisce la connessione univoca della firma al firmatario tramite l'asserzione firmata ottenuta dall'IdP dove sono presenti l'hash del documento firmato e l'identificativo dell'utente firmatario.

ASSENZA DI QUALUNQUE ELEMENTO NEI DOCUMENTI ATTO A MODIFICARNE GLI ATTI, FATTI O DATI NELLO STESSO RAPPRESENTATI

Il formato elettronico dei documenti sottoscrivibili tramite FEA è il PDF, che garantisce l'impossibilità di inserire nello stesso documento elementi in grado di modificarne i contenuti o di alterare la firma medesima.

CONNESSIONE UNIVOCA DELLA FIRMA AI DOCUMENTI SOTTOSCRITTI TRAMITE FEA
Il sistema di FEA lega l'hash del documento con le asserzioni SAML del processo di autenticazione SPID, in tal modo associando in modo univoco il firmatario ai documenti firmati attraverso elementi certificati da entità esterne *trusted* e opponibili a terzi.

Scarica documento completo