Servizio di Firma Elettronica Avanzata: documento tecnico

In questo documento viene descritto, così come previsto dalla normativa, il processo di emissione della firma elettronica avanzata (di seguito FEA) di Avvera, utilizzata per la sottoscrizione, mediante canali e tecniche di comunicazione a distanza, dei documenti informatici che costituiscono la richiesta di concessione dei prodotti finanziari di Avvera S.p.A., tra i quali il contratto di credito denominato "SplittyPay by Avvera" (di seguito, la "Dilazione" o anche "SplittyPay")

.

1. Identificazione del firmatario del documento

L'utente, in fase di primo accesso, viene indirizzato verso la procedura di registrazione che richiede l'indicazione del numero di cellulare (user name) ed una password a scelta dell'utente. Successivamente viene inviato un OTP via SMS da inserire nella *web app* SplittyPay, al fine di verificare la correttezza del numero di telefono fornito.

1.1. Onboarding: verifica identità

Una volta effettuato la pre-registrazione o effettuato il login l'utente non ancora identificato è indirizzato alla procedura di onboarding per il riconoscimento digitale/self. Potrà scegliere tra due modalità: SPID rafforzato o Video Selfie con acquisizione documento di identità valido.

SPID rafforzato

L'utente si autenticherà presso il proprio identity provider tramite l'utilizzo di credenziali di livello II, che passerà alla procedura di onboarding tutti i dati anagrafici, di residenza e del documento di riconoscimento.

Video Selfie

L'utente attraverso una procedura guidata fornirà una immagine fronte e retro di un documento di riconoscimento in corso di validità (carta identità elettronica, patente o passaporto) e successivamente verrà invitato all'acquisizione di un video selfie dinamico del proprio volto. La procedura analizzerà i dati acquisiti e attraverso algoritmi certificati verificherà l'autenticità dei documenti e la corrispondenza biometrica del video selfie con la fotografia presente sul documento.

1.2. Onboarding verifica e conferma

L'utente viene inviato ad aggiungere ulteriori dati ai fini dei controlli antiriciclaggio (PEP, occupazione, ecc..) e a confermare i dati acquisiti (dati di residenza)

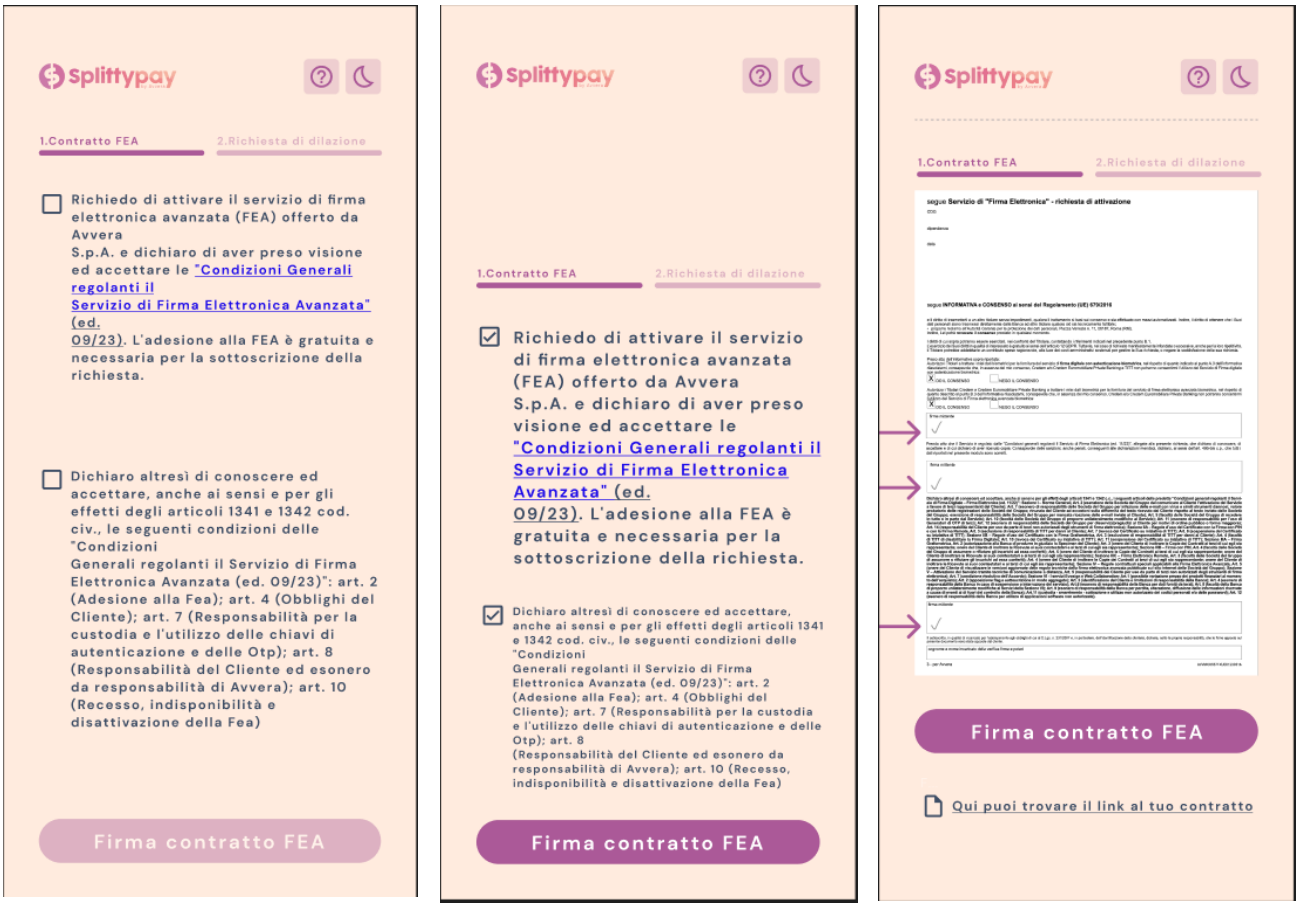
1.3. Onboarding controlli trasversali

I dati anagrafici, di residenza ed identificativi dei documenti raccolti dalle due procedure verranno inoltre sottoposti ad ulteriori verifiche di congruenza e validità. Se i controlli daranno semaforo verde la procedura d'identificazione si concluderà positivamente confermando l'identità dell'utente.

2. Adesione al servizio di FEA

Una volta conclusasi positivamente la procedura di onboarding, solo al momento della prima operazione/pratica, all'interno dell'area riservata viene proposta all'utente la richiesta di attivazione del servizio Fea.

All’utente viene mostrata la richiesta di attivazione del servizio Fea, con evidenza dei singoli punti firma, e proposto il pulsante per la firma dello stessa.

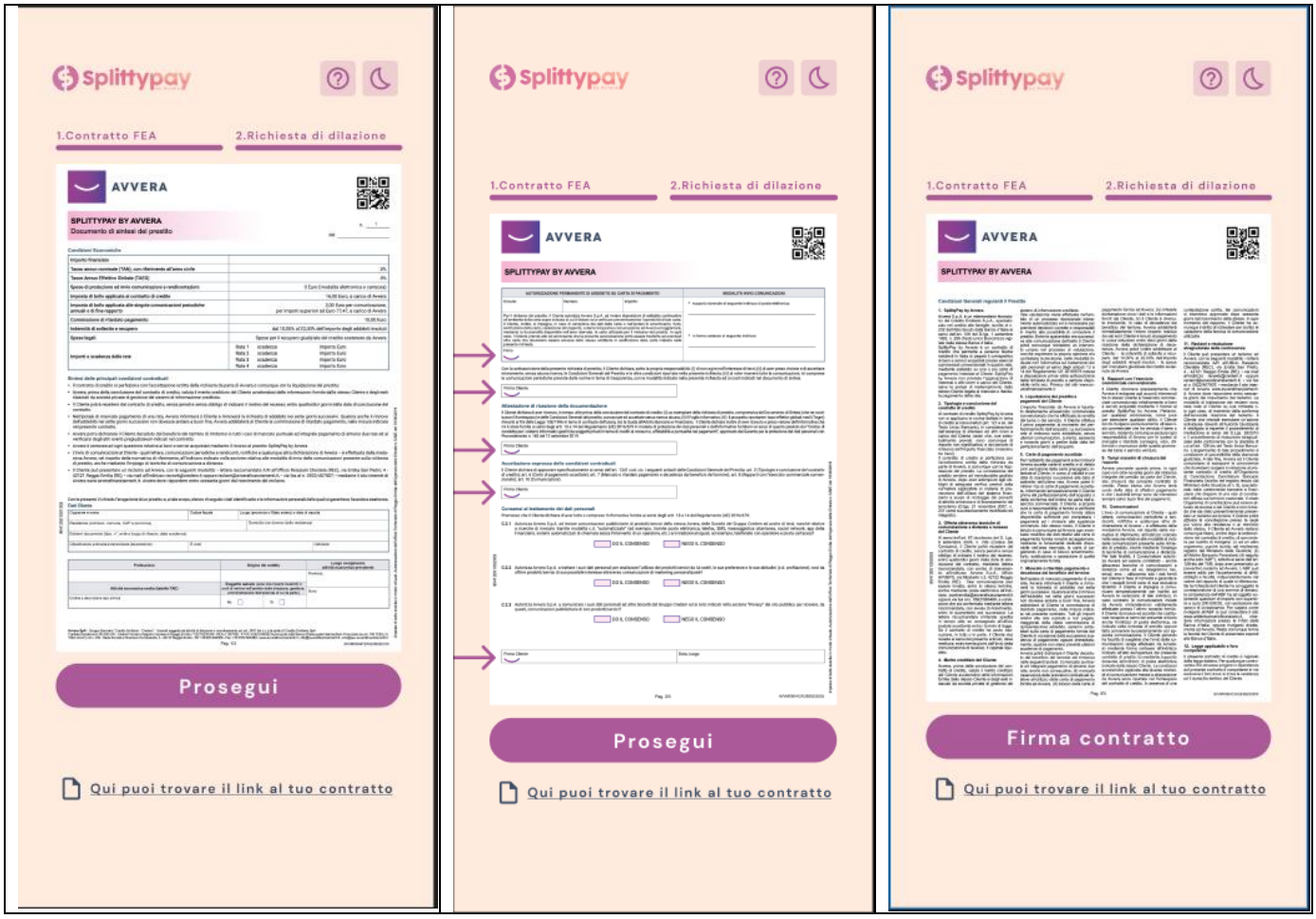


Al temine viene apposta sul documento una firma elettronica semplice (di seguito FES) in formato PadeS per ogni punto firma

3. Connessione univoca della firma all’utente

All’utente viene proposta la modulistica contrattuale per la richiesta di Dilazione, come meglio descritto di seguito. Viene richiesta prima la modalità di ricezione della documentazione, successivamente all’utente viene mostrato il piano di rimborso della dilazione, col dettaglio delle singole rate.

Una volta confermato l'utente visualizza la richiesta di Dilazione e può procedere col processo di firma. Il sistema evidenzia i punti firma, e consente all'utente l'apposizione della firma elettronica mediante l'inserimento di un codice numerico OTP, trasmesso via SMS al dispositivo mobile registrato e verificato.


Splittypay
1.Contratto FEA
2.Richiesta di dilazione
AVVERA
SPLITTYPAY BY AVVERA
Documento di sintesi del prestito
Prosegui
Qui puoi trovare il link al tuo contratto
Splittypay
1.Contratto FEA
2.Richiesta di dilazione
AVVERA
SPLITTYPAY BY AVVERA
Prosegui
Qui puoi trovare il link al tuo contratto
Splittypay
1.Contratto FEA
2.Richiesta di dilazione
AVVERA
SPLITTYPAY BY AVVERA
Firma contratto
Qui puoi trovare il link al tuo contratto

Al termine viene apposta sul documento una Fea iin formato PadeS per ogni punto firma della richiesta di Dilazione e nel caso di prima pratica, anche sul contratto di adesione al servizio Fea già firmato con FES.

Ciascun certificato emesso sarà utilizzabile esclusivamente per un’unica sessione di firma e, pertanto, per successive richieste di dilazione, sarà emesso un nuovo certificato.

4. Controllo esclusivo dell’utente del sistema di generazione della firma

L’utente arriva alla sezione di firma documento solo all’interno dell'area riservata, alla quale si accede inserendo nome utente e password. Al momento della firma il certificato di firma, che pur non essendo qualificato ha le medesime caratteristiche tecniche, viene rilasciato solo a seguito dell’inserimento di un codice OTP ricevuto sul numero di cellulare certificato. Il codice OTP ricevuto via SMS garantisce il controllo esclusivo dell’utente sul sistema di firma.

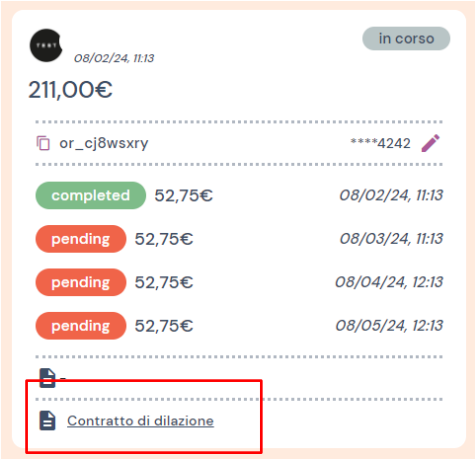
5. Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l’apposizione della firma

Il documento in formato PDF, che viene sottoscritto dal firmatario, non presenta al proprio interno elementi dinamici. Le firme apposte, uno per ogni punto firma, evidenziati all’utente prima della firma, sono in formato PadeS, così come previsto dalla normativa vigente.

Terminata la procedura di firma in qualsiasi momento potrà essere verificata l’integrità del documento con Adobe Reader o qualsiasi software di verifica firma.

6. Possibilità per l’utente di ottenere evidenza di quanto sottoscritto

Dopo la firma di un documento, l’utente riceve un avviso via mail della pubblicazione del documento firmato nella propria area riservata. Attraverso nome utente e password l’utente può accedere alla propria area riservata e visualizzare i documenti sottoscritti tramite Fea.



7. Assenza nell’oggetto della sottoscrizione di qualunque elemento idoneo a modificarne il contenuto rappresentato

Il documento in formato PDF, che viene sottoscritto dal firmatario, non presenta al proprio interno elementi dinamici che possono alterare il contenuto rappresentato senza che l’integrità della firma venga compromessa. Le firme apposte, una per ogni punto firma, evidenziati all’utente prima della firma, sono in formato PadeS, così come previsto dalla normativa vigente e garantiscono l’immodificabilità e la rappresentazione statica nel tempo.

8. Connessione univoca della firma al documento sottoscritto con FEA

Il certificato viene emesso contestualmente all'inserimento dell'OTP da parte dell'utente all'interno dell'area riservata, e viene utilizzato unicamente per l'apposizione della firma sul documento visualizzato in quel momento. Questo certificato non potrà più essere utilizzato in alcun modo per altre firme.

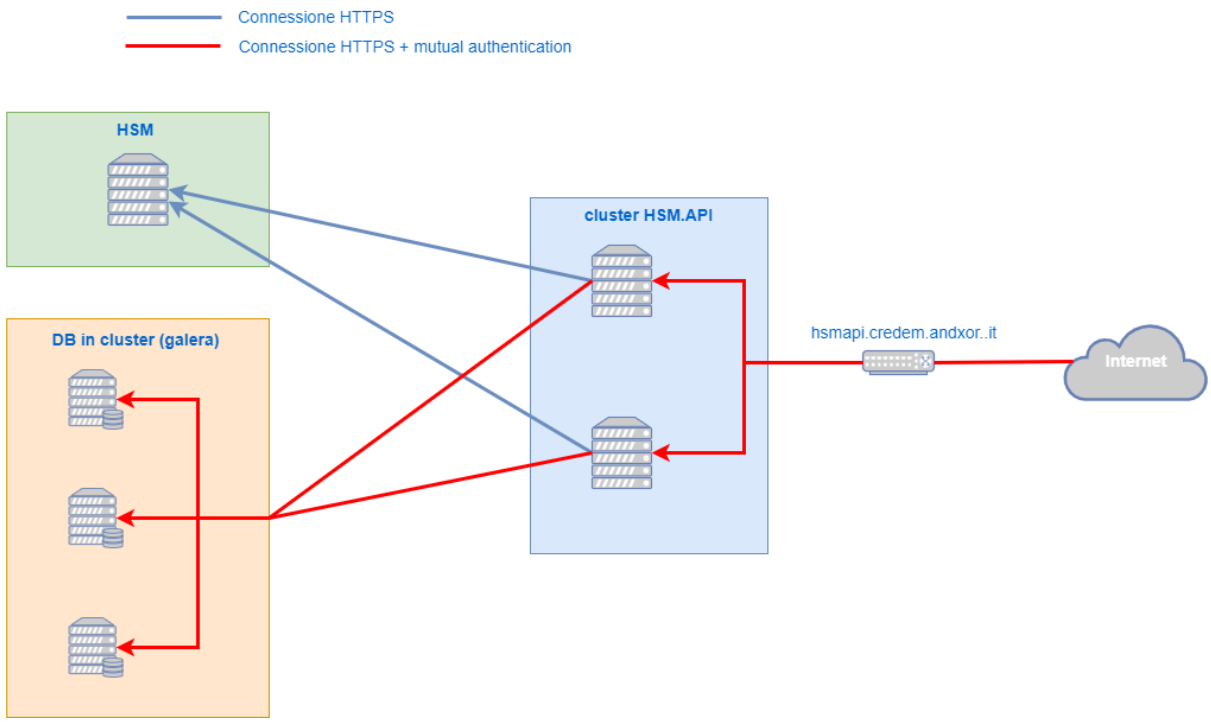
9. Architettura e servizi della soluzione di FEA

Architettura

La soluzione implementata per Avvera prevede le seguenti componenti:

- **HSM.API**: applicazione che espone una serie di API per la gestione di certificati e per le firme di documenti, pensate secondo la filosofia REST.
  L'applicazione è in HA ed è installata su due macchine distinte
- **MariaDB/Galera**: Database in cluster, installato su tre macchine distinte
- **HSM**: Server che contiene le chiavi e i certificati di firma. Questo serve non è in HA, ma è attivo un sistema di backup che effettua una snapshot dell'intera macchina ogni 30 minuti. Le snapshot vengono memorizzate su diverse macchine geograficamente distribuite, secondo quanto disposto dalla normativa sui dispositivi sicuri HSM, utilizzati per la firma digitale. La normativa prevede il divieto di duplicazione delle chiavi private ma ne consente il backup e restore al momento opportuno.

Di seguito uno schema architetturale della soluzione implementata.



Tutti i servizi rispondono esclusivamente su canale sicuro (HTTPS) con TLS 1.2+.

Le connessioni in rosso prevedono l'utilizzo di Mutual Authentication

Il cluster Galera non è esposto su internet e ci sono regole firewall che permettono l'accesso al cluster solamente ai server che hanno necessità di accedervi limitatamente alla porta designata.
Su tutti i server è installato FreeBSD 14.0; tutti i software sono installati nelle loro versioni supportate e il processo di patching è continuo.

Le utenze applicative utilizzate dai vari servizi (API, DB, HSM) hanno privilegi minimi. Gli utenti applicativi sono diversi per applicazione e hanno visibilità limitata ai dati di propria competenza
Sul DB non vengono memorizzati dati sensibili.
Le chiavi generate per i certificati FEA sono chiavi RSA 2048. Le chiavi sono utilizzabili previo inserimento di un PIN statico oppure mediante autenticazione a due fattori. In tal caso il primo fattore è sempre costituito da un PIN statico; il secondo fattore è un OTP che può essere inviato via mail o via SMS.
La scelta del tipo di autenticazione legata alla coppia chiave/certificato

LOG e conservazione digitale

I servizi di firma sono fruibili attraverso API rest, rese disponibili con Mutual Authetication. I LOG (audit trail) delle operazioni, lato HSM e lato applicativo, per le fasi di firma, vengono raccolti e mandati in conservazione digitale..