Sistema **F**irma **I**ntegrata **A**vanzata

Componenti del Sistema

Il sistema è composto da un modulo server che comprende la componente di firma e la componente di gestione dei Webservices per l'integrazione operativa. Il sistema può essere ospitato presso i server Aziendali (macchina fisica o virtuale) o può essere utilizzato come Saas (software as a service) presso il nostro datacenter ed acceduto dai dispositivi di firma tramite connessione sicura TLS (over internet o VPN). In aggiunta alle componenti hardware e software il sistema ha la necessità, per ogni installazione, di un servizio di gestione delle chiavi crittografiche da parte di un pubblico ufficiale.

Software

Il sistema è composta da 2 macrocomponenti specializzate: la prima nella gestione dei servizi d'integrazione e costruzione dei docuemnti e la seconda nella gestione delle operazioni di firma e gestione dell'algoritmo crittografico. La prima componete è preposta alla raccolta delle informazioni dagli applicativi attraverso l'esposizione di 2 WebServices asincroni <SetDocumentToSign> e <GetSignedDocument>, mentre la seconda ha la funzione di processare il file pdf ed espone verso i tablet il pannello di firma. Questo è il modulo preposto alla gestione dell'impronta autografa e alla criptazione attraverso la chiave pubblica. Il sistema ha una compente frontend accessibile via web per l'esposizione dell'interfaccia di firma e per permettere all'operatore di visualizzare i documenti da firmare qualora il processo di firma sul tablet di default fallisca o non sia identificato un tablet di default durante l'avvio del processo di firma (vedi schema d'integrazione).

Hardware

Il sistema è stato progettato con architettura completamente web ed è quindi possibile utilizzare praticamente tutti i dispositivi in commercio che rispettino le caratteristiche minime di sicurezza suggerita dalla normativa e dalle regole tecniche in vigore. Tutti i dispositivi Wacom, i tablet Surface ed anche iPad (dalla 3° generazione) possono essere utilizzati dal sistema. Attualmente sono stati testati specificatamente:

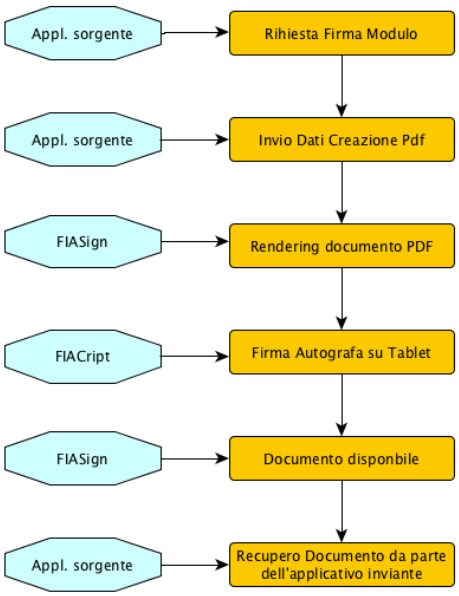
- Musa
- Wacom Adonis
- Apple iPad (S.O. IoS)
- Surface Pro

Sono comunque utilizzabili anche altri tablet/pad previa verifica.

Servizi

Per ogni Azienda che decida di dotarsi del sistema è necessario che venga richiesta una chiave crittografica "tecnica" per la chiusura delle impronte grafometriche delle firme. Questo processo permette, nel rispetto della normativa e delle regole tecniche (DPCM 22 febbraio 2013) di operare senza la necessità di acquisire preventivamente la firma del cittadino, in assoluta sicurezza e senza l'incombenza ed il rischio di furto di dati biometrici. Da un punto di vista operativo la Certification Authority genera una chiave crittografica pubblica mantenendo sotto la sua responsabilità la chiave privata. La chiave pubblica, immessa nel sistema FIA, permette di criptare in origine l'impronta grafometrica (la firma autografa su tablet) in modo "irreversibile".
In caso di contestazione della firma potranno essere eseguite le perizie previste per legge (con strumenti che permettono un'accuratezza di oltre il 500% rispetto alle attuali perizie calligrafiche "analogiche") direttamente dalla CA scelta (nel nostro caso ArubaPEC) che possiede la chiave privata di decriptazione dell'algoritmo con la garanzia di riservatezza. Sarà comunque possibile, nel caso in cui l'Azienda garantisca per la corretta conservazione e tenuta della chiave privata, predisporre un autocertificazione del sistema.

Flusso Operativo



Il flusso operativo del sistema FIA è estremamente lineare ed è completamente indipendente dall'applicativo integrato. Unavolta che si necessita la compilazione di un modulo da far firmare ad un utente basterà richiamare il Servizio di richiesta firma e passare al sistema FIA il nome del modulo con tutti i campi con cui deve essere compilato oltre naturalmente ad un identificativo univoco che permetta, una volta firmato, di essere recuperato. Le operazioni, completamente asincrone, permettono di non aver un vincolo sui flussi da parte dell'applicativo sorgente che sarà svincolato dai tempi della firma autografa. L'applicativo sorgente in questo modo non dovrà esporre WebServices e manterrà il controllo del documento potendo in qualsiasi momento richiederlo, controllarne lo stato e, nel caso di firma eseguita, recuperalo direttamente. Potranno altresì essere definite regole di cancellazione della coda dei documenti su base di eventi trigger o temporali

Schema d'integrazione

L'integrazione avviene attraverso un WebService Asincrono per l'invio che contiene l'indicazione del modulo da sottoscrivere [IdModule], i campi relativi all'id del documento [IdDocument] necessario per il recupero del documento firmato, il nome del tablet su cui è predisposta di default la firma [IdTablet], il tipo di richiesta [ActionRequest] e 50 campi contenti i dati per utili per la compilazione del documento [field1….50].
Un altro WebService permette invece di controllare lo stato di firma del documento e di recuperare il documento firmato se disponibile richiamandolo attraverso l'IdDocument.

Esempio di richiesta di firma:

```
<SetDocument>
        <Parameters>
                <IdModule>
                RIS_Privacy_001
                </IdModule>
                <IdDocument>
                ACC_NUM_123
                </IdDocument>
                <IdTablet>
                T_WAC_local
                </IdTablet>
                <ActionRequest>
                Sign_Doc
                </ActionRequest>
        </Parameters>
        <Fields>
                <Field001>
                ROSSI
                </Field001>
                <Field002>
                MARIO
                </Field002>
                <Field003>
                RX MANO DESTRA
                RX MANO SINISTRA
```

```
                </Field003>
                <Field004>
                01-07-2013
                </Field004>
                <Field005>
                AMBULATORIALE
                </Field005>
                <Field...>
                </Field...>
        </Fields>
</SetDocument>
```

Esempio di richiesta di cancellazione documento:

```
<SetDocument>
        <Parameters>
                <IdModule>
                RIS_Privacy_001
                </IdModule>
                <IdDocument>
                ACC_NUM_123
                </IdDocument>
                <IdTablet>
                T_WAC_local
                </IdTablet>
                <ActionRequest>
                Delete_doc
                </ActionRequest>
        </Parameters>
        <Fields>
                <Field...>
                </Field...>
        </Fields>
</SetDocument>
```

Esempio Modulo con highlight campi

Sotto un esempio di modulo compilato con evidenziate in rosso i campi personalizzati ed in verde il campo di firma

AZIENDA USL7

Dipartimento dei Servizi: DIRETTORE DOTT. ALDO TADDEI

OSPEDALE ALTA VALDELSA - SERVIZIO DI RADIOLOGIA

Direttore U.O. Dr. Aldo Taddei

Modulo Consenso Privacy

Unita' Operativa: **Ospedale Campostaggia**

Nome	M[redacted]A	ID Paziente	- 86279) - Nato/a il:	14-05-1952
Indirizzo	VIA BOLOGNA,7 INT.44			
Cod. Fisc.	MROSVN52E54G752C			

Data Prenotazione	
Provenienza	ESTERNI SENESE
Studi da eseguire	**RX MANO DX** **RX MANO SX** **RX POLSO DX** **RX POLSO SX** **RX PIEDE DX** **RX PIEDE SX**

Il sottoscritto: [redacted]

DICHIARA:

Livello	Consenso
Il trattamento dei miei dati di salute ai fini dell'erogazione della prestazione	**Acconsento**
A rendere disponibile l'esame e il referto ai medici di questa Azienda che si occuperanno anche in futuro della mia salute	**Acconsento**
A rendere disponibile l'esame e il referto ai medici delle altre Aziende sanitarie dell'Area Vasta Sud-Est che si occupano e che si occuperanno anche in futuro della mia salute	**NON Acconsento**