Piattaforma λService

Introduzione

λService è la Piattaforma GT50 che permette di fornire servizi dedicati a firmare/sigillare file PDF (formato PAdES) comprensivi di un codice QRCode -che in questo contesto è identificato come **λSeal**- inserito nell'area grafica della firma PAdES.

L'obiettivo e' quello di garantire la verifica dell'Autenticita', Integrità e se del caso il Non Ripudio di uno di questi documenti, anche dalla sua copia cartacea.

Il sistema inoltre abilita -a richiesta- la notarizzazione su **blockchain**; attualmente l'implementazione in esercizio utilizza esclusivamente **FACTOM**, ma verra' successivamente ampliata l'integrazione ad altre blockchain come Quadrans ed Algorand.

La piattaforma è totalmente compliant al GDPR: non ha infatti nessuna informazione relativa ai file su cui opera; ad eccezione della data dell'evento e di indici anonimi relativi ai dati codificati, ogni dato generato da una transazione viene cancellato volontariamente da ogni componente hw e sw, non appena il suo utilizzo è terminato.

I soli file memorizzati per un periodo temporale indefinito (durata della licenza d'uso) sono codificati con algoritmo di cifratura forte [AES256]; le chiavi di codifica non sono conservate dalla Piattaforma λService.

In Fig A una immagine che riepiloga l'architettura cloud e i vari sistemi "client" che possono interfacciarsi con essa.

I vari elementi operativi, gli appliance e le VM sono basati su sistemi Red Hat o Debian.

Quando sono forniti in modalità locale ed integrati nella rete di un Cliente, gli appliance sono delle **Black Box**: il Cliente ha una interfaccia di amministrazione web based, dalla quale è possibile operare in modo completo sul sistema, dalla configurazione di rete alle regole di routing, dalla definizione dei firmatari, alle Applicazioni che possono interfacciarsi con gli Appliance stessi.

Per ragioni di sicurezza nelle operazioni di firma e per le policy e procedure operative implementate, il Cliente non ha necessità né diritto di accedere sui sistemi forniti a livello di sistema operativo.

La documentazione disponibile è presente a questa URL:

https://services.gt50.org/documentation/

§

I componenti

FrontEnd λService

La Piattaforma **λService (**di seguito **λService)** comprende un sistema centrale di governo delle licenze e del flusso dei dati trattati, definito **FrontEnd λService** che vive nel Cloud GT50, a sua volta interno ad un Service Provider qualificato -per i servizi cloud- con sede in Europa.

Al FrontEnd λService fanno riferimento tutti i sistemi **λPeS** dei vari clienti che hanno scelto l'opzione on-premise, il sistema_**λPeS** presente nel cloud GT50, i vari **λSign** di chi opera direttamente da desktop e l'Applicazione iOS&Android **Universal QReader**.

Una volta che è stato attivato un nuovo Cliente nel FrontEnd λService, gli è stato anche associato il sistema di storage dei documenti codificati (definito genericamente **λStore**:) di default ed incluso nella licenza, λService fornisce lo spazio di storage su un sistema S3 del Service Provider.

Il FrontEnd λService comprende una User Interface web based che permette ai Clienti (owner dei documenti) una minima personalizzazione del proprio profilo ed un accesso alla lista dei documenti che sono stati gestiti tramite λService.

Dei file gestiti, le uniche informazioni disponibili sono:

il nome del file, l'orario dell'operazione, i valori dei digest del file originale e di quello firmato, l'eventuale notarizzazione in blockchain.

Il Cliente ha la possibilità di sospendere, revocare o cancellare il file codificato dallo λStore dove si trova e di associare a questa operazione una nota informativa per l'utente che sta tentando di recuperare il file.

L'interfaccia permette -per ogni elemento registrato- di accedere alle informazioni memorizzate nella blockchain di riferimento, se l'opzione e' attiva per il Cliente in questione.

È presente una interfaccia di amministrazione e gestione delle licenze d'uso e dello spazio di storage, gestita esclusivamente da GT50.

Sono inoltre presenti due interfacce applicative di input e due di output:

a. la prima interfaccia in input accetta da sistemi λPeS o λSign (vedi oltre) dati codificati -tipicamente file PAdES, ma anche immagini, registrazioni video o altro- ed una serie di metadati a questi connessi;

b. la seconda interfaccia in input accetta una richiesta -tipicamente proveniente da Universal QReader (vedi oltre) - per recuperare un file codificato dal **λStore** (vedi oltre) in cui è memorizzato

c. la prima interfaccia di output prevede di inviare al sistema di storage scelto e configurato per quel particolare Cliente, il file codificato da memorizzare.

    a. Alla data attuale il sistema scelto deve avere una interfaccia S3

d. la seconda interfaccia (opzionale) permette di inviare una serie di metadati alla blockchain scelta e configurata per quel particolare Cliente

    a. Alla data attuale la blockchain disponibile è FACTOM

Tutte le informazioni pertinenti la corretta gestione dei Clienti, delle licenze d'uso, dello storage disponibile e dell'operatività sono inserite in un DBMS; attualmente questo DBMS è interno al FrontEnd λService.

Naturalmente l'accesso alle funzioni del FrontEnd λService da parte dei vari "client" è soggetto al controllo di credenziali e token temporali associati ad una licenza Cliente.

§

Appliance λPeS

Questo elemento si concretizza in un Appliance inserito nella rete informativa del Cliente e gestito da quest'ultimo tramite una figura di Amministratore, ovvero nella macchina -con le stesse funzioni- presente nel cloud GT50 per i Clienti che non vogliono gestire apparati fisici, gestito direttamente da GT50 in modalità multi-tenant.

In ambedue i casi il comportamento è equivalente; le sue funzioni sono:

i) ricevere i file PDF su cui operare, da una o piu' applicazioni (tramite connessione in mutua autenticazione forte basata su certificati X.509)

ii) richiedere la creazione di una firma o di un sigillo per i file ricevuti (al momento la richiesta è inviata ai sistemi gateway di un Service Provider Qualificato [eIDAS])

iii) generare il λSeal (elemento grafico comprensivo del QRCode e della chiave di codifica)

iv) preparare il file PAdES finale, comprensivo del λSeal

v) restituire il file PAdES all'applicazione chiamante

vi) creare una copia codificata (AES256 con la chiave pre-calcolata al punto iii) del file PAdES

vii) inviare la copia codificata, insieme ad una serie di metadati al FrontEnd λServer

Il sistema permette all'Amministratore dell'Appliance λPeS di configurare la modalità di utilizzo del sistema stesso:

- viene identificata -tramite certificato di autenticazione X.509- una o più Applicazione che ha il diritto di richiedere i servizi λPeS
- viene definito uno o più titolari di firma/sigillo:
    - ad ognuno di questi Titolari è possibile associare uno o più certificati di firma/sigillo ad esso intestati o da esso gestiti:
        - per ogni certificato di firma/sigillo è possibile definire uno o più tipi di documenti su cui operare.

Tutti questi elementi permettono di essere compliant alla norma italiana ed europea che garantisce -anche nella firma automatica e nei sigilli- la necessità di completo controllo da parte dei titolari.

Una volta configurati dall'Amministratore, solo i Titolari potranno attivare le operazioni di firma/sigillo definendo -se voluto- il periodo temporale di attività, il numero delle operazioni di firma/sigillo permesso, l'applicazione e la tipologia dei documenti che si accetta di firmare/sigillare.

Il titolare ha sempre la possibilità di disabilitare le operazioni di firma che gli competono.

Ad ogni interfaccia di firma/sigillo definita, è associata una configurazione: una struttura dati dove vengono indicate le regole da seguire per l'esecuzione dell'operazione di firma/sigillo vera e propria. Di massima questa struttura dati contiene:

- URI λStore (o equivalente) con modalità di accesso e parametri d'uso
- Descrizione di eventuali dettagli nella creazione della parte grafica del PAdES
- Posizione della rappresentazione grafica della firma nel PAdES (primo/ultimo foglio + sx/centr/dx. Ovvero foglio aggiunto con specifica del layout da usare)
- Codice licenza d'uso associata
- Descrizione Azienda / Cliente

In generale i Clienti installano un λPeS (Appliance) all'interno dei loro sistemi informativi; il sistema possiede una credenziale di autenticazione (X.509) per essere riconosciuto dal FrontEnd λServer.

Da ottobre 2018, alcuni clienti hanno iniziando a spostare nel cloud questo servizio; quindi i loro applicativi si interfacciano direttamente al sistema λPeS GT50 in cloud ovvero ad un λPeS presente nel cloud dei partner GT50 che forniscono questo servizio ai propri Clienti.

§

Piattaforma λService

λSign

Anche se è solo un software desktop[1] tipicamente utilizzato da un Professionista o da una piccola azienda, effettua sui file PDF le stesse operazioni svolte dall'Appliance λPeS.

Prevede una licenza attiva e la disponibilità delle credenziali per l'accesso al FrontEnd λService. Permette la firma di più file PDF (fino al max di 10 alla volta)

Un file PDF firmato tramite λSign subisce lo stesso trattamento oprato da λPeS e fornisce le stesse caratteristiche, compresa l'applicazione del λSeal.

L'applicazione λSign gestisce sia token di firma fisici: smart card, token USB intelligenti o meno; sia firma remota (attualmente il servizio implementato è quello di Aruba; l'accesso ai servizi di firma remota di altri fornitori verrà implementata da GT50 su richiesta dei Clienti).

Ogni installazione di λSign prevede un file di configurazione, modificabile dall'utente tramite interfaccia guidata. Principalmente sono presenti le scelte relative ai dettagli nella creazione della parte grafica del PAdES.

Nella documentazione disponibile è presente un manuale utente per l'utilizzo di λSign.

§

λStore

È un servizio di storage in cloud con interfaccia S3; con funzioni di:

- accettazione di file PAdES codificati da parte di un λPeS o λSign ed inserimento in DB/FS con associazione ad un IdDoc univoco (hash del file)
- Accettazione di query (IdDoc) dal FrontEnd λService, alla quale viene risposto con l'invio del PAdES codificato associato

Il servizio λStore è compreso nella licenza d'uso λService; se richiesto, è possibile associare ad un profilo Cliente l'utilizzo di un sistema di storage diverso. Attualmente l'unico vincolo è che l'interfaccia di accesso sia aperta su Internet e rispetti lo standard S3 - Simple Storage System v2.4

GT50 è disponibile a valutare lo sviluppo di interfacce diverse da S3.

§

[1] attualmente per ambienti Windows; la versione Mac OSX è in rilascio per luglio 2019

Gateway Blockchain (GWFactom)

È l'elemento che permette di interfacciarsi con l'ambiente Blockchain.

Attualmente GWFactom è un nodo della rete follower di Factom e permette l'inserimento in questa blockchain di pochi dati anonimi relativi ad un documento, operando di fatto una notarizzazione dell'esistenza del file: digest del documento prima e dopo la firma e la data dell'operazione (può differire dalla data certificata dalla blockchain stessa).

Come detto in precedenza, i dati relativi alla notarizzazione posso essere recuperati dall'owner dei documenti, tramite User Interface del FrontEnd λService.

Una guida all'utilizzo dei dati presenti nella blockchain è nella documentazione Lambda Service.

§

Universal QReader

È il sw client di verifica ed uso dei λSeal: Universal QReader per smartphone (Android ed iOS).

L'App interpreta il λSeal, tramite FrontEnd λService accede al corretto λStore (GT50 o del Cliente), verifica la firma (eventualmente presente in) λSeal, decodifica il file binario tramite la chiave presente in λSeal, rendendo nuovamente disponibile il file PAdES per l'utente finale con la possibilità di condividerlo tramite le interfacce standard dell'O.S. presente nello smartphone.

§

λSeal

È un QRCode che contiene una struttura dati formale, pubblicata da GT50.

Per i limiti dello spazio disponibile da un QRCode, la struttura è semplificata e gestisce i dati tramite un formato CSV (dati separati da ";" in alcuni contesti applicativi vengono interpretati dopo aver popolato un .xml di riferimento.

- [opzione: preambolo nella forma standard]
- AppCode= varie; 306= λSeal;

- [opzione: SHA256 di un file ***Lambda_Pres[x.y].zip*** contenente .xml di interpretazione dati, certificato NON qualificato GT50 x verifica firms λSeal]
- [opzione
  - URL di riferimento accesso ai file .cpdf
  - Eventuali strutture/metodi di accesso: richiesta UserID+Passwd o altro

  [se non presente, si interpreta come λStore GT50:

  https://services.gt50.org/Lambda/SLS_RepSearch=]
- Codice univoco documento. **IdDoc**
- Chiave decodifica simmetrica **KeyDoc**
- Nome Azienda/Professionista (da configurazione λPeS/Sign)
- Nome file
- [opzione: Breve descrizione]
- Data creazione
- [opzione: Firma sw RSA di GT50 dei dati contenuti in λSeal [come in DSS -> Q-Check]]

Nella documentazione disponibile è presente il documento:

Descrizione contenuto Lambda Seal - 306 (SLSSqCode0306.pdf)

§

Appendice

Nota1: il formato di rappresentazione dei dati binari (hash, crypto key ...) quando devono essere rappresentabili come caratteri stampati è Base64

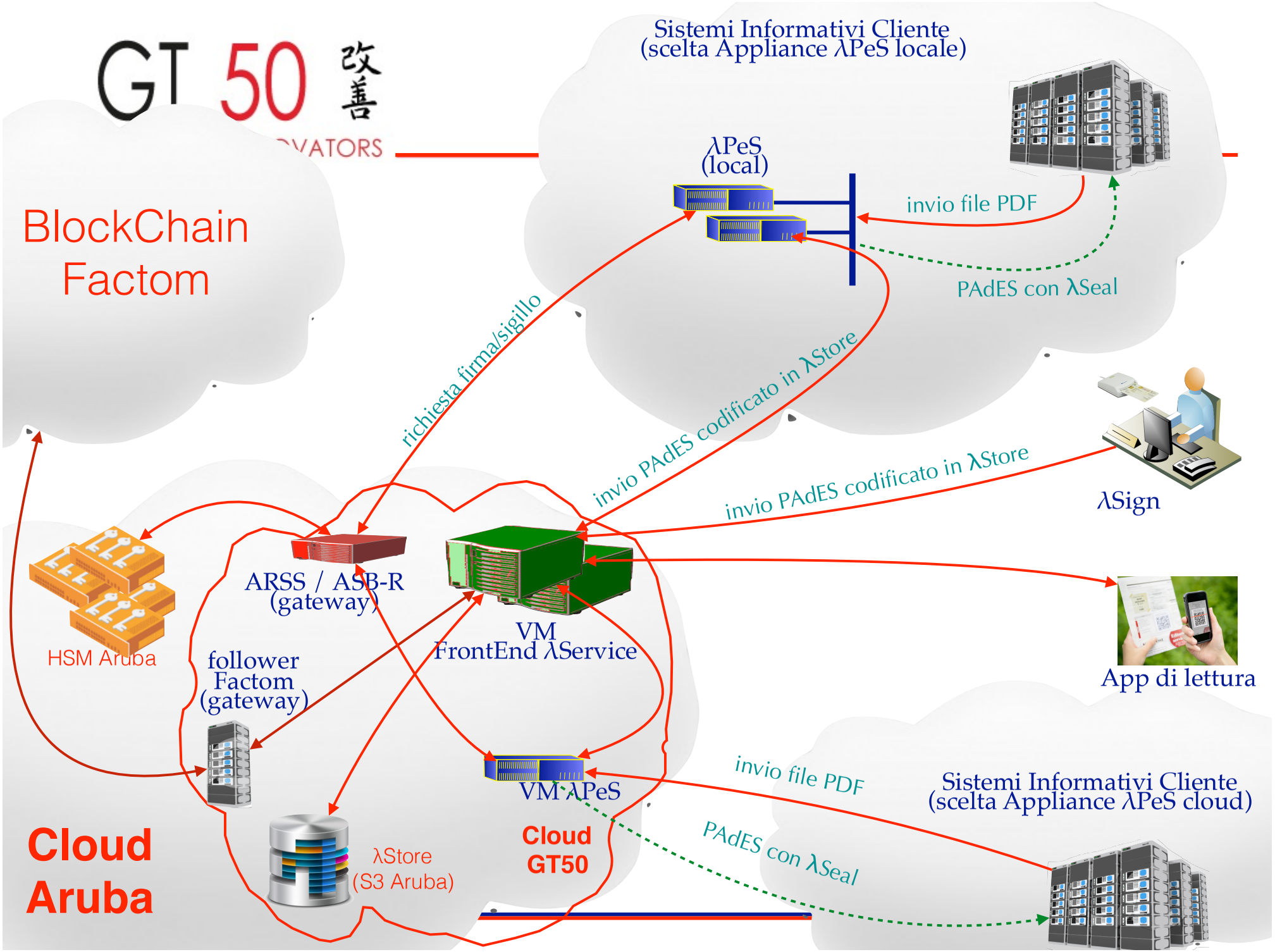
Nota2: i codici ID e short sono in base 62 (maius+minus+decDigit); la loro lunghezza è libera per i Clienti; λPeS e λSign usano 5char per IdDoc e 3char per ShortURL

Nota3: le chiavi di cifratura sono da 256bit algoritmo AES

le chiavi RSA per la firma sw GT50 sono da 1024/2048 bit

gli hash sono da 256bit algoritmo SHA256

Le chiavi di cifratura sono generate randomicamente, quindi utilizzate una volta e poi eliminate


GT 50 改善
VATORS
Sistemi Informativi Cliente
(scelta Appliance λPeS locale)
λPeS
(local)
invio file PDF
PAdES con λSeal
BlockChain
Factom
richiesta firma/sigillo
invio PAdES codificato in λStore
invio PAdES codificato in λStore
λSign
HSM Aruba
ARSS / ASB-R
(gateway)
VM
FrontEnd λService
App di lettura
follower
Factom
(gateway)
VM λPeS
invio file PDF
Sistemi Informativi Cliente
(scelta Appliance λPeS cloud)
Cloud
Aruba
λStore
(S3 Aruba)
Cloud
GT50
PAdES con λSeal