GT 50 改善
VISIONARY INNOVATORS

NOTARIZZAZIONE SCALABILE ED AUTENTICATA DI DATI IOT

Report 1:

Specifiche tecniche sul funzionamento di sistemi attualmente esistenti e production-ready per la notarizzazione su piattaforme distribuite basate su tecnologia blockchain che integrino l'autenticazione tramite firma digitale.

Fornitore:
GT50 Srl

Attività svolta nell'ambito dell'Avviso promosso dal Ministero dell'Università e della Ricerca per la presentazione di Idee progettuali per Smart Cities and Communities and Social Innovation di cui al D.D. n. 391/Ric. del 5 luglio 2012 e ss.mm.ii. - SIN_00968 THE LEARNING METERS NETWORK: workpackage formativo del SCN_00398 - CUP J49G14000140008.

GT 50 改善
VISIONARY INNOVATORS

Prj Università di Perugia
Dipartimento Ingegneria

Ordine 5927252 - CIG ZE32F314CA

La tecnologia blockchain per la notarizzazione di documenti firmati elettronicamente Specifiche tecniche

Abstract

Nel presente documento presentiamo una piattaforma in cloud (Lambda Service), che implementa sistemi di firma elettronica qualificata e memorizzazione su blockchain della transazione di firma e dei metadati del documento firmato.

L'uso della blockchain permette di definire con certezza l'esistenza di un documento a partire da una particolare istante temporale; l'uso della firma qualificata a norma eIDAS, fornisce gli attributi di autenticità, integrità e non ripudio al documento elettronico.

Viene analizzato l'utilizzo della firma qualificata, in ambienti dove la documentazione stampata rimane una prassi comune e vengono introdotti dei meccanismi e delle modalità operative per le firme PAdES che permettono il mantenimento del valore legale del documento firmato anche se stampato.

Viene inoltre introdotta una modalità operativa, che permette il recupero on-line dei documenti firmati, in modo trasparente per l'owner dei documenti stessi, con una forte garanzia rispetto al tema del trattamento dei dati personali (GDPR)

Indice:

Introduzione

GT50 Srl è azienda leader di mercato dei sistemi di Firma Elettronica Qualificata conformi alla norma Italiana ed al Regolamento **eIDAS**[1](EU) ed è una Registration Authority Aruba.

La tecnologia che viene descritta di seguito -Timbro Digitale Lambda- è all'avanguardia nelle scelte tecnologiche adottate e permette la produzione e distribuzione di documentazione elettronica o stampata, con garanzie di Integrità ed Autenticità e Non Ripudio proprie della Firma Elettronica Qualificata (già Firma Digitale[2]) e del Sigillo Digitale Qualificato a norma eIDAS[3].

La tecnologia GT50 viene utilizzata in Italia, da più di 150 Enti di Pubblica Amministrazione Centrale e Locale e da organizzazioni private che in questo modo, possono attivare completi processi di dematerializzazione, continuando a distribuire tramite i loro portali WEB vari tipi di documenti, con la certezza che anche dopo essere stati stampati, questi documenti manterranno le caratteristiche di Integrità, Autenticità e Non Ripudio proprie della Firma Elettronica Qualificata e quindi il loro valore legale.

La piattaforma Timbro Digitale Lambda è stata validata ed inserita nel "Cloud MarketPlace" di AgID: https://cloud.italia.it/marketplace/service/760 ed è compliance a GDPR.

Ci occupiamo di sicurezza dati da più di venti anni ed integriamo nelle nostre architetture o nelle strutture dati che definiamo solo algoritmi di crittografia standard e protocolli di trattamento dati standard; nel 2001 abbiamo inventato il concetto di Timbro Digitale e contrassegno elettronico, divenendo leader del mercato nazionale.

http://www.timbrodigitale.com/referenze.php.

§

[1] eIDAS Regolamento(UE) N. 910/2014 del Parlamento Europeo e del Consiglio 23/07/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

[2] in questo documento Firma Digitale e Firma Elettronica Qualificata si intendono sinonimi

[3] a meno che non sia indicato altrimenti, in questo documento verrà utilizzato il termine firme elettronica qualificata anche per indicare il sigillo elettronico qualificato

Utilizzo della firma qualificata

I governi e le aziende fanno sempre più spesso uso di portali per gestire documenti e form per via elettronica.

Questo si traduce in un servizio migliore e più veloce, più efficiente e anche più economico sia per l'Azienda che lo produce che per i destinatari, che sempre di più possono fruire del download in tempo reale o anche di un semplice invio del documento sulla propria casella di posta elettronica.

Spesso i documenti contengono informazioni che devono essere difese da possibili contraffazioni: in questo caso è buona norma applicare al documento la firma elettronica qualificata (da qui in avanti QES ovvero QESeal nel caso di sigillo qualificato), in quanto questo garantisce l'autenticità e l'integrità dei documenti elettronici

Ci sono però due aspetti importanti da prendere in considerazione, quando si decide di introdurre un processo di QES all'interno di una Organizzazione:

i) Impiegare una QES attraverso applicazioni documentali, può risultare problematico quando le operazioni di firma avvengano utilizzando direttamente apparati locali: lettori e smart card ovvero token di firma. L'uso di queste device comporta costi ricorrenti per le attività relative alla gestione, distribuzione e controllo di questi token e del lettore dedicato, oltre a problemi di installazione e manutenzione nel software locale e nei driver che gestiscono carta e lettore e nel software centrale che lo interfaccia.

   Questa ed altre motivazioni hanno portato l'Europa e l'Italia a normare l'utilizzo di QES in modalità remota: le chiavi per operare una QES in questo caso sono conservate in cloud in ambienti certificati e validati dei Qualified Trust Service Provider (QTSP), all'interno di opportuni apparati a loro volta certificati per questo scopo: Qualified Electronic Signature Creation Device (QSCD), generalmente definiti HSM (Hardware Security Module).

ii) Quando un documento firmato viene stampato, le caratteristiche di sicurezza della QES sono perse e il documento non ha più valore legale, dato che software di grafica e stampanti sofisticate permettono di contraffare o riprodurre con facilità qualsiasi documento stampato.

Esistono varie soluzioni per poter dare accesso agli utenti ai documenti firmati, partendo dalla stampa di questi. Le soluzioni più semplici forniscono solo un link ad un sito da cui scaricare il file, ma questo comporta per chi ha emesso il documento originale l'attivazione di servizi on line, che potrebbero essere violati, lasciando quindi una illecita disponibilità di molti file e di informazioni private o sensibili.

§

La piattaforma Lambda Service

Per ovviare a queste tematiche, GT50 mette a disposizione la sua Piattaforma Timbro Digitale Lambda (λService) che opera sia come servizio cloud, sia on-premises come appliance fisica (λPeS) da installare nella rete del Cliente.

La piattaforma Timbro Digitale Lambda, permette di creare documenti PDF firmati digitalmente (formato PAdES), i quali mantengono la loro validità legale anche in formato cartaceo.

La Piattaforma λService può gestire anche richieste più complesse, che riguardano più file e di tipologia diversa. Questo documento si concentra nel caso d'uso più semplice: quello della creazione di file PAdES comprensivo del Timbro Digitale Lambda..

La piattaforma fornisce un servizio (SaaS) che nasce per essere facilmente integrato in un ambiente documentale già esistente

La validità legale del documento cartaceo, deriva dalla presenza del contrassegno elettronico[4] λ Seal, uno speciale QRCode sicuro inserito nella rappresentazione grafica dell'oggetto firma del PAdES: il documento originale quindi non viene alterato da questo procedimento.

Il contenuto di λSeal garantisce il collegamento inviolabile e certo, tra il documento digitale firmato e la copia cartacea di questo. I documenti firmati, oltre che restituiti inizialmente alle Applicazioni del Cliente, vengono mantenuti on-line in modalità cifrata in un particolare storage in cloud: λStore.

Il server λStore non possiede le chiavi di cifratura di questi file, ne conosce il loro contenuto o la loro provenienza: anche in caso di violazione non può rivelare nulla.

L'utilizzo della tecnologia blockchain permissionless, non mette a rischio alcun dato in quanto verranno gestiti in modo aperto solo i metadati della transazione Lambda.

Come gli altri prodotti di sicurezza da noi disegnati, la piattaforma λService segue gli standard di sicurezza ed implementa solo algoritmi standard di crittografia.

Con la sicurezza dati come primo obiettivo, la piattaforma è stata disegnata in modo semplice, così come è semplice la sua implementazione e -grazie agli algoritmi standard di crittografia e firma digitale utilizzati- permette la creazione di documenti inviolabili ma facilmente fruibili da chi è autorizzato.

§

[4] il contrassegno elettronico è definito in Codice Amministrazione Digitale - Dlgs 7 marzo 2005 n.82 Art.23 c.2-bis

Integrazione

L'integrazione con il Sistema Informativo del Cliente avviene con un impatto minimo: l'interfaccia verso la Piattaforma λService è implementata da web service REST e POST su canali https, tramite cui le Applicazioni del Cliente inviano file PDF da firmare e ricevono di ritorno file PDF firmati (formato PAdES).

Questo comporta che le due modalità -in cloud ovvero on-premises- risultino completamente trasparenti agli applicativi del Cliente; inoltre dato il grande utilizzo e conoscenza delle interfacce web service, in questo modo si può garantire l'interoperabilità anche con future applicazioni.

L'utilizzo della Piattaforma Timbro Digitale Lambda rende trasparente per le Applicazioni del Cliente, le interfacce da utilizzare per operare sulle piattaforme dei fornitori di certificati di firma (Prestatori di servizi fiduciari qualificati o QTSP).

Attualmente la firma in cloud che è integrata nella Piattaforma Appliance λPeS, è quella di Aruba; GT50 è disponibile a valutare -su richiesta formale da parte del Cliente- l'integrazione della Piattaforma Appliance λ PeS, anche con altri QTSP autorizzati da AgID.

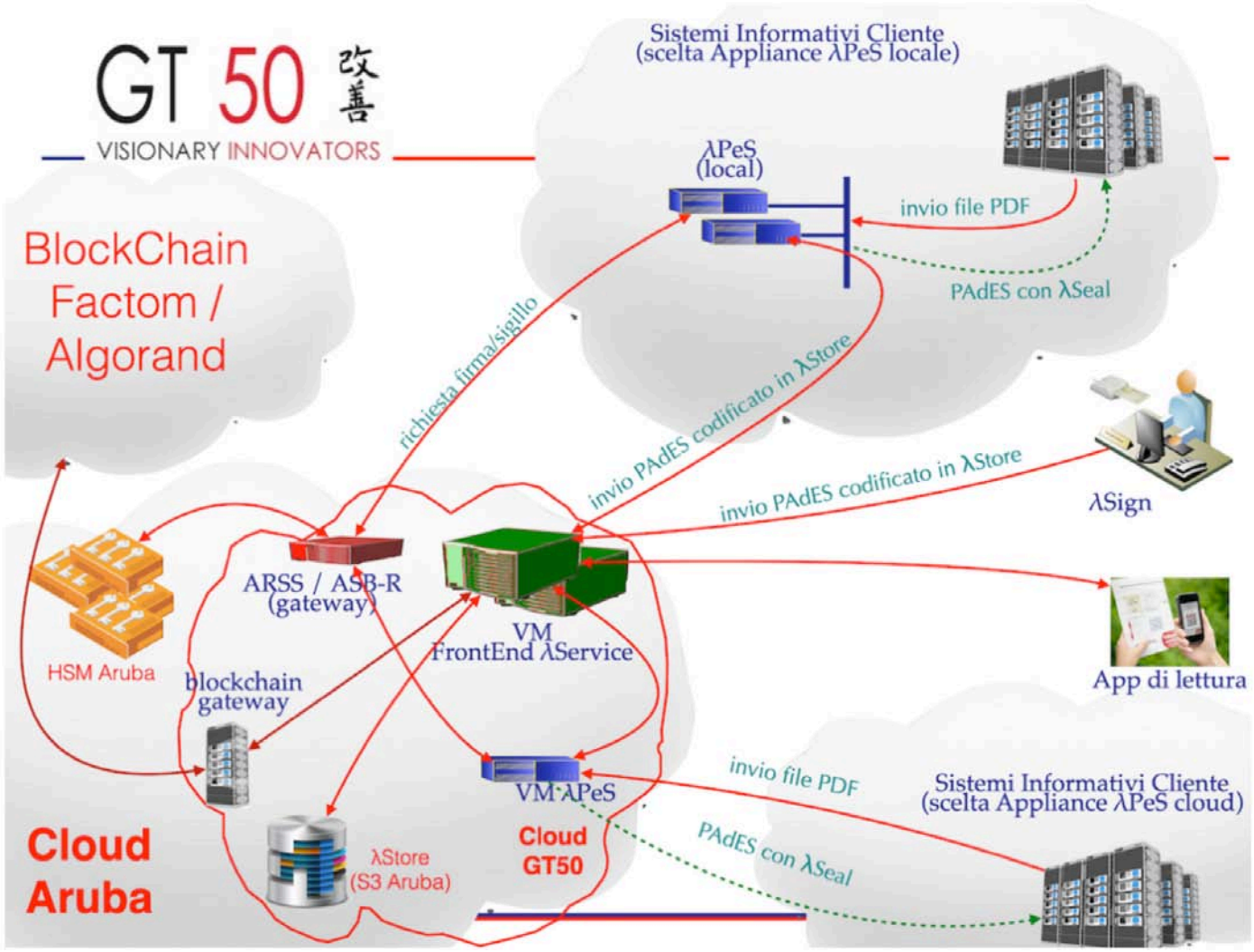
§

Sicurezza e compliance GDPR

La Piattaforma Timbro Digitale Lambda è stata qualificata da AgID per essere inclusa nel Cloud Marketplace della PA: https://cloud.italia.it/marketplace/service/760

È quindi compliance al regolamento generale sulla protezione dei dati (GDPR).

L'architettura di seguito rappresentata, garantisce che nessun documento verrà portato all'esterno della Piattaforma stessa: il processo di firma operato da swCore all'interno dell'Appliance λ PeS, calcola l'hash di ogni documento ed invia questo elemento -di per se totalmente anonimo- alle apparecchiature del QTSP in cloud che operano il puro valore della firma.



Una volta ricevuto indietro questo valore, swCore completa il processo di firma, confezionando il file finale nel formato PAdES o CAdES a seconda della richiesta dell'Applicazione del Cliente.

La piattaforma è totalmente conforme alla normativa per la protezione dei dati personali (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 cifrati, 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 la durata della licenza d'uso, sono cifrati con algoritmo di cifratura forte [AES256]; le chiavi di cifratura sono generate in modo (pseudo)random una per documento e NON sono conservate dalla Piattaforma λService.

Specifiche tecniche

I vari elementi operativi, le 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 λ Service (di seguito λ Service) comprende un sistema centrale di governo delle licenze e del flusso dei dati trattati, definito FrontEnd λ Service 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 λ PeS presente nel cloud GT50, i vari λ Sign di chi opera direttamente da desktop e l'Applicazione iOS&Android Universal QReader.

Una volta attivato un nuovo Cliente nel FrontEnd λ Service, a questo viene associato il sistema di storage dei documenti cifrati, definito genericamente λ Store; di default ed incluso nella licenza, λ Service fornisce lo spazio di storage su un sistema S3 del Service Provider, ma è possibile per un Cliente richiedere la memorizzazione dei suoi file su un sistema di storage alternativo.

Il FrontEnd λ Service 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, la notarizzazione in blockchain.

I file cifrati e memorizzati nel λ Store non sono disponibili tramite questa User Interface, in quanto la Piattaforma nella sua interezza non possiede le chiavi di decifratura (vedi oltre).

Il Cliente ha la possibilità di sospendere, revocare o cancellare il file cifrato 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 (λStore), gestita esclusivamente da GT50.

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

- la prima interfaccia in input accetta da sistemi λPeS o λSign (vedi oltre) dati cifrati -tipicamente file PAdES, ma anche immagini, registrazioni video o altro- ed una serie di metadati a questi connessi;
- la seconda interfaccia in input accetta una richiesta -tipicamente proveniente da Universal QReader- per recuperare un file cifrato dal λStore in cui è memorizzato
- la prima interfaccia di output prevede di inviare al sistema λ Store scelto e configurato per quel particolare Cliente, il file cifrato da memorizzare. Attualmente il sistema scelto deve avere una interfaccia S3
- la seconda interfaccia (opzionale) permette di inviare una serie di metadati alla blockchain scelta e configurata per quel particolare Cliente

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: 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 cifratura)
iv) preparare il file PAdES finale, comprensivo del λSeal
v) restituire il file PAdES all'applicazione chiamante
vi) creare una copia cifrata (AES256 con la chiave pre-calcolata al punto iii) del file PAdES
vii) inviare la copia cifrata, insieme ad una serie di metadati al FrontEnd λServer

Il sistema permette all'Amministratore dell'Appliance λ PeS 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/tutti foglio + sx/centr/dx. Ovvero foglio aggiunto con specifica del layout da usare)
- Codice licenza d'uso associata
- Descrizione Azienda / Cliente

È possibile avere una appliance λPeS (Appliance) all'interno del proprio sistema informativo; il sistema possiede una credenziale di autenticazione (X.509) per essere riconosciuto dal FrontEnd λServer.

§

λSign

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

Prevede l'esistenza di una licenza attiva e la disponibilità delle credenziali per l'accesso al FrontEnd λService. Permette la firma di più file PDF.

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

L'applicazione λ Sign 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 λ Sign 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 basato sul protocollo S3; con funzioni di:

- accettazione di file PAdES cifrato 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 cifrato 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.

§

Gateway blockchain (GWAlgorand)

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

Attualmente GWAlgorand è un nodo della rete follower di Algorand e permette l'inserimento in questa blockchain di alcuni meta-dati anonimi relativi ad un documento, operando di fatto una notarizzazione dell'esistenza del file.

Come detto in precedenza, i meta-dati relativi alla notarizzazione posso essere recuperati dall'owner dei documenti, tramite User Interface del FrontEnd λService e naturalmente sono disponibili alla applicazione Universal QReader.

Questo è un esempio reale di quanto memorizzato in blockchain fronte di una transazione di notarizzazione:

{
"Type":"Data",
"HashFile":"009BF60332C4924D2A9C17FB28225F47D801468DF689693AE8F2C37FD44CA76A",
"HashFilePADES":"FE9B802355B77004E32F592012474C0FF691D63264B615B197C5E7C36238C0AB",
"DateTime":"20210422184944"}}

E questo è un link per poter visualizzare il contenuto direttamente dalla MainNet Algorand:

https://goalseeker.purestake.io/algorand/mainnet/transaction/5ACQZLNMT45PVZJNHAWJNF6OBREESM2V6FS7PBOQ5ICVYUQ2GCKA

§

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

Codice univoco documento. IdDoc

- Chiave di cifratura 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)

§

Universal QReader

La verifica dell'integrità e l'utilizzo dei dati contenuti in Lambda Seal, avviene tramite l'uso di Universal QReader™ una App per smartphone/tablet, liberamente scaricabile da PlayStore(Android) ed AppStore(IOS). .

Se letto da diversa applicazione, Lambda Seal può informare l'utente della necessità di utilizzare Universal QReader™, fornendo un link allo store per il download dell'App.

§

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

I dettagli di programmazione, le API disponibili per interfacciare la Piattaforma Timbro Digitale 2D-Plus sono disponibili on-line qui:

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

❖

❖ ❖ ❖