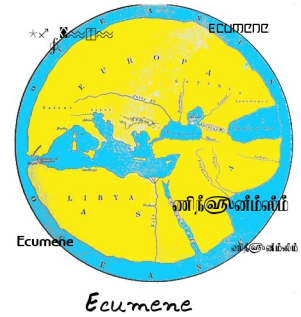


T-Services

Bridge & ttp



Convegno:

Documento elettronico, firma digitale e nuovo processo civile

Intervento:

Aspetti tecnici del documento informatico e della firma elettronica

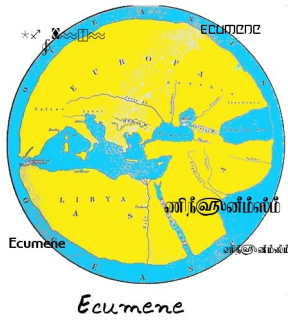
Dott. Remo Tabanelli

(Consigliere ISOC Italia)

remo@t-bizcom.com

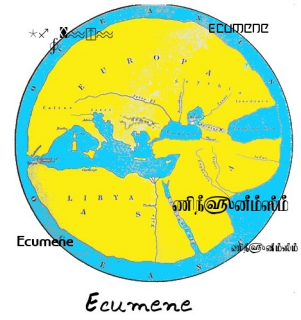
cell. 348 5160400

12 maggio 2006 - Università di Udine, Sala Tomadini



T-Services

Bridge & ttp



White paper sull' archiviazione a lungo termine

Dal Decreto del Presidente della Repubblica 28 dicembre 2000 n. 4451¹

SEZIONE I

DOCUMENTI AMMINISTRATIVI E ATTI PUBBLICI

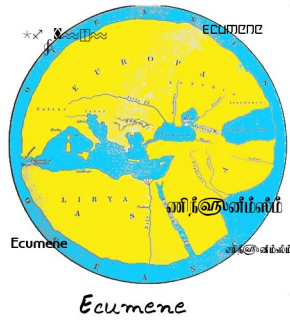
Articolo 6 (L-R) Riproduzione e conservazione di documenti

1. *Le pubbliche amministrazioni ed i privati hanno facoltà di sostituire, a tutti gli effetti, i documenti dei propri archivi, le scritture contabili, la corrispondenza e gli altri atti di cui per legge o regolamento è prescritta la conservazione, con la loro riproduzione su supporto fotografico, su supporto ottico o con altro mezzo idoneo a garantire la conformità dei documenti agli originali.*
2. *Gli obblighi di conservazione ed esibizione dei documenti di cui al comma 1 si intendono soddisfatti, sia ai fini amministrativi che probatori, anche se realizzati su supporto ottico quando le procedure utilizzate sono conformi alle regole tecniche dettate dall' Autorità per l'informatica nella pubblica amministrazione. (L)*
3. *I limiti e le modalità tecniche della riproduzione e dell'autenticazione dei documenti di cui al comma 1 su supporto fotografico o con altro mezzo tecnico idoneo a garantire la conformità agli originali, sono stabiliti con decreto del Presidente del Consiglio dei Ministri.*
4. *Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle amministrazioni pubbliche e sugli archivi privati dichiarati di notevole interesse storico, ai sensi delle disposizioni del Capo II del decreto legislativo 29 ottobre 1999, n. 490.*

Articolo 8 (R) Documento informatico

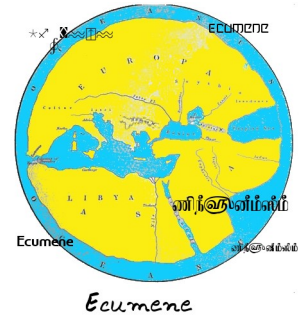
1. *Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente testo unico.*

¹ E successive modifiche apportate con Decreto del Presidente della Repubblica 7 Aprile 2003, n. 137



T-Services

Bridge & ttp



Alcuni indispensabili prerequisites

Abbiamo ritenuto opportuno iniziare la trattazione dell'argomento a partire dal decreto legislativo che ha introdotto in Italia l'uso della archiviazione elettronica tramite la firma digitale dandogli valenza legale e equivalenza alla *forma scritta* tradizionale (plain paper).

Con questa norma, rivoluzionaria per il nostro ordinamento, si introduce la nozione di *originale* per l'archiviazione elettronica, nonché l'equivalenza legale tra documenti firmati digitalmente e documenti firmati in modo tradizionale.

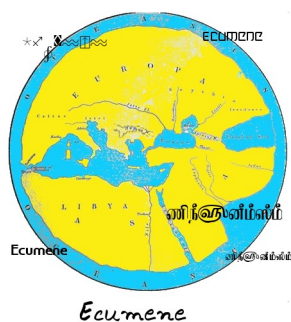
Lo *spirito* e le forme utilizzate nella normativa tendono, in generale, stabiliti i criteri di sicurezza e i loro requisiti tecnici di massima, a conservare tutti gli aspetti di questa equivalenza di principio in modo tale da continuare a ritenere inalterati i principi del codice civile che regolano la materia (preesistenti a tale decreto) in modo da limitare al minimo l'impatto col corpo giuridico e la giurisprudenza preesistenti.

Uno dei fondamentali *criteri guida* presenti nella normativa è costituito dall'idea che gli aspetti *tecnologici* possano o debbano essere *interpretati* in modo tale da seguire questa *filosofia ispiratrice*.

Per questo motivo diventa fondamentale, se si vogliono costruire soluzioni tecniche adeguate, interpretarle in uno spirito che mantenga una contiguità maggiore possibile tra mondo *elettronico* e mondo tradizionale.

La norma sopra presa in considerazione, definisce la possibilità di conservare e archiviare la documentazione elettronica con valore legale a prescindere da quella che sia la sua specifica natura.

Le tecnologie attualmente disponibili di firma digitale rendono certamente possibile la realizzazione di questo obiettivo purché si tengano in considerazione alcune *caratteristiche e requisiti formali* che (a prescindere dalle tecnologie impiegate) tali documenti devono necessariamente *avere e conservare* per tutto il tempo assegnato al loro *ciclo di vita*.



T-Services

Bridge & ttp



Considerazioni sulla *durata* o intervallo temporale di *validità legale* e relativo periodo di *conservazione degli archivi*

Il ciclo di vita che la legge assegna ad alcuni tipi di documenti, a prescindere dalla loro natura elettronica o meno, è in genere, di gran lunga superiore al periodo di validità comunemente assegnato alle chiavi crittografiche e ai certificati che sono usati per produrre le firme digitali o i *sigilli elettronici* in genere, tali *sigilli* sono anche successivamente utilizzati nelle operazioni di *verifica di integrità* o *verifica di autenticità conformità* dei documenti stessi.

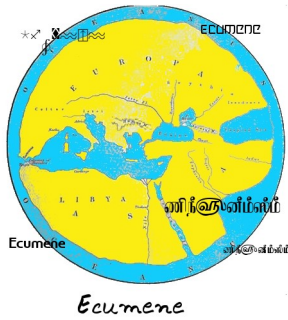
Inoltre l'insieme dei dati necessari a compiere tali operazioni di *verifica* possono, per diversi e legittimi motivi, non essere più disponibili o non essere disponibili nella stessa forma, per tutto il periodo per cui il *documento/i* ha necessità di essere conservato.

A titolo esemplificativo di come tale situazione possa verificarsi basta pensare alla eventualità di cessazione di attività di una Certification Authority che abbia emesso uno (o più) certificati di firma utilizzato in un documento o insieme di documenti.

Oppure, banalmente, alla scadenza o revoca di uno dei certificati nel corso del periodo di *conservazione*.

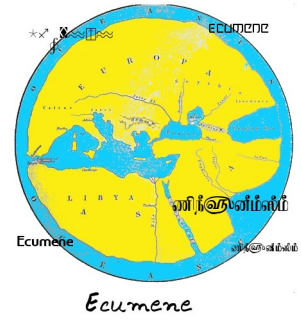
Ambedue queste eventualità renderebbero impossibili le operazioni di *verifica* che dovessero essere effettuate in periodi successivi al verificarsi degli avvenimenti descritti come esempio.

Una caratteristica importante dei documenti che debbano essere conservati per lunghi periodi è (come appare chiaro dagli esempi) la *auto consistenza*, intesa come indipendenza da dati esterni, e la *invarianza*, intesa come il permanere degli attributi peculiari del documento per tutto il periodo di conservazione e a prescindere dallo specifico *contesto* operativo o dai dati disponibili (presso fonti esterne) al momento in cui si effettuano le operazioni di *verifica*.



T-Services

Bridge & ttp



Dati di contesto *comuni o indispensabili* alle operazioni di verifica

Le operazioni comunemente dette di verifica utilizzano tipicamente dati di contesto che sarebbero, da un punto di vista squisitamente teorico, desumibili dalle proprietà del documento/i su cui si intende effettuare l'operazione. Tali dati, sempre da un punto di vista teorico, non sono dati *comunemente* considerati come dati *contenuti* nel documento ma vengono *generalmente* considerati come dati esterni; è nostra intenzione dimostrare come tali dati debbano invece essere considerati **essenziali** nell'affrontare la questione della conservazione a lungo termine con effetti legali.

Cerchiamo di definire ora, concretamente, tali strutture di dati e il loro significato e uso pratico in una operazione di verifica.

1) CRL (Certificate Revocation List) Trattasi di un oggetto firmato emesso da una Certification Authority.

Tale oggetto contiene, almeno, i seguenti elementi: lista dei certificati revocati e per ogni certificato, la data di revoca (riferimento temporale al momento di revoca/sospensione della validità del certificato) e il numero di serie del certificato stesso.

La CRL contiene inoltre il certificato della CA emittente, la CRL stessa e i riferimenti temporali relativi al prossimo aggiornamento.

Lo scopo della CRL durante le operazioni di verifica di un documento consiste nella possibilità di verificare che, al momento in cui si compie tale operazione (verifica) il/i certificato/i sia assente dalla CRL, (quindi valido) al momento della verifica stessa.

Nel caso che invece il documento presenti al suo interno un riferimento temporale (o sia già associato ad un token temporale) la CRL dovrà riferirsi ad un periodo (data di emissione e data di aggiornamento) il cui intervallo comprenda il riferimento temporale del documento stesso.

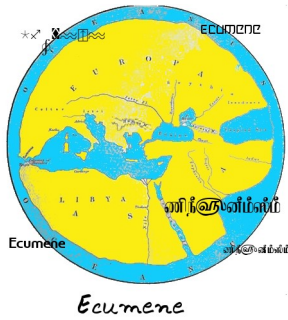
In tal caso avremo anche la possibilità di verificare se il certificato con cui è firmato il documento era non revocato/sospeso alla data corrispondente al riferimento temporale relativo al documento stesso.

Ciò che va in ogni caso sottolineato è che in ambedue i casi (con o senza riferimento temporale sul documento) l'operazione di verifica sulla CRL, diventa un fattore di contesto **STATICO** (riferito o alla data contenuta nel documento o al momento in cui la verifica stessa viene effettuata).

IN NESSUN CASO il cambio (eventuale) di stato del certificato usato per la firma del documento può o deve influenzare le operazioni di verifica successive.

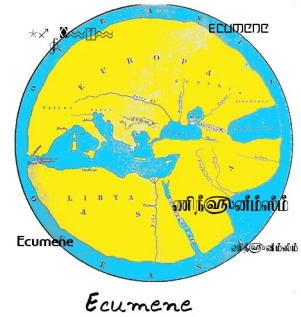
Il dato CRL diventa quindi uno degli elementi di contesto che può (deve) essere *fissato* e associato al documento e non deve essere ulteriormente prelevato *da sorgenti esterne di dati*, pena la variazione di stato da *trusted a untrusted* del documento stesso in funzione delle variazioni di stato (nel corso del tempo) del certificato stesso.

Occorre quindi identificare un metodo che consenta di associare permanentemente tale dato al documento **nel momento in cui se ne effettua l'archiviazione.**



T-Services

Bridge & ttp



2) Riferimento temporale (o token temporale) relativo al momento in cui si effettua la verifica.

Tale riferimento temporale va distinto da altri riferimenti temporali o token già presenti prima della operazione di archiviazione.

Il riferimento temporale in questione ha lo scopo di attestare lo *stato* del documento e della CRL al momento in cui l'archiviazione stessa avviene.

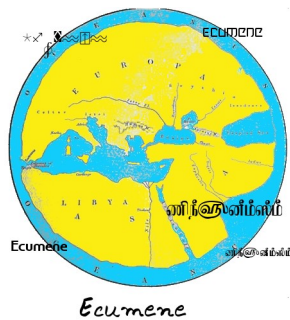
A tale scopo è evidente che il riferimento (token) temporale deve riguardare univocamente e il documento stesso e la/e CRL relative ai certificati che compaiono sul documento stesso (CA compresa).

Tale riferimento temporale (token) sigilla e associa inalterabilmente documento e dati statici di contesto in forma auto consistente (non è necessario ricorrere a fonti esterne di dati per verificare l'integrità del documento stesso).

La funzione di *ARCHIVIAZIONE* o l'operatore/addetto possono a loro volta (per esigenze di workflow o tracciabilità *sigillare e protocollare* con firma digitale l'insieme dei dati statici di contesto (riapplicando in tal caso i passi sopra descritti anche a questo ultimo sigillo).

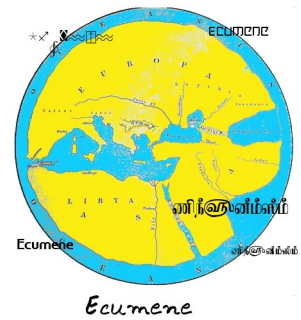
Evidentemente anche il riferimento (token) temporale, essendo per sua natura una forma di *firma digitale* avrà una *scadenza* dei propri dati e del proprio contesto.

Per completare, quindi, la procedura di archiviazione occorrerà aggiungere una operazione (periodica) di rinnovo del sigillo (token) ad ogni scadenza del sigillo stesso.



T-Services

Bridge & ttp



Rappresentazione logica del *documento*

Abbiamo cercato di dare una idea di quelli che sono i requisiti minimi di una forma di rappresentazione logica dei documenti archiviati.

Tali requisiti (pur avendo una loro possibile rappresentazione *concreta* in termini *tecnologici*) non derivano da necessità o considerazioni tecnologiche ma sono semplicemente la *applicazione concreta* di quanto è stabilito, per vie normative e generali, dai principi fissati nei decreti e nelle norme relative alla conservazione/archiviazione di documenti (tradizionali o elettronici) e alla necessità di mantenere il loro stato e contenuto (semantico informativo) inalterato (statico) nell'arco del loro ciclo di vita/conservazione.

La struttura proposta non entra nel merito dei criteri (formati, bitmap, testo, risultato di scansione ottica o altro) di formazione del (dei) documento/i, né delle tecnologie utilizzate nella formazione delle *rappresentazioni elettroniche* dei documenti stessi.

La struttura proposta, inoltre, non entra neppure nel merito della *validità* o *rilevanza legale* dei documenti stessi (tale validità o rilevanza può, eventualmente, essere dedotta solo da una verifica semantica della natura esplicita del documento/i in funzione dei suoi specifici scopi); ad esempio, un contratto dove, una parte, venda gratuitamente le proprie prestazioni lavorative a titolo *gratuito*, ad una altra parte, risulterebbe *non valido* per il suo contenuto (semantica) in violazione alle norme del codice che regolano i rapporti di lavoro, anche qualora le firme e gli attributi e i poteri dei contraenti fossero perfettamente validi e *verificati*.

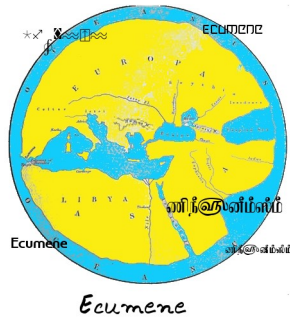
L'idea di *verifica* formale di un documento qui esposta (automatica o manuale che sia) ha valenza di sola *verifica formale e crittografica* sulla integrità e *validità* della rappresentazione fornita, **non del valore semantico o della validità del suo contenuto** e, tanto meno, della sua completezza coerenza e consistenza giuridica.

Tali valutazioni rimangono nei criteri di giudizio (legale o meno a seconda delle circostanze) di chi valuta i documenti stessi.

Lo scopo essenziale che si vuole raggiungere è invece quello di **fornire a chi valuta o deve valutare il contenuto e il merito dei documenti, uno strumento di confidenza o certezza riguardo alla autenticità della rappresentazione fornita.**

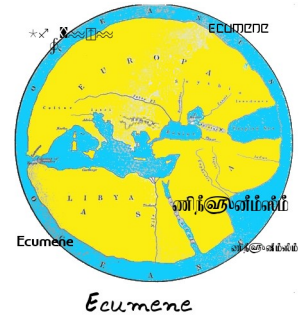
Dato per acquisito ciò che abbiamo esposto in precedenza emerge con chiarezza la natura *read only* delle forme di archivi azione a lungo termine.

Certo, i documenti (meglio sarebbe dire copie dei documenti archiviati) o parte di essi possono



T-Services

Bridge & ttp

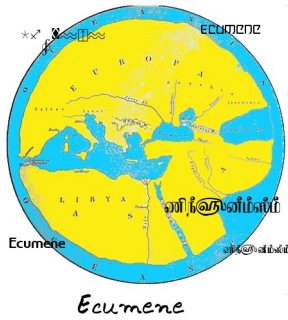


essere estratti letti o anche eventualmente modificati, ma non possono, una volta effettuate tali operazioni *rientrare* nella struttura di archivi azione (che rimane statica e invariata).

Qualora si voglia procedere alla archivi azione di modifiche o interventi su documenti archiviati in precedenza occorrerà procedere ad una nuova archivi azione (mantenendo anche in questo caso la analogia con i documenti *cartacei o tradizionali che dir si voglia*).

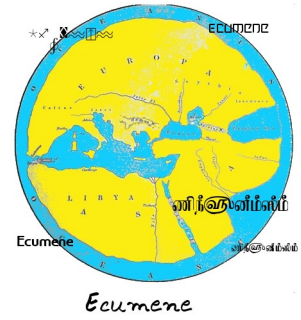
Esiste quindi una separazione logica e procedurale che necessariamente si colloca tra le fasi di processo e procedura (workflow) che si applicano ai documenti durante il ciclo di *lavorazione* e la fase in cui il ciclo di vita dei documenti stessi entra *nell'archivio*.

Certo, possono esistere repository di documenti che svolgono funzioni di memorizzazione o deposito temporaneo nel corso dei processi di workflow, ma la funzione di tali repository rimane di fatto distinta e ben separata, anche da un punto di vista logico, dalla funzione di archivio propriamente intesa.



T-Services

Bridge & ttp



Note di analisi tecnica delle strutture formali per l'archiviazione a lungo termine dei documenti²

Premessa

In queste note tecniche si intende per *documento* la definizione richiamata dal **Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445** e modifiche apportate con **Decreto del Presidente della Repubblica 7 aprile 2003, n. 137**.

Dal punto di vista strettamente informatico un documento è quindi un insieme di dati comunque codificati o originati a prescindere dal contesto applicativo (applicazione o insieme di applicazioni) che li ha generati.

L'unico reale requisito che si può ragionevolmente individuare è che tali dati siano *rappresentabili* (o consentano ad una applicazione, sistema operativo o sottosistema di *rappresentarli*) tramite un **unico insieme** (ad es. file) **univocamente definito**.

La forma tecnica o informatica (file di testo, bitmap, scansione digitale, pdf, XML o altre forme) con cui il *documento*, come definito nel decreto citato, è rappresentato e codificato non ha rilevanza giuridica o amministrativa, quindi è del tutto ininfluenza rispetto alla validità o alla natura del documento stesso.

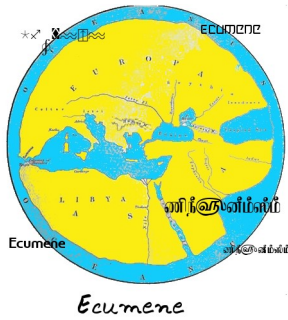
Il concetto di *originale* riferito al documento digitale

Quanto sopra premesso, il decreto introduce in modo sia esplicito sia implicito il concetto di *originale digitale* di un documento, cioè la rappresentazione diretta (non derivata dalla digitalizzazione o *copia digitale* di un documento altrimenti formato) *informatica* dei dati significativi (o *rilevanti*). In altri termini la distinzione tra *copia*, *originale*, e *copia autentica*, si applica solo (eventualmente) a quei *documenti informatici* che siano il risultato di operazioni di copia o digitalizzazione di *documenti tradizionali* e quindi non formati in origine tramite procedure informatiche ma tramite *mezzi tradizionali*.

L'eventuale procedura di autenticazione o certificazione di conformità all'originale si può applicare quindi solo per quei pochi casi (e solo se si ha derivazione da *documenti tradizionalmente formati*) per cui è strettamente richiesto.

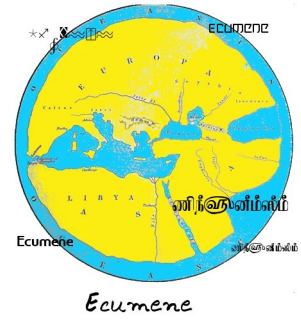
Un documento formato **direttamente** in modo informatico ha in sé il requisito di *originalità*.

² Si veda anche il documento “White paper sull'archiviazione a lungo termine”



T-Services

Bridge & ttp



Attori e partecipanti al processo di archiviazione elettronica

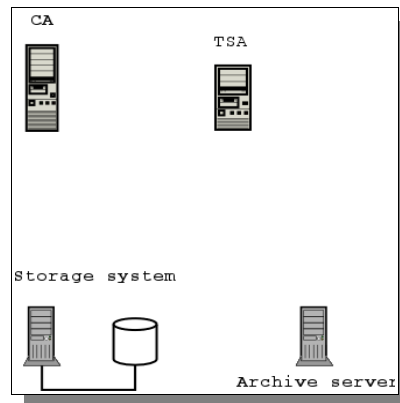


Fig. 1: Servizi e componenti.

C.A.: Certification authority.

Per Certification Authority si intende l'ente o gli enti emittenti i certificati di *sottoscrizione* utilizzati sia nei processi (eventuali) di firma dei documenti da archiviare o relativi ai processi di archiviazione stessa. Per semplicità si è rappresentato un unico ente, tale situazione tuttavia, è una semplificazione utilizzata per semplicità di rappresentazione, nella realtà si avranno, verosimilmente riferimenti a una pluralità di CA.

Storage System:

Per storage system si intende l'insieme dei sistemi e sottosistemi che fungono da *repository* dei documenti durante il loro *normale lifecycle* (o workflow) precedente le fasi di **archiviazione**.

Per storage system si intende, contemporaneamente, l'insieme dei sistemi e sottosistemi che fungono da supporto per la memorizzazione (e information retrieval) dei dati e dei documenti che vengono archiviati tramite la procedurale di archiviazione. Tale funzione di archivio è logicamente separata da quella di *repository* sopra descritta; in questo schema si sono sommate le due funzioni in una unica entità per semplicità di rappresentazione.

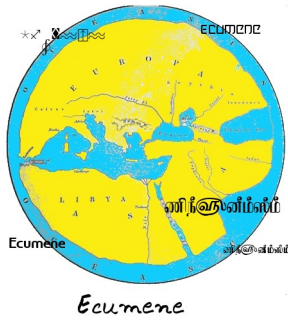
Archive server:

Per archive server si intende il sistema che presiede alla erogazione dei servizi e delle applicazioni che presiedono i processi e i flussi relativi alle operazioni di archiviazione **elettronica a lungo termine**.

T.S.A.: Time Stamping Authority.

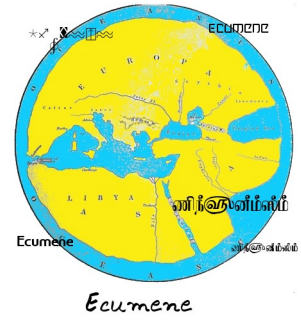
Per Time Stamping Authority si intende un servizio (presumibilmente fornito da una parte terza) preposto al rilascio di *time stamp token* ovvero la associazione tramite firma digitale di una data e ora **certa** al contenuto di un documento informatico.

Stabiliti gli attori coinvolti nella architettura tecnica di una soluzione di archiviazione elettronica a *lungo termine*, possiamo passare a precisare gli aspetti di flusso e procedurali da applicare.



T-Services

Bridge & ttp



Processi e flussi

Acquisizione e analisi dei documenti da archiviare

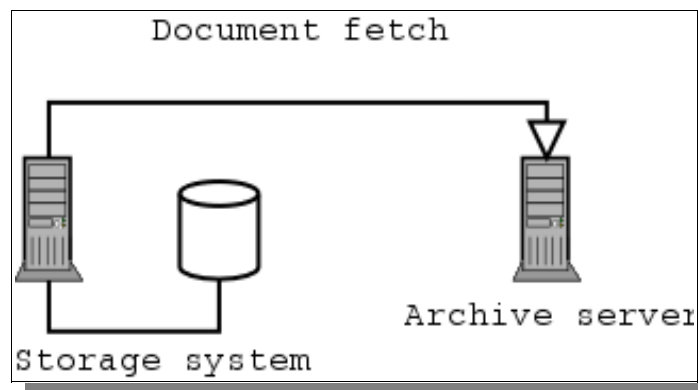


Fig.2:Acquisizione documenti da archiviare.

La prima fase di una procedura di archiviazione consiste nella acquisizione del/dei documento/i su cui si effettuano le operazioni di archiviazione.

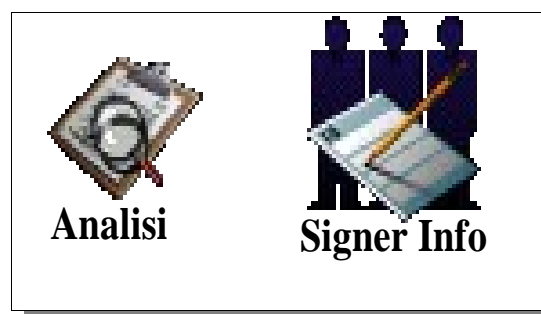
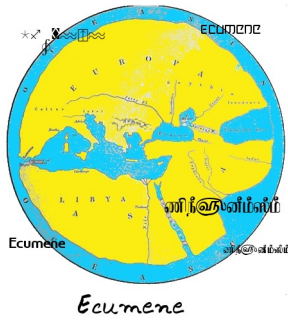


Fig.3:Analisi e estrazione signer info.

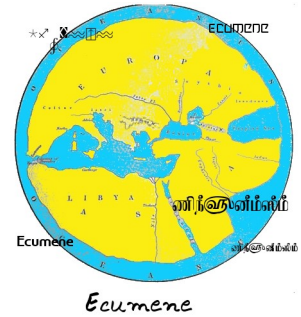
Questa fase darà origine (contestualmente o in un processo separato) ad una *analisi* della struttura e natura del documento tesa ad individuare (ad esempio tramite le proprietà MIME (o estensioni associate) o (eventualmente) S-MIME alcune informazioni *peculiari*.

Tali informazioni riguarderanno (se presenti) i *signers* (firmatari) dei/del documento/i. Tali informazioni andranno utilizzate nelle fasi immediatamente successive.



T-Services

Bridge & ttp



Interazione con la/le C.A.

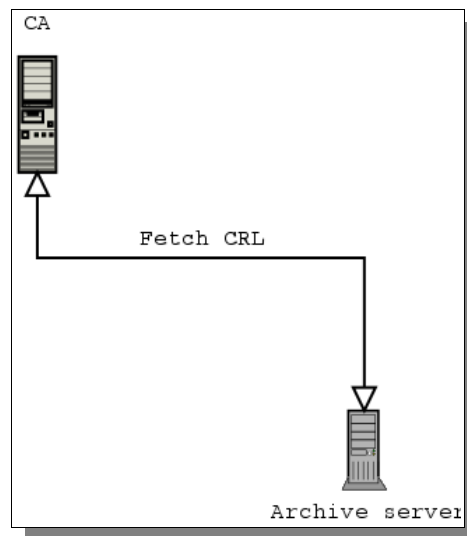


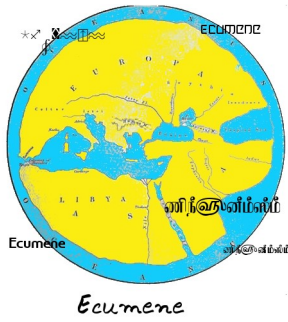
Fig.4: Aquisizione delle CRL.

Si possono dare 2 situazioni:

- 1) Per ogni signer info eventualmente presente (e in assenza di riferimenti temporali impliciti o espliciti) occorrerà procedere al *fetch* della CRL (relativa all'intervallo intercorrente tra l'operazione di archiviazione e la prossima emissione di CRL; posto che la CRL sia di tipo incrementale, in caso contrario il fetch sarà riferito alla CRL **corrente**).
- 2) Non sono presenti signers e relative signer info (il documento non è firmato in precedenza) quindi non si avrà la relativa operazione di *fetch CRL*.

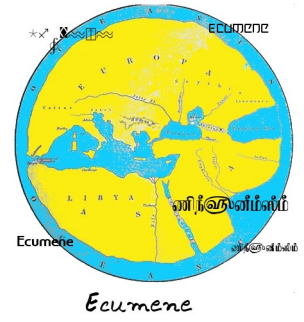
In ogni caso andranno prelevate le CRL relative alla TSA e quella relativa (se tale operazione è prevista) al certificato di firma (sigillo o protocollo) apposto dall'operatore (o server) di archivio. Se tale operazione (sigillo o protocollo) è prevista dovrà essere creata una firma relativa all'insieme costituito dai dati risultanti dal prelievo delle CRL e dal/dai documento/i da archiviare.

Successivamente a tale operazione si procederà come sotto descritto.



T-Services

Bridge & ttp



Time stamping

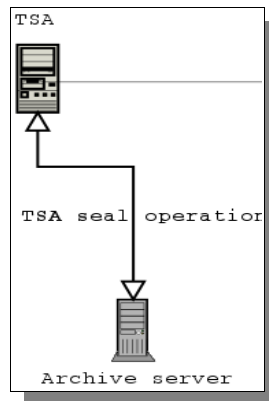


Fig.5: Sigillo Temporale

Verrà effettuata una richiesta di *digital timestamping* relativa al documento costituito dalla somma dei dati descritti in precedenza (comprendenti eventualmente il sigillo di protocollo); la struttura/documento risultante dall'insieme dei dati unitamente al *sigillo temporale* effettuato dalla TSA conterrà quindi le seguenti informazioni:

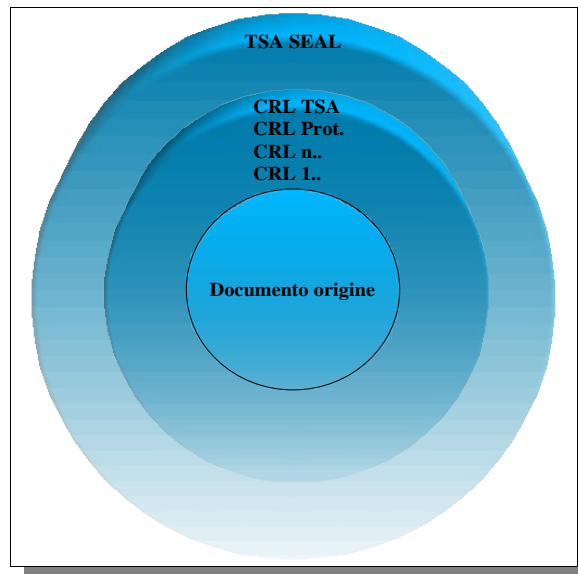
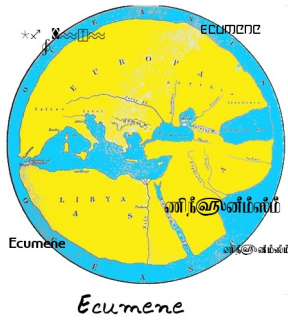


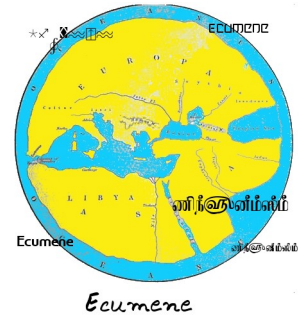
Fig.6: Struttura risultante (Archive token).

Chiameremo, per semplicità tale struttura col nome di *Archive token*.



T-Services

Bridge & ttp



Storage operations

Effettuati i passi sopra descritti rimangono da attuare alcune specifiche operazioni di interazione con il sistema di storage (*storage system*).

Alcune operazioni possono richiedere, a seconda della natura (ad es. riservatezza) dei documenti presenti nell' *archive token*, il settaggio (se possibile) di particolari proprietà del sistema di storage oltre che eventuali ulteriori operazioni di **cifratura** del *archive token*.

In estrema sintesi³ si tratterà di stabilire un *canale sicuro* di comunicazione (a seconda della sua natura trusted o semitrusted) con il sistema di storage e, dopo aver effettuato la (eventuale) cifratura del *archive token* tramite la chiave *dell'operatore archivio*, inviare, lungo tale canale, la richiesta di archivi azione, nelle modalità operative previste dalle proprietà dello storage stesso.

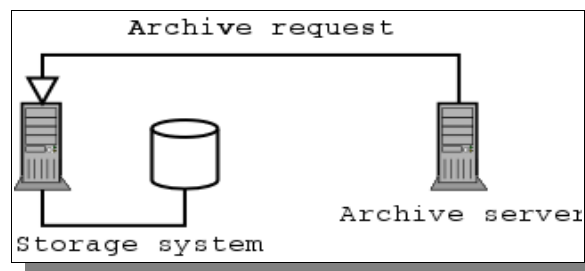


Fig.7:Archive transaction.

Tale operazione potrebbe, in astratto, essere considerata la *operazione conclusiva* della infrastruttura coinvolta nelle operazioni di archiviazione.

Tuttavia, rimane da risolvere una importante questione.

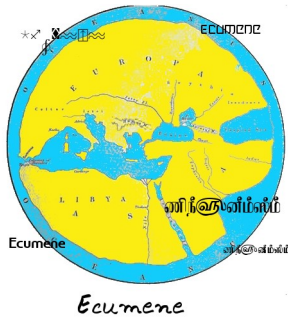
La chiave di volta di tutta la costruzione può facilmente essere identificata nelle operazioni di apposizione del *sigillo temporale* (fig.5) indispensabile al fine di costruire i dati del *archive token*.

Il certificato utilizzato dalla TSA per produrre il *sigillo temporale* avrà (con tutta probabilità una scadenza o un intervallo di validità che può cadere nel periodo in cui è ancora necessario il mantenimento del *archive token* nel suo stato di validità e auto consistenza.

In tal caso sarà necessario che l'archive server (l'operazione può essere automatizzata e schedulata) provveda immediatamente prima della scadenza del certificato ad ottenere dalla TSA (non necessariamente la stessa) la emissione di un nuovo sigillo temporale da aggiungere al *archive token*.

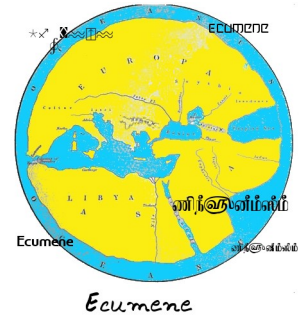
In tal modo (in assenza di una specifica policy di *discard* regolata sull'intervallo massimo di conservazione del *archive token*) il token di archivio può essere conservato per un tempo indefinito tramite le operazioni di *rinnovo* programmate.

³ Si veda il documento "Proprietà di trust dei filesystems e sistemi di storage" T-Business 07-2003.



T-Services

Bridge & ttp



Considerazioni su alcune importanti funzionalità *accessorie*

Nel presente documento non vengono affrontate problematiche di workflow, document management e document/information retrieval. Tali tipi di funzionalità non sono, per loro natura, strettamente legate o *integrate* al problema in esame. La eventuale stretta integrazione tra questo tipo di funzionalità e i sistemi di archiviazione *legale* a lungo termine, oltre a non essere necessaria corre il rischio di aumentare a in modo pericoloso (e potenzialmente caotico) le interazioni tra i diversi componenti e sottosistemi riducendo di fatto la flessibilità e rischiando il *blocco* del sistema *globale* di document management in caso di mancanza o di inoperatività funzionale o procedurale di una singola *feature* (la integrazione a tutti i costi non è sempre necessariamente un pregio).

Nei sistemi complessi occorre sempre considerare con favore quelle architetture in cui ogni componente o sottosistema sono in grado di compiere completamente le proprie funzioni con il minimo possibile di interazione e il massimo possibile di autonomia, senza necessità di *conoscere* o dare per implicitamente conosciuto, il/i processo/i che stanno a monte e a valle del sottosistema stesso. Tali funzioni sono comunque trattate in documenti a parte e riguardanti il *trusted workflow*, e lo *storage management*. Nonostante le considerazioni sopra esposte, si vogliono tuttavia accennare alcune funzioni che possono essere ritenute utili o importanti, anche se non strettamente inerenti il tipo di problematica qui affrontata.

1) La struttura a *envelope* o busta illustrata come *archive token* si presta a contenere, oltre ai dati che le sono propri, e precedentemente illustrati, campi (ad es. numeratori di protocollo), sotto strutture (ad es. XML) e informazioni (abstract ecc.) che possono risultare utili o utilizzabili a supporto di funzioni di information retrieval data management ecc.

Tali dati possono in funzione di *policy di gestione* specifiche essere introdotte anche *automaticamente* dal Archive Server.

2) L'Archive Server può supportare modalità di query/extract da inoltrare al/ai sistemi di storage.

Interoperabilità formati della struttura e standards

La struttura e le forme proposte si attengono ai seguenti standard:

RFC 822, EML, MIME, S-MIME, PKCS7, CMS (Cryptographic Message Syntax).

Tali standards hanno il vantaggio di offrire (in forma di commodities) alcune interessanti features disponibili su praticamente tutti i sistemi operativi e le piattaforme più diffuse (ad es. MS windows, Linux, BSD, Unix-Solaris e derivati e Mac OSX).

I mailers comunemente diffusi su tali piattaforme (ad es. outlook express) sono in grado (pur non essendo capaci di *costruirla* coi requisiti descritti) di *riconoscere* la forma descritta per la struttura di *archive token* e di estrarne e visualizzarne i singoli componenti (generalmente in forma di messaggi e allegati) nonché di verificare l'integrità formale delle firme e dei sigilli. Ciò dà il grande vantaggio di poter *distribuire* o consultare le strutture create tramite Archive Server senza necessità di software aggiuntivo e costose "*per seat licenses*".