HSM e firma digitale remota

Da alcuni anni sono sopraggiunte le soluzioni di “firma digitale remota” che stanno riscuotendo un notevole apprezzamento da parte degli utenti. Con questa soluzione l’utente non possiede fisicamente il dispositivo di firma, ma utilizza un dispositivo, denominato HSM (Hardware Security Module), su cui sono utilizzate le chiavi crittografiche necessarie per la generazione della firma digitale.

L’accesso al dispositivo è sempre protetto da adeguati fattori che garantiscono il principio di sicurezza menzionato precedentemente. Il principio di conoscenza è garantito dalla necessità di conoscere un PIN (spesso anche una userid), quello di possesso da un dispositivo fisico, quali i generatori di password usa e getta (OTP) ma, soluzione sempre più apprezzata, dal proprio telefono cellulare (più precisamente dalla propria SIM). L'uso del telefono cellulare arrichisce la sicurezza per due ragioni. Eventuali tentativi di attacchi dovrebbero essere portati a termine contemporaneamente sulla rete internet e sulla rete di telefonia mobile; l'esperienza insegna che può trascorrere molto tempo prima che un utente si accorga di non possedere più la smartcard od il token di firma, mentre dopo pochi minuti si accorge di aver smarrito il proprio cellulare.

Le soluzioni di firma remota, fornite da quasi tutti i certificatori, sono spesso disponibili anche per iPad, IPhone, Tablet.

Infine, la soluzione di firma remota ha il valore aggiunto di essere sotto il controllo del certificatore che custodisce il dispositivo HSM. Il certificatore quindi sa quando un determinato soggetto genera una firma digitale (la segretezza dell’oggetto della firma è comunque garantito). Questo consente di poter realizzare un servizio di particolare interesse: avere un avviso ogni volta che una firma digitale remota è generata.

Pa Compliance include connettori per i servizi di firma remota dei principali fornitori quali Aruba, Infocert, Actalis.

Antica Bottega Digitale srl - via Bologna 14 e/f - 52100 Arezzo (AR)
Tel: 0575294234 - Fax: 0575294269
www.abd.it
staff@abd.it

PA Compliance

Sistema centralizzato di trattamento dei documenti amministrativi a norma

IL 25 GENNAIO 2010 è entrato in vigore il nuovo CAD, il Codice dell’Amministrazione Digitale (Decreto legislativo n. 235/2010, pubblicato sulla Gazzetta Ufficiale del 10 gennaio 2011, n. 6).

Tra le novità introdotte di particolare rilelevanza appaiono quelle che vanno a definire le modalità di interazione della Pubblica Amministrazione con i cittadini relativamente a documenti informatici e canali telematici, sopratutto in considerazione del fatto che sempre di più i documenti amministrativi sono prodotti e gestiti tramite sistemi informatici.
(Art. 1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l’uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti di cui all’articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.)

Per effetto dell’art. 5-bis del CAD stesso, i rapporti tra le PA e le imprese dovranno avvenire esclusivamente per via telematica. Ciò vale sia nel caso in cui è l’impresa a presentare istanze e dichiarazioni, sia quando le PA adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese. Ciò costituisce un obbligo con una ampia serie di implicazioni proprio riguardo al trattamento dei documenti e degli atti dell'ente.

L'Articolo 4.1 - Partecipazione al procedimento amministrativo informatico
sancisce che "La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l’uso delle tecnologie dell’informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445."

L'insieme di queste ed altre norme che riguardano firma digitale, data certa, documento amministrativo elettronico, l'emissione di copie analogiche di documenti amministrativi elettronici, la garanzia del diritto di accesso, la conservazione a norma dei documenti amministrativi elettronici, il protocollo digitale, la pec, etc pone la pubblica amministrazione di fronte alla esigenza di predisporre processi e soluzioni tecnologiche di trattamento documentale in grado di assicurare la "compliance" complessiva dell'ente.

Alfresco

ServiceMix

"PA-Compliance è una soluzione tecnologica e metodologica, basata su componenti open source, per rispondere agli obblighi di trattamento dei documenti digitali nella pubblica amministrazione"

Servizi centralizzati di trattamento a norma

I servizi messi a disposizione da PA Compliance sono:

Conservazione a norma dei documenti digitali

Accessibilità dei documenti informatici da parte del cittadino

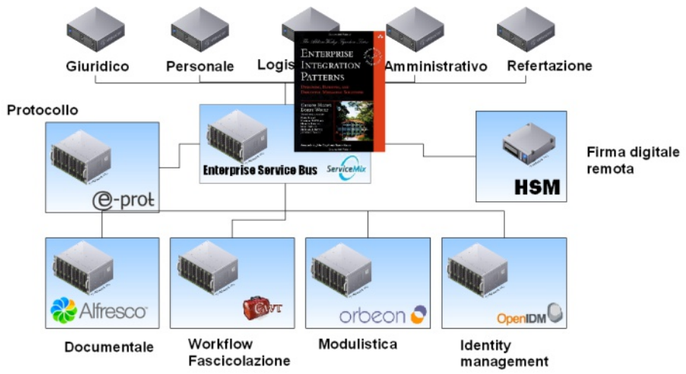
Integrabilità informatica dei documenti nei flussi della organizzazione

Rispetto della normativa della privacy

Auditing degli accessi

Controllo degli accessi

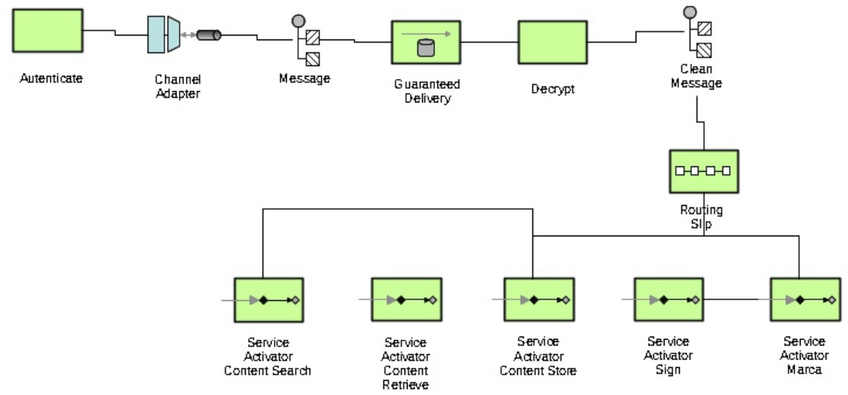
Emissione di copie analogiche con con timbro digitale



PA-Compliance utilizza le funzionalità di un Enterprise Service Bus ovvero quella di “interconnettere” isole tecnologiche e/o applicative eterogenee costruendo una infrastruttura Service Oriented nella quale all'ESB sono delegate funzioni orchestrative, di routing ed eventualmente anche di trasformazione adattiva delle comunicazioni tra le varie “isole” informative.

Mediante l'Enterprise Service Bus le applicazioni che producono documenti (sistemi di refertazione, protocollo, gestione atti e delibere, anagrafe etc etc) possono "consegnare" il documento completo di metadati al sistema centralizzato di trattamento PA Compliance utilizzando vari protocolli (SOAP, Ftp, SMTP, Rest, etc) specificando quale tipo di trattamento dello stesso desiderano che sia svolto da PA Compliance. E' possibile richiedere la semplice archiviazione centralizzata, così come richiedere l'apposizione di una firma digitale, della marcatura temporale o la produzione di una copia conforme con timbro digitale.

In modalità asincrona l'applicazione riceverà al termine del processo di trattamento un messaggio con i puntatori al documento originale (eventualmente firmato e marcato temporalmente) ed alla copia conforme timbrata.



Architettura EIP

L'architettura di Pa Compliance è stata progettata secondo la metodologia degli Enterprise Integration Patterns ed utilizza un paradigna di Slip Router per processare le richieste di servizio. Ciascun documento preso in carico viene incapsulato all'interno di una struttura di messaggio normalizzata tipica degli ESB. Il messaggio è corredato di una lista di comandi che lo slip router è in grado di interpretare, computando la "rotta" opportuna verso gli altri componenti incapsulano i servizi. Questi componenti si occupano ciascuno di compiti precisi e specifici come la archiviazione nel repository (Alfresco), il recupero di documenti dallo stesso, l'esecuzione di una firma digitale (sono gestibili firme sui formati pdf/a, odt, docx, xml oltre al "vecchio" formato p7m) oppure la produzione di un copia conforme del documento per la stampa completa, in ottemperanza alla vigente normativa, del timbro digitale.

Timbro digitale

Il timbro digitale è una tecnologia utilizzata nell'ambito della Pubblica Amministrazione italiana e di alcune società private per consentire la creazione di documenti informatici (ad esempio, certificati di anagrafe) validi legalmente anche dopo essere stati stampati.

Una volta stampato, il documento include un codice grafico (normalmente codici a barre bi-dimensionali, in quanto quelli mono-dimensionali non consentirebbero di registrare la quantità di dati necessaria), che contiene le informazioni relative al documento informatico e alla firma digitale. Questo approccio ed il concetto di "firma digitale su carta", è stato presentato per la prima volta nel 2001 alla XXXIX Annual Conference AICA. Il termine "timbro digitale" è stato coniato dal CNIPA (ex AIPA, ora DigitPA).

Il timbro digitale consente di mantenere inalterata, anche nel processo di stampa, la validità legale di un documento informatico firmato digitalmente, dal momento che la versione stampata può essere letta e decodificata tramite uno scanner o in certi casi anche con un lettore di codici a barre bidimensionali ed un apposito software di visualizzazione.

L'adozione del timbro digitale consente agli enti pubblici di emettere certificazioni via web, con risparmi di tempo per gli utenti (cittadini ed imprese) e di costi per l'ente stesso.

Una tecnologia analoga al timbro digitale fu attivata già nel 2003 ma soltanto con l'intervento del CNIPA è stato possibile definirne con esattezza alcuni requisiti. Al 2010, il timbro digitale è adottato da regioni (Emilia-Romagna, Sardegna), comuni (anche grandi, come Marsala, Agrigento, Milano, Roma, Torino, Perugia) e province soprattutto per il rilascio di certificati anagrafici ma anche, per esempio, per l'emissione di cedolini.

Il Timbro Digitale è stato adottato dal Ministero dell'Economia e delle Finanze (per il progetto eCedolino 2006 e certificazioni on line), dall'IPZS (Gazzette Ufficiali da gennaio 2009) ed altri Enti della Pubblica Amministrazione Centrale.