Lo stato di avanzamento della legislazione e della standardizzazione della firma elettronica in Europa

Il Cen è il Comitato Europeo che si occupa della standardizzazione: in particolare, il Cen/Isss si occupa della "Società dell'Informazione".

L'E-Sign Workshop è il gruppo di lavoro nell'ambito del Cen/Isss che impegna le proprie risorse nella standardizzazione della firma elettronica e di tutte le procedure di sicurezza ad essa correlate.

Il processo di standardizzazione segue le stesse regole ed è identico al processo che ha portato alla definizione dello standard GSM. Si configura perciò come un pre-standard. Una volta stabilizzati i relativi contenuti tecnici è possibile che divenga uno standard Cen, seguendo la procedura formale di approvazione da parte dei membri del Cen, che sono esclusivamente i singoli enti nazionali di standardizzazione (UNI, DIN, BS, etc.). Inoltre, secondo quanto dichiarato a Bruxelles alla EESSI Conference del 19 giugno 2001 dal Commissario Liikanen, il Comitato previsto dall'articolo 9 della Direttiva 1999/93/CE in materia di firma elettronica "referenzierà" detti pre-standard e ne raccomanderà alla Commissione la pubblicazione nella Gazzetta Ufficiale della Comunità Europea.

Mentre nel Cen sono rappresentati tutti gli stati membri della Comunità Europea attraverso la partecipazione ai lavori degli enti nazionali di standardizzazione, il Cen/Isss, è un Open Workshop gestito sul piano organizzativo ed amministrativo dal Cen, ma interamente finanziato dalla Comunità Europea. Pertanto ai lavori del Cen/Isss partecipano non solo aziende coinvolte nelle produzione o commercializzazione di PKI, ma altresì privati e organizzazioni scientifiche o rappresentative di interessi diffusi. Due le ragioni principali per cui si è organizzato un Open Workshop in luogo di seguire il processo formale di standardizzazione:

1) l'esigenza di conseguire una rapida approvazione degli standard, fondamentale nel settore della sicurezza informatica dove elevato è il rischio di non riuscire a tenere il passo con l'evoluzione tecnologica e del mercato,

2) l''esigenza di favorire il più ampio coinvolgimento possibile nella determinazione del contenuto di standard che sono richiamati da importanti norme del diritto europeo (quale la direttiva 1999/93/CE sulla firma digitale), nonché dalle normative nazionali di attuazione in corso di approvazione da parte degli stati membri.

Il risultato dell'attività di standardizzazione nell'ambito del Cen/Isss sono i CWAs (Cen Workshop Agreements) che vengono votati dai membri del workshop secondo il principio di un voto per membro. Le specificazioni tecniche così approvate costituiscono i pre-standards a cui si è accennato.

Ma esistono altre ragioni per cui la Commissione ha deciso di promuovere e finanziare Cen/Isss.

Innanzitutto la legislazione nazionale (ed Europea) può avere solo un impatto limitato sugli standard e sulle tecnologie in uso su Internet (e dunque utilizzate ben oltre i confini del singolo stato o dell'Unione Europea).. Le leggi non possono (e non devono) condizionare lo sviluppo tecnologico più di quanto non accada già. È possibile, invece, riscontrare che Internet (e la tecnologia informatica) influenzano la normativa legale in modo quasi unilaterale. Ciò è stato sostenuto in modo convincente dal prof. Lawrence Lessig con le sue ricerche presso l'Università statunitense di Harvard. Ne consegue che occorre coordinare la potestà normativa statale con la capacità autoregolativa della tecnologia informatica. A tal fine occorre che il livello di sicurezza all'interno delle reti aperte sia incrementato trovando un punto di equilibrio fra tra la qualità del servizio (QOS) e il principio di end-to-end. Tale equilibrio nell'ambito dell'IETF e del World Wide Web Consortium non è ancora stato raggiunto, lasciando spazio ad iniziative che intendono garantire il QOS a scapito della apertura delle reti. Infatti monopolisti e alcuni grandi produttori di tecnologia tendono a sostenere le proprie soluzioni proprietarie a scapito sia della apertura delle reti aperte, sia della loro sicurezza. Il fatto che grandi aziende quali IBM e SUN abbiano iniziato a supportare lo sviluppo di tecnologie "open source" consente tuttavia di sperare in meglio.

Una ragionevole fiducia nella tecnologia significa anche neutralità dell'infrastruttura e del suoi gestori, vale a dire piena applicazione del modello della "terza parte fidata".

Questi principi ed obbiettivi stanno alla base dell'infrastruttura in via di costruzione in Europa:

1. conseguire i vantaggi dell'Information Technology senza però rinunciare alle garanzie e alle funzionalità della carta (in primo luogo, costituiti dalla disponibilità a lungo termine delle informazioni.

2. combinare la libertà e l'anonimato delle tradizionali transazioni commerciali con una migliore qualità della documentazione, incrementando la trasparenza nei confronti dei clienti (consumatori e utenti professionali) attraverso una documentazione appropriata. Ottenere un tale risultato permetterebbe anche alle piccole e medie imprese di raggiungere un'integrazione tra la prassi degli affari e i sistemi di Information Technology e ciò è molto importante, soprattutto se si riflette su un possibile allargamento ad Est dell'Unione Europea, dove la maggioranza delle imprese sono di piccole dimensioni.

3. ottenere una maggiore partecipazione dei cittadini alle attività delle istituzioni europee.

Questi obiettivi sono innovativi ed è chiara la loro straordinaria importanza, ma è altresì chiaro come può essere difficile il loro raggiungimento. Per conseguirli, è necessario che l'infrastruttura stessa sia in grado di risolvere alcune problematiche.

- Innanzitutto, per creare un'infrastruttura tecnologica valida nel settore della firma elettronica, esiste il problema della rilevanza legale del nuovo tipo di firma e della responsabilità correlate, problema che la Direttiva Europea 1999/93/CE si prefigge di risolvere creando due categorie principali di firme elettroniche: quelle equiparate alla firma autografa e quelle la cui rilevanza legale non può essere negata (i cui strumenti di

generazione ed applicazione non sono soggetti ad una verifica di qualità da parte di laboratori di valutazione indipendenti, ovvero da parte della autorità di supervisione).

- Un altro ostacolo è sicuramente quello di trovare un equilibrio tra la sicurezza e la protezione dei dati personali, in via di soluzione nell'attività di standardizzazione europea. Il formato di certificato proposto in Italia da questo punto di vista dall'Assocertificatori costituisce una soluzione che fa un uso eccessivamente intensivo di dati personali e di fatto impedisce la possibilità di operare sotto pseudonimo, per cui è lecito dubitare se possa costituire un certificato qualificato ai sensi della direttiva 1999/93/CE, nonché che possa essere considerato compatibile con la direttiva comunitaria in materia1997/66/CE). Infatti gli esperti di privacy hanno espresso persino dubbi che lo pseudonimo previsto dall'Allegato I alla direttiva 1999/93/CE sia uno strumento in grado di garantire adeguata riservatezza.

- L'accettazione sociale dei modelli di business costituirà comunque il principale impedimento al definitivo lancio dei servizi connessi alla firma elettronica. In realtà occorre ancora riflettere con attenzione se sia giusto e praticabile in concreto, richiedere agli utenti delle reti aperte di firmare le tutte le transazioni. Ciò ha implicazioni giuridiche ed organizzative immani. Occorrerebbe sapere invece focalizzare le applicazioni della firma digitale non alla sottoscrizione dei contratti, bensì alla autenticazione a distanza. Oltre a risolvere i problemi tecnici ed organizzativi connessi, occorre sapere concepire nuove complesse forme di identificazione personale, che siano adeguate a resistere ad un intenso uso "on-line". Infatti è una idea assai superficiale, ritenere che sia possibile identificare una persona solo mediante l'esibizione di un documento di identità con fotografia (3 cm x 3 cm, magari neppure di recente data). Il concetto stesso di identità sta subendo una mutazione, dal momento che è stato definito per essere utilizzato in transazioni in cui vi era un contatto (magari indiretto o mediato) fra parti fisiche, mentre ora il medesimo concetto di identità (identificazione) dovrebbe funzionare per rapporti sempre a distanza e privi di mediazioni.

Cerchiamo ora di capire da una breve analisi dei principi racchiusi nella Direttiva Europea 1999/93/CE che cosa sta succedendo da un punto di vista legale in tema di PKI in Europa.

- Il principio della co-regolamentazione. Il legislatore determina gli scopi, l'autoregolamentazione tecnica definisce i mezzi nel pieno rispetto degli standards internazionali già esistenti. Questo approccio europeo è innovativo ed è molto importante, perché la Comunità Europea cerca di ovviare agli eccessi di regolamentazione per i quali è stata spesso oggetto di critiche: ora si cerca di trovare il giusto equilibrio tra la necessità di garantire che le leggi siano definite nei contenuti a livello politico e la necessità che la normativa tecnica di dettaglio sia determinata e supportata anche dall'industria e dagli utilizzatori.. Questo difficile equilibrio può essere raggiunto proprio grazie alla co-regolamentazione: il legislatore definisce i principi da rispettare, l'industria e i consumatori determinano i contenuti, le procedure e gli standards necessari per garantire la corretta implementazione ed applicazione dei principi stessi. La co-regolamentazione sembra inoltre,

l'approccio normativo capace di coordinare architetture e protocolli tecnici (definiti a livello globale) con le norme della legge nazionale: è pertanto un processo che potrebbe avere una capacità stabilizzatrice dei rapporti oggi estremamente conflittuali fra legge e norme tecniche.

- Il principio della neutralità a livello tecnico. La Direttiva Europea cerca di non interferire sulle modalità tecniche di raggiungimento degli obiettivi preposti: per firmare elettronicamente una transazione, non si è fatto riferimento alle smartcards, ma anche al telefono mobile piuttosto che ai PDA o qualsiasi altra tecnologia esistente o in via di creazione (potrebbe essere persino una tecnologia diversa dalla crittografia asimmetrica).

- La protezione dei dati. La Direttiva Europea dà molta importanza a questo principio. L'uso delle firme elettroniche non deve permettere di accedere ai dati personali degli utenti più facilmente di quanto accada con l'uso della firma autografa. La libertà di usare uno pseudonimo deve essere garantita, perché l'anonimato è un diritto da tutelare soprattutto per le transazioni di commercio elettronico; l'anonimato deve essere difeso così come è difeso in un esercizio commerciale reale e non virtuale come un sito Internet. Naturalmente l'Unione Europea, che ha fatto della protezione dei consumatori uno dei suoi principi cardine, sta rendendo tale tutela molto forte, creando una infrastruttura che renda la tecnologia il più trasparente possibile nei confronti degli utenti e ciò per quanto riguarda il dispositivo di firma, i certificati e tutto il sistema che ruota attorno alla firma elettronica. Le più recenti ricerche scientifiche in materia di tecnologia per l'anonimizzazione, tuttavia, hanno sollevato alcuni dubbi sulla idoneità del certificato qualificato, come delineato dall'allegato I alla direttiva 1999/93/CE, a tutelare adeguatamente la privacy ed il diritto ad agire sotto pseudonimo.

- Il principio di non-discriminazione di mutuo riconoscimento all'interno dell'Unione Europea.Benché la direttiva 1999/93/CE non si riferisca specificamente agli standards in via di creazione da Etsi e Cen/Isss, essi avranno un ruolo particolarmente importante trattandosi presumibilmente dei primi standards che saranno pubblicati dalla Commissione, sulla base di una delibera del cosiddetto Comitato ex articolo 9. Altri sicuramente seguiranno. La co-operazione multilaterale tra i supervisori in Europa è già cominciata ed a Milano in Ottobre si terrà una delle prime riunioni di coordinamento fra enti di valutazione e certificazione (fra i quali anche numerosi enti di supervisione nazionale dei certificatori qualificati).

- Il principio della non-discriminazione internazionale. La Direttiva è cosciente dell'importanza della non-discriminazione internazionale. L'art. 7 prevede il riconoscimento internazionale alla firma elettronica proveniente da un Paese terzo, purché il prestatore dei servizi di certificazione possieda i requisiti previsti dalla Direttiva Europea e sia stato accreditato nell'ambito di un sistema di accreditamento volontario; oppure, quando i certificati sono garantiti da un prestatore di servizi di certificazione stabilito nella Comunità Europea in possesso dei requisiti previsti dalla Direttiva o ancora se il certificato o il prestatore dei servizi di certificazione è riconosciuto in virtù di un accordo bilaterale o multilaterale tra la Comunità e i Paesi Terzi o organizzazioni internazionali. Le tre condizioni sono alternative e quindi soltanto una di esse basta per soddisfare i requisiti che impongono il riconoscimento della firma elettronica "extracomunitaria". Il fatto che sia data rilevanza agli accordi internazionali

con Stati extra-Europei e organizzazioni internazionali è molto importante per dare rilevanza globale alla soluzione normativa ed agli standard tecnici in via di definizione in Europa.

- Un ulteriore principio è costituito dalla libertà di fornire servizi di certificazione. La supervisione statale può avere ad oggetto solo i certificatori qualificati e le leggi nazionali non possono sottoporre neppure i certificatori qualificati a procedimenti di concessione di licenze o autorizzazioni per potere iniziare l'attività..

- Infine, la Direttiva Europea prevede una differenza nella rilevanza legale della firma elettronica. Se la firma è generata mediante un dispositivo di firma sicura, ha le caratteristiche formali e tecniche della firma elettronica avanzata ed è connessa ad un certificato qualificato, la direttiva le attribuisce lo stesso livello di rilevanza legale della firma autografa (art. 5.1 della direttiva). È altresì sancito che, qualsiasi altro tipo di firma elettronica debba potere avere rilevanza legale: non è possibile negare alla firma elettronica valore giuridico per il solo fatto che non sia una firma elettronica sicura. Infatti neppure le firme autografe (ed i relativi documenti cartacei) sono a prova di falsificazione eppure la loro rilevanza legale è fuori discussione da almeno due secoli (prima era spesso necessaria anche la presenza di un notaio o di testimoni). I problemi maggiori problemi di sicurezza dei documenti firmati elettronicamente sono una conseguenza del fatto che si tratta di contratti a distanza che circolano e sono conservati su sistemi aperti spesso poco sicuri, non dalla intrinseca debolezza della firma digitale. Per accrescere la affidabilità dei documenti digitali occorrono ora applicazioni e soluzioni organizzative alla altezza delle esigenze degli utenti e non meccanismi di firma più sicuri.. Infatti l'unico anello debole del processo di firma è il WYSIWYS (What You See Is What You Sign) e questo può essere rafforzato solo se si disponesse di hardware e software sicuri. Allo stato delle tecnologie in uso occorrerebbe studiare soluzioni per evitare che sia eccessivamente facile ingannare il dispositivo di firma sostituendo i dati da firmare con altri. Da questo punto di vista telefoni cellulari e PDA costituiscono ambienti sicuramente più affidabili dei personal computers per apporre la firma elettronica.

La Direttiva Europea 1999/93/CE è diventata obbligatoria per gli Stati Membri il 19 luglio 2001.

Molte legislazioni nazionali devono a tutt'oggi essere completate. L'organizzazione e la gestione operativa degli Enti di Supervisione non è del tutto strutturata e i loro nominativi, insieme a quelli dei Prestatori dei Servizi di Certificazione, devono essere notificati alla Commissione Europea.

L'implementazione della Direttiva è particolarmente avanzata in Germania, Francia e Austria. In Italia si è in presenza di una bozza di decreto che ancora deve seguire l'iter legislativo previsto dalle normativa italiana.

Una questione ancora aperta nell'implementazione della Direttiva Europea è l'interoperabilità.

In Europa se ne occupa un progetto all'interno del 5° Programma Quadro denominato "PKI Challenge" che sta coinvolgendo le aziende leader nell'area della sicurezza informatica e che

lavora a stretto contatto con il PKI Forum statunitense. Ci sono altresì molti progetti di schemi di certificazione omogenei all'interno dell'Europa. L'accreditamento è volontario, secondo la Direttiva, ma questo non significa che sia irrilevante.

Vediamo ora nel dettaglio a che punto è il lavoro svolto nell'ambito di Eessi, l'iniziativa europea per la standardizzazione delle firme elettroniche, frutto della cooperazione tra Etsi e Cen/Isss.

Il Workshop Cen/Isss E-Sign ha già approvato standards che riguardano il processo di firma, il processo di verifica della firma,il dispositivo di firma sicura e i requisiti di sicurezza per i sistemi che si occupano di emettere i certificati qualificati (definisce il c.d. Trustworthy System). Il gruppo di lavoro Etsi Esi Sec ha approvato quattro standards: i profili relativi alla marcatura temporale, i formati della firma elettronica, i requisiti per le Autorità di Certificazione che emettono certificati qualificati e i requisiti dei certificati qualificati stessi.

Un altro CWA è in dirittura d'arrivo:è denominato "Linee guida per l'accertamento della conformità" ed è molto importante per la definizione dei ruoli dei sistemi di accreditamento.

L'attività di Eessi continuerà fino alla fine del 2002 e altri temi saranno sviluppati dai gruppi di lavoro: molto rilevante l'attività portata avanti dal gruppo AA di Cen/Isss Ws E-Sign che cerca di definire i requisiti per l'uso sicuro dei certificati qualificati in ambienti specifici, quali ad esempio le applicazioni di e-commerce. Altrettanto importante l'area K, che si occupa delle specifiche per l'interoperabilità delle smartcards. Un "Algorhythm Group" sta compiendo una ricerca volontaria sulla sicurezza degli algoritmi.

La standardizzazione Etsi ha a sua volta obiettivi molto ambiziosi e sta continuando a lavorare su temi importanti quali la sicurezza della gestione e le linee di condotta per i prestatori di servizi di certificazione che emettono marcature temporali e altro rispetto ai certificati qualificati, la sintassi della firma elettronica e i formati di codificazione, le linee di condotta per la firma elettronica e altre previsioni per l'armonizzazione dei servizi di certificazione.

Probabilmente il giusto equilibrio tra il bisogno di sensibilità politica e di trasparenza potrebbe essere raggiunto con una maggiore cooperazione tra il processo di standardizzazione europeo, il PKI Forum statunitense e quello asiatico e sforzi in tal senso sono continuamente compiuti dal comitato di direzione di Eessi.

In questo modo, si cerca di creare standards che costituiscano le basi per un'infrastruttura comune che porti al successo della firma elettronica. Ma nello stesso tempo, si sta mettendo in atto un'attività di negoziazione politica per raggiungere il grado massimo di efficacia che una soluzione troppo tecnica potrebbe mancare.

E' importante a questo fine pensare e agire globalmente e utilizzare gli standards internazionali in modo trasparente, possibilmente senza vincoli proprietari, in modo che il loro utilizzo sia libero e possa portare ad una interoperabilità internazionale, necessaria affinché il lavoro di questi anni non si riveli inutile.

Il business plan per l'attività di standardizzazione nell'anno 2002 è in corso di discussione e sarà presumibilmente approvato nel meeting di Milano di Etsi del 2 e 3 ottobre e Cen/Isss del 3 e 4 ottobre. Indicazioni, suggerimenti, commenti sono graditi all'indirizzo di e-mail e.security@sng.it. Gradita sarebbe anche una massiccia partecipazione dei certificatori italiani.

Riccardo Genghini
Chairman Cen/Isss Ws E-Sign

Cinisello B. 20092 via Libertà n. 89
Tel. 02. 66099.1 Fax. 02. 66099.666
EMAIL : cinisello.office@sng.it

Milano 20121 via S. Pietro all'Orto n. 17
Tel. 02. 763030.1 Fax. 02. 763030.29
EMAIL: milano.office@sng.it

00198 R o m a Via Luigi Boccherini, 3
Tel..06. 85356919 Fax.06. 8540260
EMAIL roma.office@sng.it