Stato di avanzamento della standardizzazione della firma elettronica in Europa

A che punto è il processo di realizzazione delle infrastrutture per la firma digitale ?

La disciplina della firma elettronica e dei suoi requisiti tecnici di sicurezza necessita di regole di interoperabilità che debbono avere una portata che le regole nazionali non possono avere. Solo regole di sicurezza e di interoperabilità di portata globale possono garantire che, in un mercato aperto e transnazionale come quello di Internet, chiunque sia in grado di scambiarsi documenti elettronici firmati, a prescindere dal soggetto certificatore e da eventuali differenze nelle tecnologie e nella struttura dei certificati utilizzati.

La Direttiva Europea sulla firma elettronica (1999/93/CE) ha cercato di risolvere il problema, indicando obbiettivi di sicurezza e criteri di rilevanza giuridica, lasciando però ad organi di autoregolamentazione internazionale (Cen ed ETSI) la specificazione delle modalità organizzative e tecniche. La problematica dell'interoperabilità della firma elettronica non è stata risolta (e non poteva essere risolta) dall'emanazione della Direttiva 1999/93/CE. Il processo di autoregolamentazione è stato affidato ad una apposita iniziativa: European Electronic Signatures Standardisation Initiative (EESSI), finanziata dalla Commissione Europea ed affidata a due enti di standardizzazione Europea: il Comité Européen de Normation (CEN), di cui sono membri i comitati nazionali di normazione (DIN, UNI, ecc.) e l'European Telecommunication Standards Institute (ETSI) che è l'organizzazione non-profit che rappresenta gli interessi di amministrazioni pubbliche, operatori del settore, aziende di produzione, fornitori di servizi, organismi di ricerca, utenti finali.

Il CEN nel 1997 per gestire la autoregolamentazione ha istituito una apposita iniziativa denominata CEN/ISSS (Information Society Standardisation System), che nel suo Workshop E-Sign si occupa della standardizzazione dello strumento di firma digitale (Aree F ed AA), dei modelli di sicurezza crittografica (Area D), del processo di generazione e di verifica della firma digitale (Area G). Il Workshop è quest'anno presieduto da un giurista italiano, il dr. Riccardo Genghini.

ETSI ha istituito a sua volta, sotto la presidenza dello svedese (di origini ungheresi) György Endersz un Workshop Etsi Sec Esi (Electronic Signatures and Infrastructures) che è l'organismo responsabile per la standardizzazione della firma elettronica e delle infrastrutture relative: tramite una speciale Task Force composta da esperti di vari Paesi europei.

I due Workshop collaborano strettamente e sono coordinati da uno Steering Group presieduto da Claude Boulle ed al quale partecipa anche il Prof. Roberto Benzi, componente dell'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA), oltre a rappresentanti della Commissione Europea, ai presidenti dei due Workshop ed a esperti di fama internazionale nel campo della sicurezza informatica.

I Workshop hanno approvato finora sette importanti standards.

Tre sono stati approvati nei mesi di marzo ed aprile del 2001da CEN-ISSS, sotto forma in CWAs (CEN Workshop Agreement): CWA 14767-1 e 14167-2; CWA 14168 e 14169; e CWA 14170 e 14171, prossimamente consultabili sul sito www.cenorm.be/isss/workshop/e-sign.

Il CWA 14767 "*Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures" è composto di due sezioni:* il CWA 14767-1 specifica i requisiti di sicurezza delle infrastrutture tecnologiche utilizzate dai fornitori dei servizi di certificazione per creare Certificati Qualificati; il CWA 14767-2 definisce i requisiti di sicurezza dei moduli crittografici.

Il CWA 14168 – 14169 "*Security Requirements for Secure Signature Creation Devices"* definisce i requisiti del dispositivo di firma sicuro conforme alle indicazioni mandatarie dell'Annex III della Direttiva 1999/93/EC, usando la metodologia dei Common Criteria (ISO 15408).

Il CWA 14170 - 14171 "*Signature Creation and Validation Process and Environment"* interessa due aspetti ritenuti non vincolanti per la Direttiva 1999/93/CE, ma considerati così importanti da giustificare lo sviluppo di due specifiche. La prima provvede affinché l'ambiente, il sistema che incorpora la creazione della firma sia implementato in modo sicuro. Il secondo propone le specifiche di sicurezza dell'ambiente di verifica della firma digitale.

Gli standard approvati da ETSI sono quattro, con i numeri di riferimento ETSI TS 101733, ETSI TS 101456, ETSI TS 101862, ETSI TS 101861(per il loro testo integrale si veda www.ict.etsi.fr/eessi).

Lo standard "*Electronic Signature Formats"* (ETSI TS 101 733) è stato pubblicato nella prima fase dei lavori (nel maggio del 2000, con alcune modifiche di minima entità a fine 2000) e definisce i formati di varie forme di firma elettronica e un formato sperimentale per le policy di firma.

Questo documento detta le specifiche per l'uso dei "Trusted Service Providers" (le Autorità di Certificazione, di registrazione, di marcatura temporale) e i dati che devono essere archiviati (ad esempio le liste di revoca) affinché una firma digitale sia valida a lungo termine. Regola altresì l'uso dei servizi di marcatura temporale al fine di provare la validità della firma anche dopo il normale ciclo di vita di alcuni suoi elementi critici essenziali.

Lo scopo dello standard *Policy Requirements for Certification Authorities issuing Qualified Certificates (*ETSI TS 101456), approvato e pubblicato nel dicembre del 2000, è quello invece di specificare le policy di sicurezza che le Autorità di Certificazione devono mantenere per la fornitura di certificati qualificati ai sensi della Direttiva 1999/93/CE. Sono state a tale proposito standardizzate le procedure di registrazione, di generazione dei certificati, di diffusione dei certificati, di gestione delle revoche, di fornitura del dispositivo di firma, oltre che il meccanismo di marcatura temporale e i certificati di attributo.

Lo standard *Qualified Certificates Profile* (ETSI TS 101 862) è basato sulla bozza IETF *X.509 Public Key Infrastructure Qualified Certificates Profile*. Lo

scopo di questo standard è quello di specificare i formati e i contenuti dei Certificati Qualificati in base alle disposizioni degli Annex I e II della Direttiva Europea. Anche questo standard, così come il precedente, è stato approvato e pubblicato nel dicembre del 2000.

L'ultimo standard approvato in via definitiva da Etsi Sec nello stesso periodo si riferisce alla marcatura temporale e definisce il *Time Stamping Profile* (ETSI TS 101 861), in particolare i formati e i protocolli relativi. La base è costituita dallo standard IETF *Time Stamp Protocol*.

I lavori previsti nell'ambito della Task Force internazionale continueranno per tutto il 2001: il programma di lavoro di EESSI è consultabile su

http://www.ict.etsi.org/eessi/EESSI-homepage.htm

Riccardo Genghini r.genghini@sng.it