DAI MAINFRAME ALL'XML TRUST PASSANDO PER IL PROCESSO TELEMATICO

I nuovi scenari di comunicazione offerti da Internet e l'apertura dei sistemi informatici verso l'esterno, ci hanno posto di fronte a nuove stimolanti prospettive, che hanno immediatamente dovuto fare i conti con l'annoso e cruciale problema legato all'accesso ed alla modifica di informazioni confidenziali da parte di persone non autorizzate.

Quando la maggior parte dell'elaborazione dei dati informatici era basata sulla tecnologia dei grossi calcolatori chiamati in gergo "mainframe", e dei terminali remoti c.d. stupidi, la gestione e la elaborazione dei dati avveniva presso centri di calcolo di notevoli dimensioni. I computers degli utenti remoti consistevano semplicemente in un monitor che assolveva alla funzione di visualizzazione delle risposte dei grossi calcolatori e di trasmissione di messaggi. L'avvento di Internet e le mutate modalità di interscambio o, *rectius*, di cyber-scambio tra i calcolatori informatici hanno subito messo in luce l'importanza di dotarsi di infrastrutture e sistemi in grado di garantire una protezione a livello di rete tramite l'installazione di firewall, antivirus e spy-ware. Tuttavia, al giorno d'oggi, neanche queste precauzioni sono più sufficienti. La spiegazione di questa affermazione è legata a tutta una serie di problematiche che le nuove tecnologie hanno fatto affiorare: una di esse riguarda la trasmissione dei file in formato Xml (Extensible Markup Language).

In questo documento mi propongo di affrontare una generale panoramica di quelli che sono gli aspetti più o meno recenti della sicurezza informatica. Parlerò di Xml Trust, un insieme di specifiche relative a servizi di cifratura, autenticazione ed integrità nello scambio di documenti Xml, e di come la crittografia, la firma e i certificati elettronici trovino nell' Xml un valido strumento applicativo. Se inquadriamo tutto ciò in un ambito giuridico e lo applichiamo al processo telematico, riusciremo ad avere una fedele fotografia degli scenari che si prospettano ai giuristi di oggi e di domani: mai come adesso la tecnologia informatica ha evidenziato i suoi punti deboli, ma nonostante ciò, la stessa ha mostrato la determinazione e la possibilità di rappresentare uno strumento sicuro ed affidabile. Dal

titanico scontro di queste due forti realtà, dipenderà la totale affermazione di un sistema informatico di trasmissione globale o meta-globale, applicato a tutte o quasi tutte le aree geografiche del nostro pianeta. È difficile immaginare che non si arrivi a questo importante traguardo.

Ma andiamo per ordine e facciamo un breve cenno su cosa è l'Xml, perchè firma elettronica e crittografia trovano in questo standard di sicurezza uno dei loro migliori alleati, e vediamo di capire perchè Xml Trust rappresenti il maggior momento evolutivo della sicurezza informatica, nonché come possa essere utile agli operatori del diritto all'interno del nuovo processo telematico alla luce delle più recenti disposizioni normative.

L'Xml (eXtensible markup language) è nato nel 1996 con lo scopo di consentire l'estensione dell'Html (Hypertext markup language). L'Xml è un meta linguaggio, ovvero uno strumento che consente di definire i linguaggi di segnatura e avente un'interessante qualità: può essere letto sia dall'uomo-utente, sia dai programmi. Il formato dell' Xml è testuale e ciò lo rende adatto alla memorizzazione a lunga scadenza. Essendo un meta linguaggio, esso non fa altro che contrassegnare le parti del testo con dei marcatori aventi lo scopo di definirne il contenuto. Ciò non significa che tali marcatori si occupino della visualizzazione finale del testo o della stampa (a differenza di quello che fa il meta linguaggio Html), essi hanno la sola funzione di definirne e specificarne i contenuti, cioè quello che è racchiuso all'interno del testo. In tema di informazioni sensibili e di privacy è immediatamente individuabile un grosso limite dell'Xml: esso mostra troppo in dettaglio le informazioni che vi sono descritte. I tag che compongono questo meta linguaggio infatti, descrivono sia la struttura del documento, sia l'essenza di ciascun elemento. Facile immaginare le conseguenze di una tale situazione. Si pensi ad eventuali atti segreti all'interno di un processo telematico o alla presenza all'interno di un documento di traffico sensibile (c.d. *mission critical*) o ai numeri delle carte di credito. Quale migliore occasione per un malfattore, un hacker o un semplice curioso, di impadronirsi di notizie riservate quali quelle di un processo, di informazioni aziendali o di informazioni riguardanti anche una semplice persona comune? Paradosslamente quello che dovrebbe essere alla base della potenza dell'Xml risulta essere all'improvviso un grosso limite funzionale. Sono le stesse informazioni contenute in un file Xml a richiamare l'attenzione su se stesse! Tutto ciò non è passato inosservato agli addetti ai lavori e sono state subito adottate politiche di cifratura per qualsiasi elemento e tag desiderato: far diventare un tag

anonimo ha consentito di rendere piuttosto complessa l'identificazione dei dati trasmessi. Facciamo un esempio: se un curioso sta cercando di individuare all'interno di un file Xml il tag che racchiude il numero di una carta di credito, utilizzerà una stringa di ricerca <cre, ma se i tag sono stati cifrati, tutto ciò non sarà assolutamente possibile. Ma non solo. Un altro importante aspetto legato alla sicurezza dei dati contenuti in un file Xml si evidenzia nella possibilità di criptare selettivamente, a differenza di un normale documento di testo, delle singole parti di un documento con caratteritiche di criptazione diverse e con firme elettroniche differenti. Se il documento è stato scritto a più mani ogni parte potrà essere firmata dalla persona che l'ha scritta, indipendentemente dall'altra.

Come abbiamo detto all'inizio, Xml Trust rappresenta il maggiore momento evolutivo della sicurezza informatica: è un insieme di specifiche relative a servizi di cifratura, autenticazione ed integrità nello scambio di documenti Xml. Esso è formato da cinque servizi: **Xml Signature, Xml Encryption, Xkms, Saml e WS-Security.**

XML Signature, è la tecnologia che permette di firmare documenti Xml o parti di essi, garantendone l'autenticità e l'integrità. Si ricorre alla tecnica della **Digital Signature** (firma digitale) per firmare un documento attraverso l'utilizzo di un algoritmo di crittografia a chiave pubblica. In particolare, la firma digitale viene creata utilizzando la chiave privata del soggetto che vuole inviare il documento. Questo garantisce l'identità della persona che ha firmato digitalmente il file Xml in quanto la firma stessa può essere decifrata solamente attraverso la sua chiave pubblica: questa modalità ci garantisce l'identità di chi ha firmato il documento. Per creare la firma digitale si ricorre alla cifratura, non del documento, bensì del suo **digest** (sintesi) o **hash**. Il digest è prodotto da un particolare algoritmo che ricevendo in input il documento, è in grado di produrne una sintesi, una sorta di "impronta" che ci permette di identificarlo con certezza. Possiamo così verificare l'integrità del documento inviato in quanto, un volta decodificata la digital signature, ci ritroviamo il digest del documento che è stato spedito: il confronto con il digest calcolato sul documento ricevuto, ci permette di stabilire se il documento inviato ha subito delle indebite modifiche o meno. Per completezza di informazione, è bene ricordare che esistono tre tipi di firme: *enveloped*, nel quale è l'elemento firmato a contenere la firma, *enveloping*, nel quale la firma ingloba l'elemento firmato e *detached*, nel quale l'elemento firmato è identificato in maniera univoca via Uri: questo significa che l'elemento firmato si trova al di fuori del documento Xml contenente la firma.

Parliamo adesso del secondo importante servizio di cifratura ed autenticazione che compone l'Xml Trust: l' **Xml Encryption**. Questa tecnologia permette all'utente di cifrare parti di un documento Xml utilizzando i più diffusi algoritmi di crittografia, sia a chiave simmetrica che a chiave pubblica (quest'ultimo detto anche sistema crittografico asimmetrico. Il concetto di crittografia a chiave pubblica fu introdotto nel 1976 da Whitfield Diffie e Martin Hellman). Utilizzando il sistema a chiave simmetrica la codifica del dato avviene attraverso l'utilizzo di un'unica chiave sia per la codifica sia per la decodifica. Diversamente, in un algoritmo a chiave pubblica abbiamo una coppia di chiavi: una pubblica, che può essere divulgata senza alcun problema, ed una privata che va tenuta segreta. Nessuna informazione segreta viaggerà dal mittente al ricevente: tutto ciò che che si deve fare per inviare a qualcuno un messaggio crittografato consisterà semplicemente nell'usare la sua chiave pubblica. In questo modo avremo la certezza che solo il ricevente potrà decodificare i dati visto che è l'unico a conoscenza della chiave privata.

Cosa possiamo fare nel caso in cui un documento non contenga un elemento Keyinfo (tag che contiene le informazioni sulla chiave pubblica di chi ha firmato il documento Xml ed il suo valore) o che compunque non siano presenti tutte le informazioni necessarie alla verifica della firma elettronica? In questo caso dovremo utilizzare il terzo elemento costituente l'Xml Trust. Il servizio in questione è l'**Xkms**, o **Xml Key Management Specification**.

Si è da più parti ritenuto che la sicurezza del canale trasmissivo raggiunta tramite una connessione HTTPS non sia più sufficiente per i documenti informatici in formato Xml che passano attraverso una serie di intermediari, ciascuno dei quali responsabili della firma, cifratura o validazione delle parti in causa. Al giorno d'oggi è necessaria una sicurezza a livello di singolo oggetto. Tutto questo richiede ovviamente più chiavi crittografiche, più catene di certificati e più persone che si occupino di far funzionare il tutto. Il W3C (Wide Web Consortium, consorzio volto a risolvere il problema più importante di Internet: la definizione di standard per lo sviluppo della rete) ha creato l'Xkms al fine di semplificare l'integrazione del Pki (Public Key Infrastructure) e la gestione in generale dei certificati elettronici. In dettaglio l'Xkms è un servizio che risiede su un servente esterno, generalmente gestito da un'autorità di certificazione, accessibile attraverso un semplice protocollo Xml. Esso è formato da due componenti: X-Kiss, o Xml Key Information Service Specification, e X-Krss (Xml Key Registration

Service Specification). La funzione del primo componente è quella di reperire tutte le informazioni di una determinata chiave pubblica al fine di verificare l'autenticità della firma o del certificato; X-Krss è finalizzato alla creazione, eliminazione o modifica di tali informazioni. Con X-Kiss, l'utente che riceve un messaggio cifrato, firmato elettronicamente o corredato di certificato digitale, delega quindi a un servizio in rete l'analisi e la verifica delle informazioni contenute nell'elemento. Con X-Krss, invece, si possono avere tre importanti servizi: *register*, *delete* e *recover*. Il primo serve a registrare una coppia di chiavi, una chiave pubblica e una privata, il secondo a revocarle e il terzo ad ottenere la chiave privata nel caso la si sia dimenticata. Per la realizzazione del terzo servizio è richiesto un meccanismo di autenticazione fuori rete, consistente nella trasmissione di un codice di autenticazione via posta o tramite linea telefonica.

All'interno dell'architettura Xml Trust troviamo il quarto servizio: **Saml**, ovvero il *Security Assertions Markup Language*. Quest'ultimo nasce dalla proposta di un altro gruppo di aziende e università fra cui Hewlett-Packard, Verisign (già presente nella proposta WS-Security), Tivoli e l'Università di Washington. Una delle migliori caratteristiche di questo nuovo linguaggio consiste nella possibilità di autenticare o garantire determinate informazioni relative a determinati soggeti o non. Un esempio potrebbe essere rappresentato da un'asserzione del tipo *«Io garantisco che il Signor Mario Rossi è un impiegato della mia azienda»*. Di facile intuizione l'utilità e la garanzie che si possono ottenere in tema di processo telematico: questo linguaggio è molto utile per le autenticazioni e le autorizzazioni.

Mentre Xml Signature, Xml Encryption e Xkms sono specifiche del W3C, **WS-Security** è una proposta congiunta di tre importanti aziende leader nel settore dell'informatica: Verisign, IBM e Microsoft ed è il quinto servizio costituente l'Xml Trust. WS-Security si basa sul protocollo Soap (uno standard W3C, che definisce le specifiche di packaging dei messaggi) e prevede un elemento apposito, per contenere tutte le informazioni relative alla sicurezza dei messaggi. Caratteristica principale di WS-Security è quella di affrontare il problema della protezione facendo ricorso a standard e a specifiche già esistenti.

Effettuata una breve panoramica su tutti gli elementi costituenti l'architettura dell'Xml trust, è giusto chiedersi cosa devono aspettarsi i giuristi di oggi e di domani da questa tecnologia informatica. Il livello di sicurezza garantitoci oggi dall'Xml Trust servirà al processo telematico? Penso proprio di sì. L'avere esaminato in maniera analitica le potenzialità di Xml Trust, ci induce a ritenere che i tempi per

prospettare una nuova era processual-informatica siano maturi. E' bene ricordare che il documento informatico sottoscritto con firma digitale ha acquistato efficacia probatoria pari a quella della scrittura privata ai sensi dell'art. 2702 c.c., solo con l'entrata in vigore della **L. 15 marzo 1997 n.59** e del **D.P.R. 10 novembre 1997 n. 513**. La principale innovazione di questa normativa consiste nel fatto che la trasmissione dei documenti con strumenti informatici può ora considerarsi valida ed efficace agli effetti di legge.

Parlare oggi di "processo telematico" non significa parlare di un nuovo processo o di nuove regole processuali: dobbiamo semplicemente rilevare una nuova possibilità offerta alle parti, al giudice ed alla cancelleria di formare, comunicare e notificare gli atti processuali mediante documenti informatici. Così, l'alternativa numero uno al sistema cartaceo all'interno di un processo diventa il sistema informatizzato e lo standard Xml non può che rappresentare il migliore strumento possibile in tema di sicurezza. A tal proposito occorre ricordare le disposizioni contenute nel **Regolamento 26.01.01**, applicabili ai giudizi iscritti al ruolo dopo il 1 gennaio 2002:

"*Tutti gli atti e i provvedimenti del processo possono essere compiuti come documenti informatici sottoscritti con firma digitale*" **(art.4)**.

Le applicazioni pratiche di tale regolamento consentiranno alla cancelleria di formare il fascicolo informatico inserendo nello stesso tutti gli atti e i documenti probatori inviati per via telematica dal difensore il quale, sempre con lo strumento informatico, invierà anche la procura alle liti "*asseverata come conforme all'originale mediante sottoscrizione con firma digitale*", nonché la nota di iscrizione al ruolo.

Pensiamo all'importanza di inserire all'interno del fascicolo atti e documenti probatori immuni da qualsiasi tentativo di modifica, alterazione o cancellazione. Servirsi di Xml Trust è attualmente la scelta obbligata: per la prima volta uno strumento informatico viene a porsi come strumento fondamentale ai fini dell'applicazione del principio della certezza del diritto. Si potrà così consultare per via telematica sia il fascicolo d'ufficio, sia quelli di parte con evidenti vantaggi di tempo e di energie.

L' Avvocato difensore (e non solo lui) dovrà dotarsi di alcune specifiche hardware e software: dovrà munirsi di un lettore di smart card in grado di effettuare la sottoscrizione tramite digital signature del

documento prodotto. Dovrà munirsi di un valido antivirus e di **un' applicazione che possa generare dall'elaboratore testi il documento Xml.**

Senza scendere nei dettagli di come si strutturerà il processo telematico (ricordiamo solo **il reg. n. 123 del 13. 02. 01** che disciplina, all'interno del processo civile e amministrativo, gli strumenti informatici e telematici individuandoli nella firma digitale e nel documento informatico), possiamo affermare, senza tema di smentita, come la sfida alla corruzione dei dati informatici abbia trovato nell' Xml Trust il maggiore baluardo in tema di sicurezza informatica, di servizi di cifratura, autenticazione ed integrità nello scambio di documenti Xml.

Per concludere, non potranno esistere più Avvocati, Giudici o Cancellieri incapaci di utilizzare uno strumento informatico: sarebbero tagliati fuori dal futuro mondo del diritto.

Dott. Luciano Fiore

Firmato digitalmente da
LUCIANO FIORE
CN = LUCIANO FIORE
C = IT