ABSTRACT

Navigare su internet è la cosa più semplice che esista basta avere un computer, un collegamento e si parte a **vele spiegate** nel web. Il web è costituito da molti elementi, che comprendono gli standard per i formati dei documenti (cioè, Html), i browser del Web (per esempio Firefox, Google Chrome, e Microsoft Internet Explorer), i server del Web (per esempio, i server Apache, Microsoft, e Netscape) e un protocollo dello strato dell'applicazione. Quest'ultimo varia a seconda della ricerca e delle informazioni che si scambiano, così nel momento in cui si cercano:

- cose semplici: come informazioni per preparare una cena thailandese o utilizzare al massimo un Tapis Roulant. Lo scambio di informazioni avviene attraverso un semplice protocollo di comunicazione (**HTTP** - *Hypertext Transfer Protocol*);
- cose difficili: come inserimento dei dati per un pagamento. Lo scambio di informazioni avviene con un protocollo che diventa un protocollo di sicurezza, che permette di proteggere i propri dati (**HTTPS** - *Hypertext Transfer Protocol Secure*).

HTTPS integra l'interazione del protocollo **HTTP** attraverso un meccanismo di crittografia. Per impostare un web server in modo che accetti connessioni di tipo **HTTPS**, l'amministratore di rete deve creare un certificato digitale ovvero un documento elettronico che associa l'identità di una persona ad una chiave pubblica.

I certificati si fondono su quattro concetti base:

- l'autenticazione;
- la privacy;
- l'integrità;
- il non ripudio.

Questi sono rilasciati dalle **Certification Authority** (**CA**) che oltre ad essere un'istituzione autonoma, deve:

- generare, trasmettere, conservare le chiavi in maniera sicura;
- pubblicare documenti necessari come ad esempio Certificate Policy, Certificate Practices Statement, Certificate Revocation List

Le **CA** per il ruolo che coprono sono sottoposti a controlli e ad una rigida regolamentazione e supervisione dello Stato di appartenenza. Inoltre:

- devono fare una valutazione dei rischi (Risk Assessment);
- devono sviluppare, implementare e gestire un Security Plan;
- devono documentare le procedure di Business Continuity e Disaster Recovery;
- devono proteggere la Private Key.

Attraverso la catena di certificazione la **ROOT CA** certifica quelle intermedie fino ad arrivare a quella finale. Da non trascurare il ruolo delle **Registration Authority** (**RA**) che ha il compito di identificare l'identità del soggetto richiedente tramite le verifiche dei dati che esso ha fornito.

Le **CA** possono rilasciare vari tipi di certificati:

- **DV** – Domain Validation;
- **OV** – Organization Validation;

- **EV** – Extended Validation.

L'ultimo è il più importante, è quello che dà il "semaforo verde" per rendere il sito affidabile. Infatti, quando la barra di navigazione del nostro Browser diventa verde è questo il segnale per una connessione sicura al sito Web.

GREEN BAR

Il Browser Web da banale strumento, diventa un importante alleato per avere informazioni sulla identificazione del sito; tramite il Browser Web si hanno i dettagli tecnici sui certificati e la loro identificazione.

All'interno di questo panorama il certificato **X.509** è quello che descrive e standardizza la struttura dei certificati dandone ad esempio:

- una versione, il numero di versione del certificato;
- un serial number che identifica in maniera univoca il certificato
- informazioni aggiuntive su chi ha chiesto il certificato

In conclusione, una volta verificato che il sito è certificato, possiamo navigare in maniera sicura? Dai test effettuati la risposta è "non sempre" perché se alcuni siti rispettano gli standard di sicurezza(ENEL, Regione Lazio), altri, pur risultando possessori di certificati, risultano vulnerabili ai più svariati attacchi(Comune di Roma, Comune di Pistoia). Se ciò non bastasse, negli ultimi tempi si sono sviluppate nuove tecniche come il **DNSSEC** (*Domain Name System Security Extensions*) per garantire sicurezza e affidabilità delle informazioni fornite dai sistemi **DNS** (*Domain Name System*).

Nonostante la tecnologia, è sempre l'utente a decidere se inserire o meno i propri dati; questo problema è noto come **EBKAC** (*Error Between Keyboard And Chair*).

.