

DOCUMENTO ELETTRONICO

Rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti

CRITTOGRAFIA

La crittografia, o cifratura, è la tecnica fondamentale per la generazione della firma digitale, e viene utilizzata per assicurare la riservatezza, l'autenticazione e il non ripudio delle informazioni archiviate o inviate attraverso reti di computer. Con la crittografia, un messaggio o, più in generale, un qualunque file di dati (testo, immagini, musica, ecc.) è trasformato in un insieme di segni e simboli assolutamente privi di significato per chi non conosca la "chiave" giusta per decifrarli. Il problema cruciale della crittografia è sempre stato la gestione della chiave. Anche il sistema di cifratura più sofisticato non serve a nulla se non si riesce a garantire la segretezza della chiave. Da questo punto di vista, si parla di due approcci principali alla crittografia: a chiave unica, detto anche a chiave privata o simmetrica; a doppia chiave, detto anche a chiave pubblica o asimmetrica

FIRMA DIGITALE

Equivalenti elettronico di una tradizionale firma apposta su carta. Facendo ricorso agli strumenti della moderna crittografia, attesta con certezza la paternità, la validità e l'integrità di un documento elettronico

SISTEMA DI VALIDAZIONE

Sistema informatico e crittografico in grado di generare e apporre la firma digitale o di verificarne la validità

CHIAVI ASIMMETRICHE

Coppia di chiavi crittografiche, una pubblica e una privata, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione

CHIAVE PRIVATA

Elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica

CHIAVE PUBBLICA

Elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi

CERTIFICATO

Insieme di informazioni utilizzato per distribuire in modo sicuro le chiavi pubbliche degli utenti. Un certificato definisce con certezza la CA che lo ha emesso nonché il periodo di tempo in cui deve essere utilizzato

CERTIFICAZIONE

Il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare, si identifica quest'ultimo, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato

ENTE CERTIFICATORE - CERTIFICATION AUTHORITY (CA) O CERTIFICATE ISSUER (CI)

Soggetto pubblico o privato che gode della fiducia di tutti gli utenti che operano nel sistema: effettua la certificazione, rilascia il certificato della chiave pubblica, lo inserisce in un archivio pubblico, pubblica e aggiorna gli elenchi dei certificati sospesi e revocati. La CA si avvale di altre entità chiamate Uffici di Registrazione (Registration Authority o RA) per garantire che l'utente richiedente un certificato sia esattamente quello riportato nel certificato

REGISTRO DELLE CHIAVI PUBBLICHE - DIRECTORY O REPOSITORY

Sistema informatico, eventualmente distribuito e normalmente gestito dalla CA, sul quale sono immagazzinati i certificati e altre informazioni correlate. Viene usato per la distribuzione di tali informazioni agli utenti

CENTRO DI REGISTRAZIONE - REGISTRATION AUTHORITY (RA)

Entità responsabile dell'identificazione e dell'autenticazione dei soggetti della certificazione, ma che non è una CA e, pertanto, non firma né emette certificati. La RA procede al riconoscimento delle persone che si recano fisicamente ai propri sportelli e ne raccoglie dati anagrafici, tipo di servizio, etc., comunicandoli in modalità protetta alla CA

TITOLARE - CERTIFICATE SUBJECT (CS)

Soggetto logico titolare di un certificato, ossia il legittimo possessore e utilizzatore della chiave privata associata alla chiave pubblica che compare nel certificato

UTENTE UTILIZZATORE - USER

Soggetto fisico che, tramite un software opportuno, utilizza i certificati emessi dalla CA: - quello di cui è titolare, per apporre firme digitali ai propri documenti o per portare in chiaro documenti crittografati a lui indirizzati; - quelli di altri utenti titolari, per verificare la firma digitale da essi apposta o per crittografare documenti a loro destinati. L'Utente potrebbe essere titolare di più certificati, emessi da diverse CA (così come ad esempio si può essere titolari di più carte di credito) oppure dalla medesima CA ma intestati a titolari differenti (ad esempio nel caso in cui il titolare indichi una funzione peculiare svolta dall'utente)

DISPOSITIVO DI FIRMA

E' uno dei possibili supporti di memorizzazione della chiave privata del titolare del certificato (protezione software/hardware con password stabilita dall'utente). Possibili supporti sono, ad esempio, una smart card, un dischetto (protezione software con password stabilita dall'utente), o un dispositivo hardware (protezione hardware con password digitata solo sulla tastiera del dispositivo)

CARTA A MICROPROCESSORE - SMART CARD

Una smart card ("carta intelligente") è essenzialmente un computer delle dimensioni di una carta di credito: incastonato nella plastica della tessera si trova un microprocessore dotato di memoria che può essere letta e, più importante, può essere scritta, nella quale è possibile memorizzare una quantità significativa di informazioni. Contraffare una smart card è estremamente difficile perché il circuito integrato è sepolto nella plastica. In più, il circuito integrato può essere programmato per generare le proprie password e codici, con sofisticate funzioni di crittografia

CERTIFICATE POLICY O POLICY

Definizione delle regole generali che indicano in che contesto, a che dominio e con quali modalità di servizio un certificato viene utilizzato. Tutte le regole di servizio vengono poi definite, nel dettaglio, dal documento di Certification Practice Statement (o CPS)

UID - IDENTIFICATORE UNIVOCO DEL DISPOSITIVO DI FIRMA

E' il codice associato univocamente al dispositivo di firma al momento della sua personalizzazione

MANUALE OPERATIVO - CERTIFICATION PRACTICE STATEMENT (CPS)

Descrizione dettagliata del modo in cui un Ente Certificatore (CA) implementa le procedure di gestione dei certificati. Durante la negoziazione di un certificato incrociato, le CA esaminano e confrontano vicendevolmente i propri CPS

CROSS-CERTIFICATION - ACCORDI DI CERTIFICAZIONE - CERTIFICAZIONE INCROCIATA

Certificazione esercitata tra CA che appartengono a domini diversi. In questo processo le CA si

certificano l'una con l'altra. Condizione necessaria affinché possa avvenire la cross-certification è che esse accettino le rispettive CPS

VALIDITA' DEL CERTIFICATO

Efficacia e opponibilità al titolare della chiave pubblica, dei dati contenuti nel certificato stesso

SOSPENSIONE DEL CERTIFICATO

Operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo

REVOCA DI UN CERTIFICATO

Operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi

ELENCO DEI CERTIFICATI REVOCATI - CERTIFICATE REVOCATION LIST (CRL)

Lista conseguente alle operazioni con cui la CA annulla la validità di un certificato da un dato momento, non retroattivo, in poi. Tale elenco è firmato digitalmente dalla CA, periodicamente aggiornato e pubblicato nella Directory.

LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

Protocollo utilizzato per accedere alla directory contenente i certificati ed effettuare tutte le operazioni di prelievo certificato, CRL, etc..

VALIDAZIONE TEMPORALE - TIME STAMPING

Il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili a terzi

ALGORITMO DI HASHING

Una firma digitale viene creata facendo passare un documento attraverso un particolare algoritmo, detto di hashing (spezzettamento): il codice prodotto dall'algoritmo, una sorta di "impronta" del documento, viene poi criptato usando la chiave privata di chi spedisce il messaggio. Si tratta di un algoritmo che partendo da un documento di qualsiasi dimensione lo elabora e produce un codice di dimensione fissa. Il metodo di elaborazione è tale che, se il documento venisse cambiato in qualunque sua parte, questo codice cambierebbe. Per esemplificare immaginiamo un algoritmo che calcola il numero di lettere, il numero di parole, la frequenza di ogni lettera ecc., se cambia una qualsiasi lettera o parola anche il risultato cambia. Dall'impronta non è possibile risalire al documento, però se il documento cambia, anche solo in minima parte, allora cambia anche l'impronta

X509

Standard che definisce il formato dei certificati digitali utilizzato per la gestione delle chiavi pubbliche degli utenti. Esso è composto da una serie di informazioni organizzate in campi che specificano: numero del certificato, la Certification Authority (CA) emittente, il nome dell'utente certificato, la sua chiave pubblica, il periodo di validità del certificato, estensioni pubbliche o private. Queste ultime informazioni rappresentano dei campi aggiuntivi e proprietari del certificato

IETF - INTERNET ENGINEERING TASK FORCE

IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori, e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet. E' aperta a chiunque sia interessato

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

Abbreviazione di International Organization for Standardization (Associazione Internazionale per la Standardizzazione). Non è che l'ISO non sia un acronimo; al contrario, il nome deriva dalla parola greca iso, che significa uguale. Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione provenienti da più di 75 paesi. Ad esempio, l'ANSI (American National Standards Institute) è un membro ISO. L'ISO

ha definito numerosi ed importanti standard per i computer. Di questi, il più significativo è forse l'OSI (Open Systems Interconnection), un'architettura standard per progettare le reti

ITU - INTERNATIONAL TELECOMMUNICATION UNION

Acronimo di International Telecommunication Union (Unione Internazionale per le Telecomunicazioni), un organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni. In precedenza, le attività di standardizzazione venivano effettuate da un gruppo interno all'ITU chiamato CCITT, ma dopo la riorganizzazione del 1992 il CCITT come corpo separato non esiste più

RRC - CODICE DI REVOCA - REVOCATION REQUEST CODE

Codice preimbastato Consegnato dalla RA all'utente titolare per l'autenticazione della richiesta di revoca di un certificato

PKI - INFRASTRUTTURA DI CHIAVE PUBBLICA - PUBLIC KEY INFRASTRUCTURE

Una PKI è un insieme di servizi che gestiscono applicazioni utilizzando tecniche crittografiche in chiave pubblica. Tali servizi includono: generazione e distribuzione chiavi, certification authority, certificate directory, certificate revocation lists (CRL), key escrow, document escrow, servizi che richiedono non-ripudiabilità. Le funzioni crittografiche gestite da una PKI includono: riservatezza (crittografia), autorizzazione (firma digitale), autenticazione e identificazione, non-ripudiabilità e integrità dei dati (firma digitale e autenticazione dei messaggi)