Lezione 12 modulo 2

Abbiamo parlato nei moduli precedenti di chiavi, chiavi che possono essere segrete, chiavi pubbliche, chiavi private nella cifratura asimmetrica... In questo modulo parliamo della gestione delle chiavi. Innanzitutto vanno distinte le due fasi: quelle della 'generazione delle chiavi' e poi abbiamo la tematica relativa alla 'conservazione delle chiavi'. Nella generazione delle chiavi in genere abbiamo una generazione che è basata su una generazione di numeri casuali, 'Random Number Generation', quindi una chiave sarà tanto migliore quanto effettivamente casuale la generazione della chiave, quindi non può essere replicata l'operazione di generazione avendo informazioni sulla modalità di generazione. L'aspetto importante però sulle chiavi, abbiamo detto, è quello della conservazione: la conservazione delle chiavi in generale si può effettuare con modalità diverse, potranno essere conservate a livello software, ad esempio all'interno di file cifrati, oppure a livello hardware e quindi su dispositivi dedicati proprio alla gestione delle chiavi, dal punto di vista appunto della loro conservazione, ma possono essere anche dispositivi attivi in grado di fare anche operazioni crittografiche, quindi non hanno solo la funzione di memorizzare la chiave, ma anche possono fare le operazioni di cifratura. Questi tipicamente sono, ad esempio, le 'smart cards', che possono essere utilizzate come dispositivo fisico che viene consegnato poi a chi utilizzerà una certa chiave. Un altro aspetto che caratterizza la gestione delle chiavi è che le chiavi devono essere scambiate. Ovviamente questo sarà diverso a seconda che la nostra cifratura sia simmetrica, in cui usiamo la stessa chiave per cifrare e decifrare, e il caso in cui sia asimmetrica, in cui la chiave privata non viene scambiata, rimane conservata dal proprietario della chiave, mentre invece la chiave pubblica è pubblica, quindi l'obiettivo è quello di renderla disponibile a chi la potrà utilizzare. Vediamo come possono essere, appunto, quindi scambiate le chiavi nel caso di cifratura simmetrica: quindi sono le chiavi segrete. Un primo aspetto da considerare è il canale che viene utilizzato per scambiare la chiave. Ovviamente se trasmetto sullo stesso canale i messaggi cifrati e anche la chiave, questo può rappresentare un pericolo per quanto riguarda la sicurezza, quindi quello che normalmente viene fatto è utilizzare un canale alternativo e si parla di 'out of band' come tecnica di distribuzione delle chiavi, quindi utilizzando canali alternativi per la distribuzione. Un'altra possibilità è quella di cifrare la chiave simmetrica con una cifratura asimmetrica, utilizzandola in modo che garantisca la riservatezza della chiave quindi possa essere letta solo dal destinatario. Possono esserci anche dei centri di distribuzione delle chiavi o 'Key Distribution Center', che distribuiscono le chiavi ai destinatari e quindi garantiscano che effettivamente la chiave venga data solo a chi ne debba entrare in possesso. Questo quando l'obiettivo è quello di mantenere la chiave segreta. Quando abbiamo una cifratura asimmetrica, quello che viene distribuito è la chiave pubblica; per definizione, non abbiamo problemi di riservatezza ma quello che è importante in questo caso è di garantire la validità della chiave, quindi questa garanzia di validità dovrà essere gestita in modo da essere sicuri che la chiave effettivamente appartenga a un certo agente che sia ancora valida quindi non sia stata invalidata successivamente. Questo richiede un' infrastruttura di gestione della chiave, che chiameremo 'Public Key Infrastructure', o più brevemente 'PKI', che andremo a descrivere per illustrare i vari aspetti che sono collegati appunto a questa garanzia di validità. Vediamo uno schema; uno schema generale può essere questo: innanzitutto quello che è importante quando parliamo di chiavi è la necessità di avere una autorità di certificazione, quindi qualcuno che mi garantisca che effettivamente una certa chiave venga associata a un certo agente, questo verrà fatto pubblicando dei certificati a chiave pubblica, cui scopo è proprio quello di assicurare che la chiave sia appartenente a un certo agente. Quindi l'autorità di certificazione, se la firma deve avere un valore legale, sarà un'autorità che sarà stata riconosciuta legalmente e quindi in Italia ad esempio può essere qualche ente, come le poste, oppure le camere di commercio, che sono inserite in una lista che è stata ufficialmente approvata e quindi portare a dei documenti che possano avere valore legale. Però questa associazione fra un nome di un agente e la chiave pubblica che è all'interno di un certificato non è sufficiente per quanto riguarda tutte le garanzie che vogliamo dare in questi casi. Innanzitutto abbiamo detto che gli agenti corrisponderanno con delle persone fisiche, oppure possono essere anche delle persone giuridiche, quello

che sarà importante è riconoscere che effettivamente la chiave privata che viene associata alla chiave pubblica, sia in possesso a un utente che sia un utente che sia stato legalmente riconosciuto. Per fare questo ci servirà una cosiddetta 'autorità di registrazione', che può essere uno sportello che va a verificare che un certo utente sia effettivamente chi dichiarerà di essere, quindi quello che verrà dichiarato all'interno del certificato. Quindi abbiamo una tematica di identificazione degli utenti. Gli utenti tipicamente chiederanno un certificato all'autorità di certificazione e si registreranno, verranno riconosciuti dalla autorità di registrazione a uno sportello. Come vedete in questo schema, non è detto che le due autorità corrispondano allo stesso ente e quindi potranno essere enti diversi e l'autorità di registrazione garantirà per l'identità di un certo utente e questa garanzia verrà utilizzata dall' autorità di certificazione. Un altro aspetto che è importante è quello della 'validità del certificato', quindi questo documento che è certificato che dà la garanzia sulla chiave pubblica associato a un certo utente potrà avere una sua validità, quindi scadere, quindi un tempo di durata, può essere un anno o due anni, ma l'altra cosa importante è che sia possibile anche revocare questi certificati ad esempio quando la chiave privata dell'utente viene rubata o viene persa da parte dell'utente. E quindi, analogamente a quello che viene fatto ad esempio per le paccate di pagamento sarà necessario che l'utente possa avere la possibilità di chiedere la revoca di un certificato, questo verrà fatto tipicamente rivolgendosi a un altro ente, che sarà in grado di gestire queste richieste tipicamente al di fuori anche di orari di apertura, ad esempio degli sportelli tipici dell'autorità di registrazione di certificazione e che riceverà queste richieste e predisporrà appunto la revoca che avrà una certa data di revoca. Questo però richiede il fatto che ci sia effettivamente una pubblicazione di queste informazioni, quindi quello che vediamo anche qua nello schema è quello che viene chiamato un 'Repository' dei certificati. Questi certificati quindi saranno pubblicati da parte dell'autorità di certificazione anche inserendoli all'interno di un repository, sarà associata ad essi una data di validità e l'autorità di revoca potrà pubblicare la revoca, appunto, del certificato e quindi cambiare uno stato di un certificato da valido a non valido. Quindi, ritornando al discorso che avevamo già fatto sulla verifica della firma digitale, quando io vado a verificare una firma digitale, oltre a verificare che l' impronta generata abbia le caratteristiche corrette, dovrò anche andare a verificare che il certificato a chiave pubblica abbia ancora validità per poter garantire che la firma sia effettivamente una firma valida. Vediamo adesso qual è la struttura di un certificato: tipicamente i certificati vengono redatti seguendo uno standard, lo standard tipico è l'X.509' dell' ITU e vediamo qua alcuni campi che sono quelli significativi; innanzitutto un certificato è un documento ed è un documento firmato, quindi abbiamo le due parti tipiche del documento firmato: il contenuto del documento nella prima parte e poi la firma che è la firma apposta dalla autorità di certificazione che viene generata sulla base, come al solito, del contenuto del documento e della chiave privata associata all'autorità di certificazione. Il documento avrà come informazione principale che rappresenta lo scopo di questo documento, le informazioni relative a chi è il soggetto che viene considerato, e quindi avremo un'identificazione al soggetto e poi l'informazione che la chiave pubblica sarà una sequenza di bit, avremo anche associato tipicamente quali sono i parametri e anche gli algoritmi che vengono utilizzati per utilizzare questa firma, ad esempio l'RSA per la crittografia asimmetrica per la cifratura e decifratura e la lunghezza della chiave di 1024 bit. Un altro aspetto importante è anche definire qual è l'algoritmo hash e quindi noi avremo la definizione appunto anche dell'algoritmo di hash che viene utilizzato nella fase di firma. Abbiamo detto che qui avremo tipicamente anche altre informazioni che sono informazioni legate alla validità di un documento, ad esempio qua vediamo un documento che ha una validità lunga, ad esempio con la scadenza nel 2020 da inizio validità nel 2006, di solito documenti di questo tipo hanno una validità più breve, ma questo è quello che descrive la durata prevista della validità del documento. Ricordo che per verificare che effettivamente una certa chiave pubblica sia valida, noi non potremo solo andare a vedere la durata dichiarata, dovremo anche andare a verificare che il certificato non sia stato revocato nel frattempo e quindi lo stato del certificato nel repository che viene gestito nella PKI dell'autorità di certificazione che ha firmato questo certificato. Finiamo con due parole sull'utilizzo delle chiavi pubbliche: ovviamente abbiamo detto che servono a firmare documenti. Se l'autorità di certificazione è ufficialmente riconosciuta, i documenti avranno anche una validità di tipo legale. Ma l'uso

della chiave pubblica è molto diffuso in realtà in molti ambiti di comunicazione su base informatica, ad esempio possiamo affermare i messaggi di posta elettronica, possiamo utilizzare meccanismi basati su chiavi pubbliche anche per l'autenticazione del server o in generale nei canali di comunicazione, ad esempio per poter cifrare delle chiavi segrete che servono per degli scambi all'interno dei protocolli di comunicazione che vogliono garantire la proprietà di sicurezza sulle informazioni che vengono trasmesse. Un altro uso delle chiavi pubbliche nelle applicazioni informatiche sono, faccio solo un esempio: l' e-commerce, in cui vogliamo garantire l'identità dell'interlocutore, quindi l'utilizzo di chiavi pubbliche mi dà garanzie appunto di identificazione di quello che è il mittente che mi manda una certa informazione. Un altro uso piuttosto diffuso è quello della firma del software: anche in questo caso per dare garanzie su quella che è l'origine di un certo modulo software, che essendo anch'esso una sequenza di bit come tutti i documenti all'interno di sistema informatico, può essere alterato con l'inserimento ad esempio di codice malevolo, quindi la firma mi dà delle garanzie di autenticità di un certo software e quindi posso andare a verificarla con i meccanismi di verifica della firma che abbiamo già discusso.