PKI

Public key infrastructure

Una Public Key Infrastructure (PKI) è una serie di accordi, che consentono a terze parte fidate di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica a un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi.
Le chiavi pubbliche tipicamente assumono la forma di certificati digitali.
Il termine PKI viene usato per indicare sia l'autorità di certificazione e i relativi accordi, sia, in senso più esteso, l'uso di algoritmi crittografici a chiave pubblica nelle comunicazioni elettroniche.
L'uso del termine nell'ultimo senso è errato in quanto una PKI non necessariamente richiede l'uso di algoritmi a chiave pubblica.
Gli accordi alla base di una PKI consentono agli utenti di essere mutualmente autenticati, e di utilizzare le informazioni contenute nei rispettivi certificati per cifrare e decifrare i messaggi in transito.
In generale una PKI consiste di software client, software server (p.e. un'autorità di certificazione), hardware (p.e. smart card) e procedure operative.
Un utente potrebbe firmare i propri messaggi con la sua chiave privata, e un altro utente controllare questa firma usando la chiave pubblica contenuta nel certificato del mittente, fornito dall'autorità di certificazione facente parte della PKI.
Questo consente a due (o più) parti desiderose di comunicare di verificare la confidenzialità, l'integrità dei messaggi e l'autenticazione degli utenti senza il bisogno di un precedente scambio di informazioni segrete.
La maggior parte delle PKI al livello delle imprese fanno affidamento su catene di certificati per stabilire l'identità delle parti: un certificato viene emesso da un'autorità di certificazione, a sua volta autenticata da un certificato emesso da un'autorità di livello più alto, e così via.
In questo modo si stabilisce una gerarchia di certificati, composta da computer, organizzazioni e pacchetti software diversi.
Gli standard sono fondamentali per il funzionamento di una PKI, e gli standard pubblici sono fondamentali per le PKI di uso esteso.
Molti degli standard nel campo delle PKI sono opera del gruppo di lavoro PKIX della IETF.
Le PKI a livello di impresa sono spesso strettamente legate ai servizi di directory dell'azienda, in cui la chiave pubblica di ogni dipendente può essere memorizzata (incorporata in un certificato) assieme ad altri dettagli personali (numero di telefono, indirizzo e-mail, dipartimento...).
Oggi la principale tecnologia per i sistemi di directory è LDAP e infatti il più comune formato usato per i certificati (X.509) nasce con il predecessore di LDAP, lo standard X.500.