Fact Sheet

Cogito Group

Public Key Infrastructure

What Is PKI?

Public Key Infrastructure (PKI) is the combination of hardware, software, policies, standards, procedures, and people needed to create, manage, store and distribute digital credentials such as keys and certificates. PKI allows the delivery of security and confidentiality services to electronic businesses solutions. It is an enabling technology that allows other solutions to provide the tangible outcome or benefit. PKI provides, along with a Corporate Directory, the building blocks to allow other solutions to be realised, not the end solution itself.

What Can It Do?

In the physical world we use hand-written signatures, sealed envelopes, photo identification, and established trust relationships as protection measures against fraud.

Authentication

Ensuring that users are who they claim they are allows resource access control decisions to be made. PKI provides identification and authentication through digital signature of a challenge. If the sender of the challenge can verify using the certificate that the challenge was signed by the holder of the private key corresponding to the public key in the certificate, then the sender knows that the entity at the other end of the transaction is the entity named in the certificate.

Confidentiality

Encoding the information into a format which is incomprehensible to the attackers allows PKI to provide confidentiality through encryption. If the public key in a certificate is used to encrypt information, only the entity named in the certificate can decrypt that information. PKI can be used for both encryption in transit and for encryption at rest.

Data Integrity

Ensuring that the information cannot be changed without detection. PKI provides data integrity through digital signature of information. If the recipient of digitally signed information can verify the signature on the information, then the recipient knows that the content has not changed since it was signed.

Non-repudiation

Prevents users from denying involvement in an electronic transaction PKI assists with technical nonrepudiation through digital signatures. If information has been digitally signed, only the entity named in the certificate had access to the private key used to sign the information and can therefore be assumed to some level of assurance to have been the entity that generated the information. PKI provides a trusted identity management infrastructure through software and hardware to bind keys for encrypting and decrypting messages and the associated user's identity, ensuring they are authentic via a Certification Authority.

Organisational Benefits

Some of the key areas where PKI would aid an organisation to better realise capabilities deriving from information technology are:

- Providing encryption and authentication for internal and external web pages such as internet banking.
- Logical access control by provide logon using strong authentication.
- Allowing single sign on to resources.
- Authentication to different environments (e.g. Windows to Unix).
- External access to corporate network services.
- Remote secure administration of ICT assets.
- Virtual Private Networks.
- Remote access for mobile devices.
- Timestamp Services.
- Identity Management.
- Physical Access to facilities and equipment.

Examples of PKI In Use Today

There are many examples of organisations using PKI. Two large commercial examples are Microsoft and Lockheed Martin. Australian government examples are Department of Defence, Department of Human Services, and the Australian Taxation Office.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.