Cogito Group

PKI: Overview

What is PKI?

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

PKI is an enabler technology that allows other solutions to provide the tangible outcome or benefit.

What can it do?

In the real world physical documents, hand-written signatures, sealed envelopes, photo identification and established trust relationships are protection measures against fraud.

PKI translates the trust conventions of the physical marketplace and makes them work online by offering the following features:

Authentication: Ensuring that users are who they claim they are, which 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

PKI provides 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 the 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. 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.

Benefits to your organisations

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

- Provide encryption and authentication for internal and external web pages (internet banking is an example of this)
- Logical access control by provide logon using strong authentication (smart card logon)
- Allowing single sign on to resources
- Authentication to different environments (e.g. Windows to Unix)
- External access to corporate network services
- Messaging solutions (such as email) for encryption and message integrity
- Code Signing
- Document signing of forms and formal correspondence
- Transaction Signing of critical services such as Databases and of financial transactions
- Resource Communications validation and/or encryption between devices
- Encrypted File System
- Secure File Transfer
- Remote secure administration of ICT assets
- Virtual Private Network
- Remote access for mobile devices
- Timestamp Services
- Identity Management
- Physical Access to facilities and equipment

Some examples 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.

2017 iAWARDS
Australian Capital Territory iAward Winner

54th Australian Export Awards
2016 NATIONAL FINALIST