Cogito Group

All of Government PKI

What is a PKI?

Public Key Infrastructure (PKI) is a system of cryptographic technologies, standards, management processes and controls governing the use of digital certificates. It is an enabling technology. This means it enables users of an insecure public network (such as the internet) to securely and privately exchange data through the use of a public/private cryptographic key pair that is obtained and shared through a trusted authority

The Business Need: Establishing Trust

High assurance cyber security solutions, like a PKI, are necessary to establish a hierarchal chain of trust to certify users and devices.

Cogito Group were selected by the Department of Internal Affairs to run their All of Government (AoG) Root CA and the GNet policy CA for the New Zealand Government.

This would assist New Zealand government agencies improve security by guaranteeing high assurance on critical systems.

Our client wanted an All of Government PKI provided as a Service.

Digital Certificate Classes:

- Government to Government (G2G) digital certificates
- Business to Government (B2G) digital certificates

The Challenge

Design a trustworthy and resilient PKI taking into account the security challenges that mobile, cloud computing and Internet connected devices bring.

The PKI was expected to support a large number of users, devices, software applications, business systems and organisations acting for or on behalf of the New Zealand (NZ) Government across complex eco systems.

To provide this service, it was critical data remained in country and services were provided by security cleared citizens. Cogito also built the backend product, Jellyfish to support the service.

Factors that were considered:

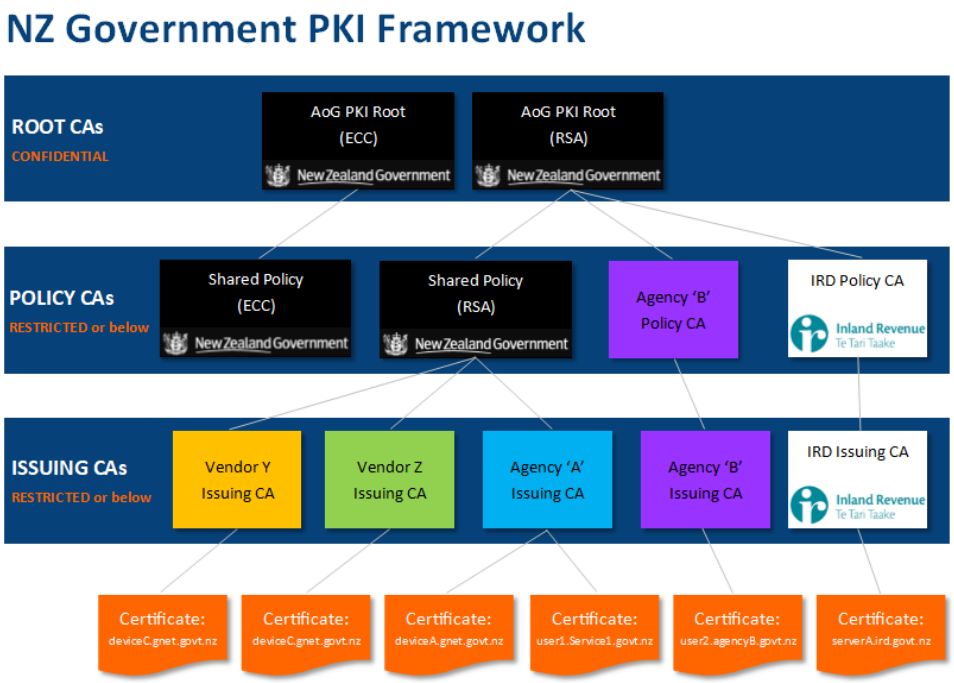
- Harden the CA to meet the evolving security needs of the organisation
- The volume of certificates issued by the CA
- The number of applications to be supported

- Compliance & auditing requirements
- Evolving requirements of the agency
- Geography and topology
- Existing cryptographic policies and legacy systems

NIST SP800-32 PKI Definition: "A public key infrastructure (PKI) binds public keys to entities, enables other entities to verify public key bindings, and provides the services needed for ongoing management of keys in a distributed system"

The Solution

- ✓ Cogito implemented the Jellyfish solution as the back-end solution
- ✓ A dedicated Hardware Security Module (HSM)
- ✓ Developed policies on access controls, separation of duties, key lengths and auditing mechanisms to mitigate risks
- ✓ Developed Certificate Policy and Key Management Plan
- ✓ Architecturally, the solution was developed using a distributed certificate revocation capability to ensure no single point of failure.



The Benefits

The benefits of a PKI are numerous as it provides a foundation for confidentiality, data integrity, authentication and non-repudiation. It's what we call enabling technology. PKI use cases include:

- **Wi-Fi Authentication** – multi-tenanted government office accommodation environments
- **Voice and video conferencing** – GNet secure voice and video transport (DTLS/SRTP)
- **User Authentication** – especially where high assurance and non-repudiation is required. Protocols such as SAML, OATH and others based on X.509 certificates can be used for Single Sign-On (SSO) over GNet and mutual authentication of both users and devices.
- **End User Device / Organisational / Hardware Authentication**
- **Line of Business System/Application Authentication and Verification**
- **Signature Verification** – for agency systems, online forms signing for users
- **PKI Managed Service** – Use of the TaaS Catalogue construct allows most agency-managed PKI environments and system requirements to be met through a 'PKI as a Service' like catalogue of selectable services.
- **Communities of Interest (CoI)** – Enabling creation of CoIs by adding registered endpoints to a group using a shared key, which means CoIs can be created very quickly and cheaply on an ad-hoc basis. GNet is an example of a permanent, large scale, CoI.

The PKI implementation played a major part in satisfying these requirements:

Non-Repudiation: The PKI offers evidence – verifiable by a third party – that a transaction has been sent or authorized by the purported sender. PKI uses digital signatures to bind the identity of a party to the transaction so that knowledge of the transaction cannot later be denied.

Authentication: The PKI offers authentication, that is, the process of testing or verifying an assertion of identity, in order to establish a reliable level of confidence in those assertions.

Integrity: PKI offers integrity through digital signatures, which are used to prove that data has not been altered in transit – effectively preventing malicious third parties from tampering with messages. This is important in its own right, but also for non-repudiation.

Confidentiality: PKI offers confidentiality, that is, it allows selected users to confidentially exchange sensitive information. Recipient-targeted encryption ensures that only the intended recipients of a message will be able to decrypt and read the message.

About Cogito Group

Cogito Group is an award winning Australian owned and operated ICT company that specialise 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 insider