Case Study

Cogito Group

Protecting New Zealand's ePassports

The Client Need

New Zealand is a founding member of the International Civil Aviation Authority Public Key Directory (ICAO PKD) therefore it is essential for the New Zealand government – through the Department of Internal Affairs (the client) – to issue ePassports in compliance with standards set by ICAO. To satisfy necessity, the client required a high assurance cyber security solution to establish a hierarchal chain of trust to certify ePassports users.

The Challenge

The ePassport validation process determines the authenticity and integrity of an ePassport by verifying the digital signature on the passport's chip. To carry out this validation process, a secure environment must be created within the ePassport system.

The Solution

Cogito Group deployed Jellyfish in an as a Service Public Key Infrastructure (PKI) offering for the client. Jellyfish's PKI service adds a layer of security to traditional non-electronic passports by embedding an electronic chip in the passport booklet that stores the biographical information visible on page 2 of the passport, as well as digital security features. These digital security features include a New Zealand specific "digital signature." These digital signatures are unique to each country and can be authenticated and verified using their respective certificates.

Jellyfish establishes a hierarchal chain of trust to certify users and devices. Together, the signature and certificates form a trust chain wherein one end is securely anchored in the authority of the issuing State and the other end is securely stored in the chip of the ePassport as the Document Security Object.

The chip within the ePassport is the secure environment within the system which provides digital signatures to ePassports. Therefore, Cogito Group's Jellyfish solution addresses the client's need and challenge. Concurrently, the Jellyfish PKI solution adheres to the ICAO security standards, as the service enables secure interagency collaboration by providing trusted identity, authentication, and authorisation mechanisms. Cogito Group's Jellyfish PKI service further enable inter-agency trust through the provision of credentials and digital signatures.

Protecting New Zealand's ePassports

Case Study

Outcome

By adhering to the ICAO security standards, New Zealand now confirms to borders and customs the authenticity of its passports. Deploying ePassports was a complex 15-month long project, which dealt with both New Zealand Government agencies and major international service providers. At present, there are more than 100 States, including Australia and New Zealand and non-state entities (like the United Nations) currently issuing ePassports, and over 490 million ePassports in circulation. We are proud our joint Australian and New Zealand team-developed cyber security solution, Jellyfish, is being utilised here.

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.