Fact Sheet

Cogito Group

Public Key Enabling

Introduction to Public Key Enabling

Public Key Enabling (PKE) is a term used to describe the process of changing systems to utilise Public Key Infrastructure (PKI). In some security conscious organisations such as the United States Department of Defence and Microsoft, PKI is heavily leveraged to provide many business and security benefits. In most organisations however, PKI is often a severely underutilised capability within their IT landscape. Digital information and electronic transactions have removed almost all paper-based processes, exposing the enterprise to attacks or accidents on critical business information and assets.

Organisations taking steps to add PKI often do so to meet a point need such as adding HTTPS security to internal websites. PKI, however, can provide much higher value to the business than most organisations realise. Where the investment in PKI has already been made, additional major capability and security benefits can be realised for almost no capital or ongoing costs.

PKE allows for the "four pillars of PKI" to be added as a feature to every PKE-capable service. The four pillars are:

- **Authentication:** the ability for a user or computer to identify itself to systems securely.
- **Integrity:** the ability to protect data from alteration, either maliciously or accidentally.
- **Confidentiality:** the ability to make sure data is private, that only the authorised people can view it, and that no eavesdroppers can read data as it moves through the network.
- **Non-repudiation:** the ability to ensure that a signed transaction cannot be repudiated after the fact, a key feature of binding agreements.

Most PKE scenarios are not difficult to implement, but they do require some analysis and planning to ensure that solutions are built to be more efficient, more cost-effective, and more secure.

Jellyfish and PKE

While an internal PKI can be used to protect internal websites, a globally trusted solution is required to protect external websites, otherwise warnings and errors will be shown to your users. While these certificates can be purchased from a number of providers, Cogito Group's Jellyfish solution allows for automated generation of these externally trusted certificates automatically using Let's Encrypt.

Public Key Enabling

Fact Sheet

Let's Encrypt is a free and open PKI designed to enable fast and easy HTTPS capabilities for the internet. Cogito Group provide the ability to request certificates from the service through Jellyfish, so you can still track and report on the use of these certificates within the Enterprise and maintain complete control over your PKI utilisation.

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.