

Certificate Management

What is Certificate Management?

Digital certificate management allows the verification of the identity of machines. In machine identity protection, digital certificates allow for encrypted data to be safeguarded between systems. The most widely used standard for digital certificates is X.509.

Vulnerable certificates represent a significant threat to your network. As the Internet of Things and our technological ecosystem become more complex, more and more certificates are produced, becoming integral to the safety of our daily activities. From banking and shopping, to business as usual operations.

A centralised Digital Certificate Management system like Cogito Group's 'Jellyfish' automates the detection of expired or vulnerable certificates within your network, allowing full lifecycle management of all existing certificates, no matter the CA.

Business Challenges

Vulnerable certificates leave organisational networks with insecurities that can be exploited by hackers and other malicious actors. With more certificates than ever before now present across organisations, digital certificates can no longer be managed by methods such as spreadsheets.

This takes too long, and leaves room for human error. A holistic and automated view of all certificates currently operating within a network ecosystem is needed to properly manage and identify vulnerable, expired, and soon to expire certificates.

Platforms such as 'Jellyfish', which provide insight into such certificate revocations, soon-to-expire certificates and certificates outside of the central network, reduce the strain on information technology officers and mitigate the risks of vulnerable certificates.

The Costs Associated with Certificate Outages

Organisations cannot afford the repercussions associated with certificate outages. Outages damage organisational reputations, affect customer trust, and cause enormous financial losses.

Capabilities

Our 'Jellyfish' solution offers, as part of its Credential Management / Managed PKI Service, the ability to manage certificates issued from disparate Certificate Authorities. This management capability includes:

- Number of certificates issued.
- Certificates expiring.
- Certificates issued to domains outside of central network.
- View who or what the certificate was issued to.
- Request certificates.
- Manage approvals.
- View revocations.

We manage certification from disparate CAs through a single pane of glass and bring under management those certificates that previously were not, i.e. certificates not issued by managed CAs.

What are the Benefits?

The benefits associated with the management of an organisation's certificates include:

- Automated management.
- Improves governance and compliance.
- Conformance to ISO and other standards by providing additional layer of security.
- Process control for on-boarding and off-boarding.
- Reduced strain on IT staff responsible for certificate management.
- Faster risk detection.

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.