Case Study

Cogito Group

Integrated PKI and CMS

The Client Need

Our client wanted to address the issue of many stove-piped security systems that didn't talk to one another, specifically in regard to its Public Key Infrastructure (PKI) and Card Management Solution. The goal was to develop linkages and workflows to centrally manage all of their security platforms in one place.

Specifically:

- Provide a holistic view of connected security systems.
- Search across multiple CA's (and CA vendors).
- Each CA has its own interface to request certificates.
- Register soft certificates in an anonymous portal.
- Registration from CMS portal.

The Challenge

The Challenge faced was separate and disparate interfaces, including legacy systems that were never designed to talk to other systems. These included:

- Multiple Web RA interfaces.
- Multiple Web Hander interfaces.
- CMS registration portal.
- Card Management System (CMS) interface.
- Directory Interface.

The Solution

Cogito Group implemented the Jellyfish solution to connect disparate systems. Jellyfish has been designed to significantly improve the way identity, credentials, access, and other security products are managed by developing a series of connectors (Cognectors).

These connectors enable the creation of automatic workflows, pass data through disparate systems and use triggers on one platform (example PACS) to affect another (example LACS). The Cognectors feed data from disparate systems into the Service Bus. This enables a number of benefits including enhanced monitoring and reporting of activity.

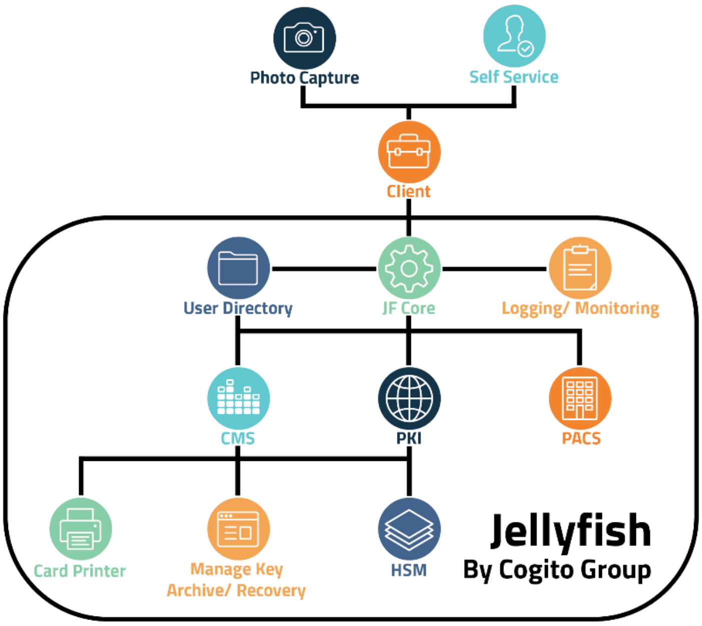

Figure 1: Jellyfish Cognectors

The Benefits

- Over 10 million certificates issued to date.
- Connected the trust platforms with partners and other Government agencies.
- Allow for trusted information sharing and security.
- Rollout of 125,000 hard tokens to improve security of logical and physical access.
- Cost savings achieved in printing consumables.
- Ensures the security of printed documents.

This gave the client:

- Streamlined and improved reporting within the PKI environment.
- Visibility of issued certificates, including expiry, issuer, and type.
- Ability to issue certificate types such as SSL and Virtual Smartcard without additional cost.
- Enhanced access control on the user interface.
- Integrated user self service capability.
- Ability to interact with any corporate directory solution allowing the addition or removal of Roles, Groups and Organisational Units (OU).
- A full IdAM capability without the limitation of some solutions that limit the unique Identity of the Common Name (CN) to a single value attribute where it is used as a multi-attribute field.
- Ability for certification requirements to be met by reporting the issuance of non-standard domain certificates.
- Enhanced features including:
  - Create Update Delete (CRUD) into LACS.
  - CRUD for integrated PACS solutions.
- Support ticketing from the interface.

The Software Solution: Jellyfish

Jellyfish has a highly scalable, modular, easy to deploy architecture that includes:

- Credential management services.
- Browser-based user interface.
- Alerting.
- Application management.
- Audit.
- Control access management.
- Data synchronisation and transformation.
- Integration with client apps and services.
- Identity management.
- Mobile device management.
- Vulnerability protection.
- Workflow.

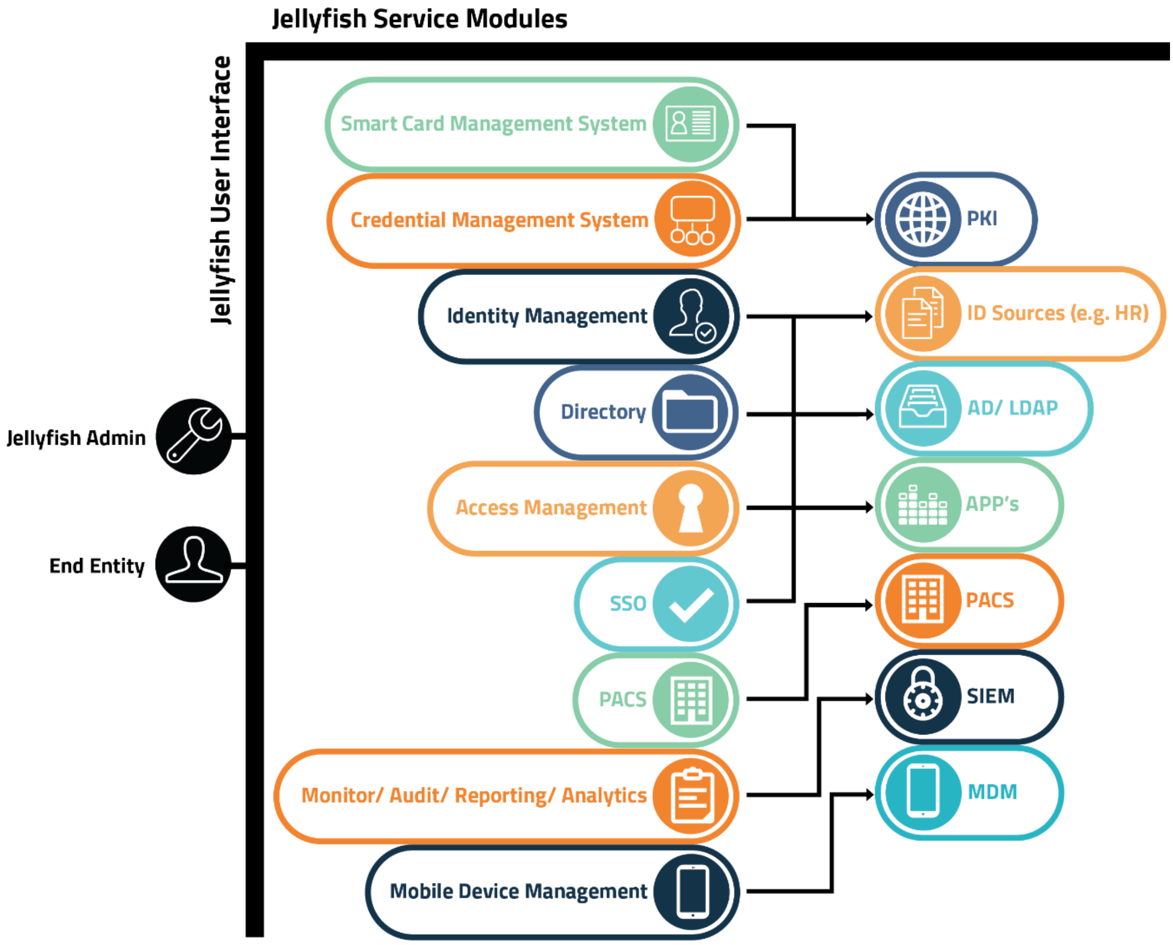

Figure 1: Jellyfish User Interface

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.