Fact Sheet

Cogito Group

Certificate Lifecycle Management

Manage Certificate Expiry and Reap the Benefits

Cogito's Certificate Lifecycle Management prevents unplanned outages by managing certificate expiry. Importantly it builds the relationship between the device, application or service and the certificates. This makes our application business outcome centric.

The Certificate Lifecycle Management functionality automates certificate creation for:

SCEP	AE	API
ACME	ACME+	CMP

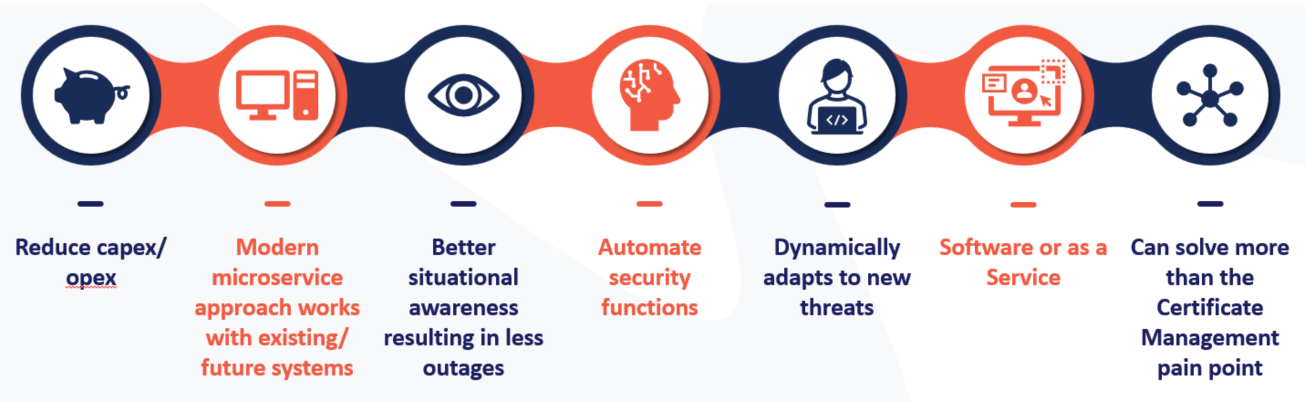
It utilises Discovery tools and build relationships with certificates to make managing and reporting far better and service centric.

Jellyfish offers full credential and key management. It is also much more than just a Certificate Lifecycle Management platform. It can also do:

- Token management
- HSM Key management
- Mobile credential management
- And automation in other areas
- Integration with SIEM

The Benefits

A single pane of glass to increase security and cut costs with both active and automated capabilities built in.


Reduce capex/ opex
Modern microservice approach works with existing/ future systems
Better situational awareness resulting in less outages
Automate security functions
Dynamically adapts to new threats
Software or as a Service
Can solve more than the Certificate Management pain point

Certificate Lifecycle Management

Fact Sheet

Certificate Lifecycle Management Functionality

PKI and Certificate Management

Automation, Search, Reports, Notifications, Manually Registering a device, user, or certificate

Smartcard and Token Management

Key Management

Specialist Active Security and Resource Tools

Tracking and Reporting

Certificate Tools

Portal

Also available - self Service and Self Service Reset Tools

SOC Tools

For monitoring and alerting, Logging, System Incident Event Management, and Asset Management

Full CMDB

Bring related records together for Users, Devices, Applications and Services

IdAM light

For Individuals, Credentials, Assets (CMDB), Provisioning and Deprovisioning, and Synching Data between stores and organisations. Can interface with full IdAM platforms

Discovery

Discover certificates and keys on devices and bring existing platforms under management at any time

Automation and Reporting

Automate and Report on your certificate holdings at any time

Certificate Lifecycle Management Components

- Credential management (PKI smartcard and soft certificate management, discovery, OTP, SSO)
- Encryption (DB, tokenizer, app, VM, file/ folder, BYOK, HYOK, email in transit and in cloud, e.g. O365 native encryption
- IdAM core for create, update, and delete
- Full data synch
- Others include: CASB, perimeter and endpoint protection, penetration testing, MDM, biometrics

Certificate Lifecycle Management

Fact Sheet

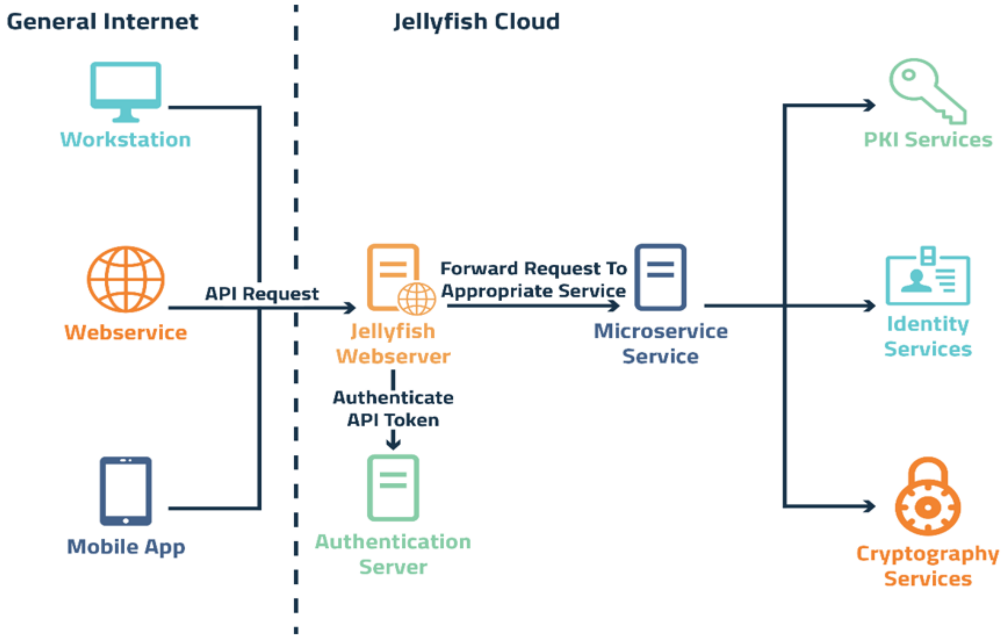
Certificate Capability

- Automation (e.g. Certificates for Windows, Linux, Network Equipment, etc)
- Integrations with other platforms (e.g. ServiceNow, Remedy/BMC, Digicert, Lets Encrypt).
- Notifications
- Boolean Search
- Reporting
- Manual Cert issuance
- Anonymous capability
- Cert Discovery and CA Polling

Automation Options

- Microsoft Automatic Enrolment Protocol (AE) both old and new versions.
- ACME and ACME+
- SCEP
- ITSM (eg Service Now)
- REST API
- JF Portal (for manual issuance)
- Cert Discovery and CA Polling

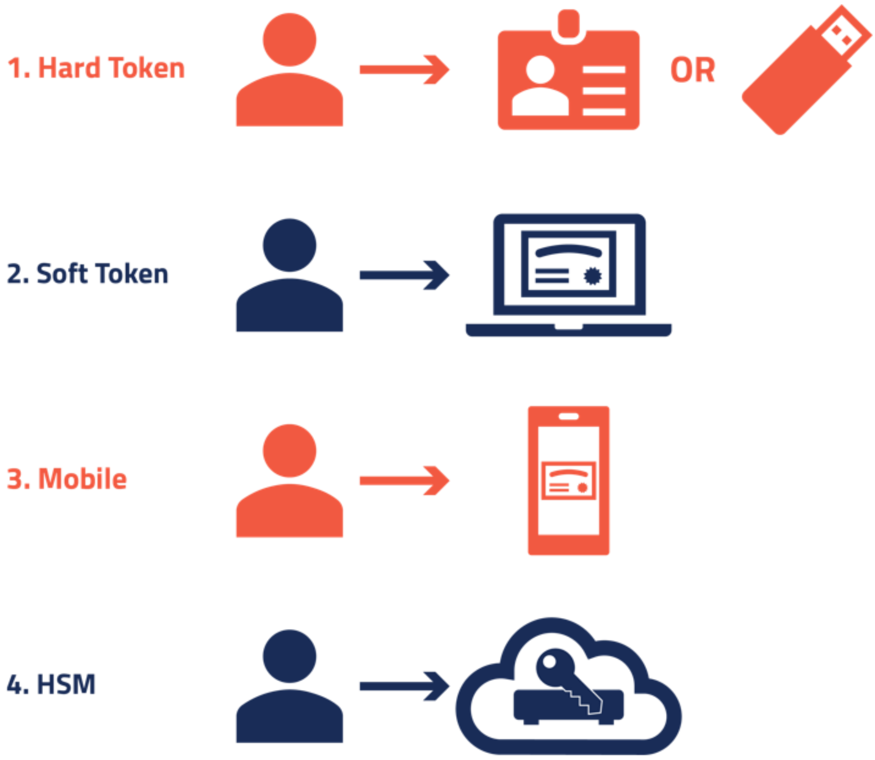
Automation - REST API



What else can Jellyfish Do?

- CA Management (cross platform)
- HSM Management (Thales/Gemalto)
- Full Card or Token Management capability (e.g. smartcards, Yubikeys, Mobile Devices, etc)
- Key Management – Generate and Manage keys for BYOK AWS, BYOK Azure and other platforms needing Asymmetric and Symmetric Key types such as RSA, ECC, AES and 3DES.
- SIEM integration for search and reporting
- Supports MFA (e.g. OTP, Soft Certs, Smartcards, Yubikey, FIDO2 etc).
- Multi-tenancy and multi-organisation (sharing or not sharing capability)

We support many Token based options



Unique points of difference

- Cost - we pride ourselves on being bot best and least expensive
- Large CA and automation method support (e.g. Let’s Encrypt, Digicert, etc)
- Modern microservices architecture (fast, reliable, and scalable)
- Green fields not required. Can maintain existing CAs and registration methods
- Can bring in credentials from offline and disparate systems manually or automatically
- Search and reporting
- Relationship between components (e.g. devices and certificates) including full CMDB
- More than just one app. Includes Credential, Token and Key Management, CMDB, Analytics, Monitoring, Logging, PACs/LACs, etc
- Greater agility for changing customer needs

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.