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. Jellyfishes Certificate Lifecycle Management (CLM) capability includes a full Configuration Management DataBase (CMDB). This is also know as an Asset Management Tool. As well as an Identity and Access Management (IdAM) capability. This allows the CLM to build relationships between users, devices, applications, services and the certificates generated for this. This makes Jellyfish unique in that it is business outcome centric, not just certificate centric. It also allows for better integration between other components in the technology stack.

The Certificate Lifecycle Management functionality prevents unplanned outages in in a number of ways. They are:

Certificate Automation

Certificate automation is the automatic registration and generation of certificates for users, devices, services and applications as well as the renewal of these entities' certificates automatically. This is the primary method by which the CLM assists in avoiding an unplanned outage. It has the added benefit of reducing the workload of ICT staff. Jellyfish offers the following automation methods:

ACME	ACME+	AutoEnrolment
CMP	REST API	SCEP

Certificate Notifications

The Jellyfish CLM tool provides automated notifications which can be customised to the individual business needs. These notifications can be sent via email automatically to a default group and even sent to an individual for a specific individual certificate. Webhooks can also be used for notifications and the REST API can also be used to query for this information.

Certificate Reporting

Detailed reporting not just on certificates but on the users, devices, applications and services that use them is an invaluable tool in the fight against certificate based unplanned outages. It also aids an ICT team in other ways such as improving the security posture of the systems and services they support. The advanced reporting tool within Jellyfish has the ability to report on any facet of a certificate or on the entity that certificate is used for or by. These reporting capabilities are customisable and complex searches can be created and saved for future use. The Boolean based capability not only supports a diverse array of positive searches but also allows for the exclusion, or combination of information in order to get the exact information that the organisation requires.

Reporting information can also be downloaded to form reports in other systems such as business intelligence systems or in excel spreadsheets for graphing. All of this capability is also available via our REST API allowing any system or service that has the requisite authorisation to access this capability.

Discovery

Our Discovery tools discover certificates on network and inside of devices. Discovery also builds relationships with certificates to make managing and reporting far better and service centric. Discovery does this through two mechanisms. They are network based where no client is required to request certificate information from devices, services and applications. The second method that can be used in conjunction with the network based approch is a client based approach. This is used where certificate information is not available to network based services. This could be because the device does not allow access to the certificate from a network connection or where there is no ability to have discovery components reach into that network segment.

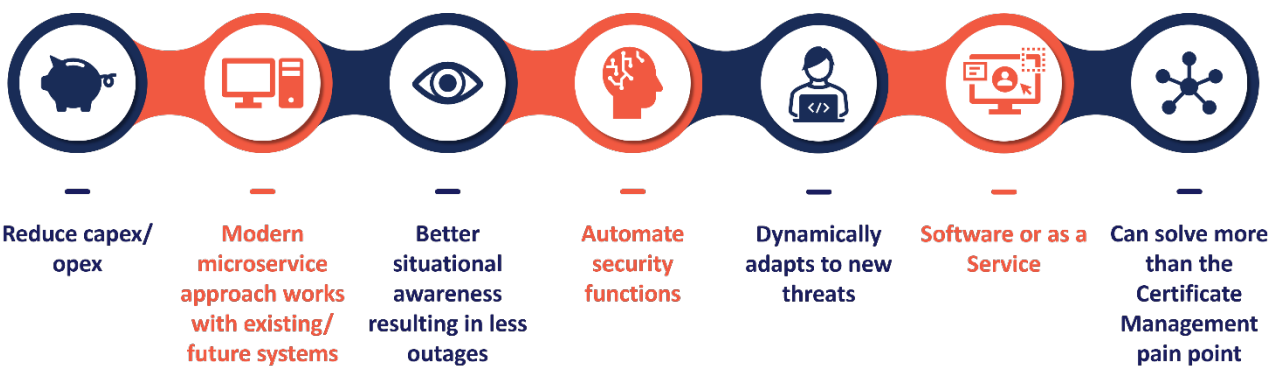
More than just a CLM

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

- Full Certification Authority capability allowing the replacement of other CA products
- Token management (also know as a Card Management System and a Card Application Management System)
- HSM Key management
- Mobile credential management
- Configuration Management Database
- Infrastructure Monitoring tool
- IdAM based automation services
- Audit tool for log Integration tool for SIEM solutions

The Benefits

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



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

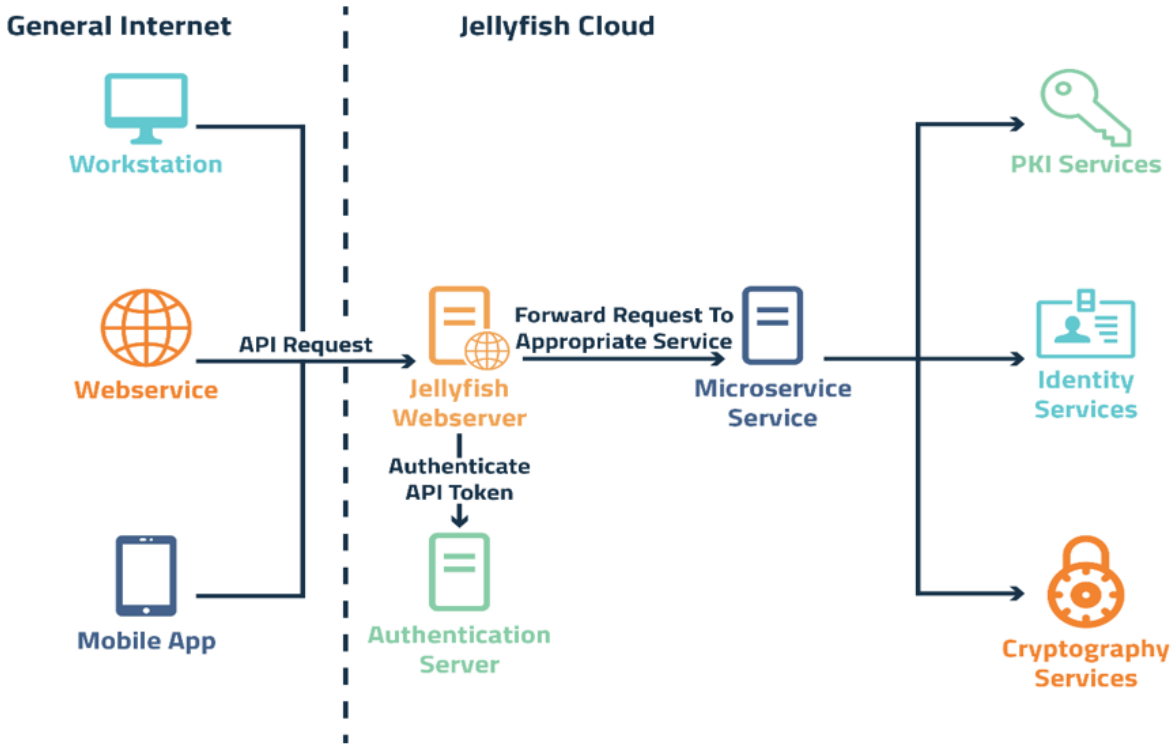
Certificate Capability

- 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



REST API Demonstration Video

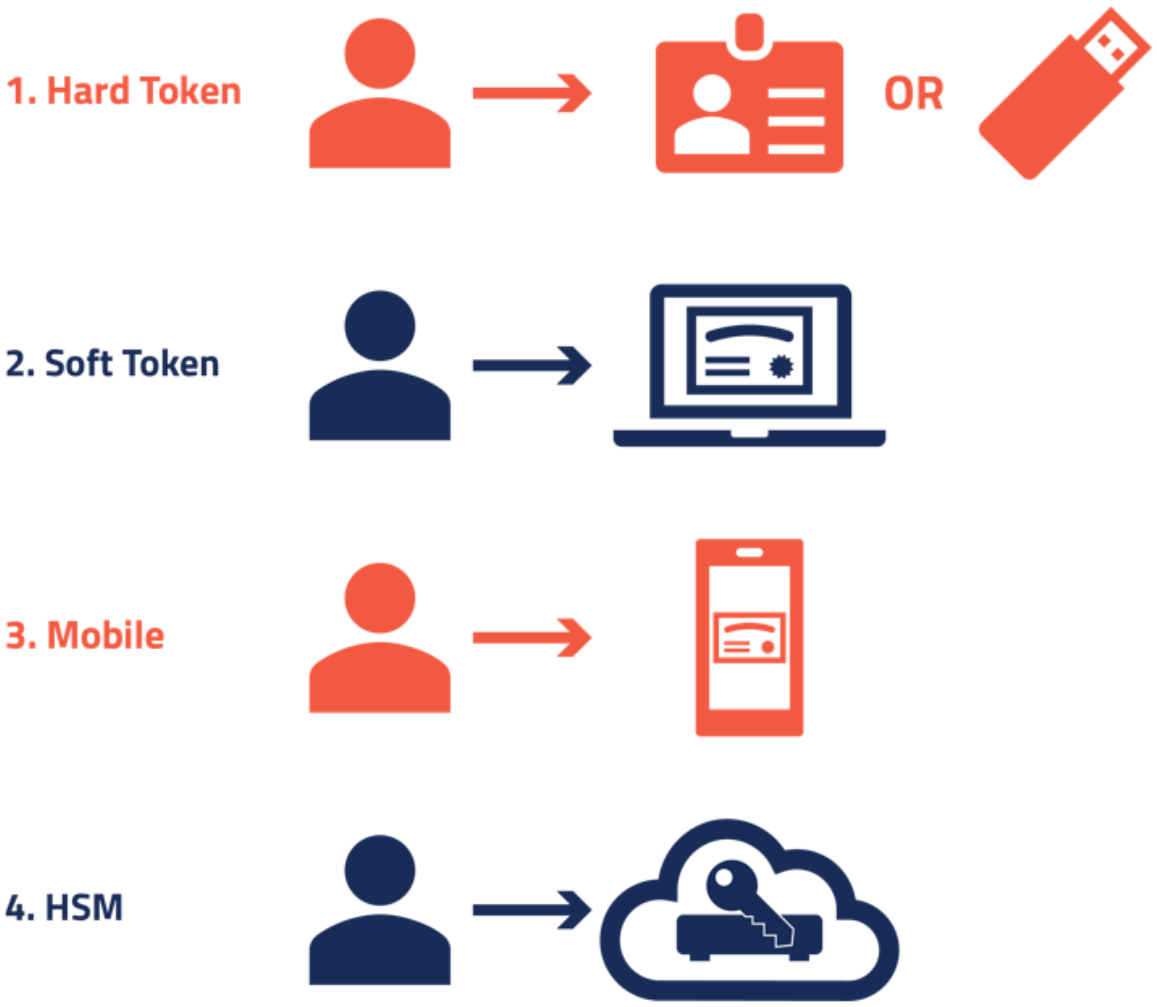
Certificate Lifecycle Management

Fact Sheet

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



Certificate Lifecycle Management

Fact Sheet

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.