Fact Sheet

Cogito Group

Certificate Automation

The next generation of Certificate Automation

Cogito's Certificate Automation Services prevent certificate outages and makes life easier for its users.

Cogito have developed a solution that simplifies the requesting and issuing of certificates. Most certificates are automated, but users will receive notifications about the expiry of any non-automated certificates. The Cogito Group certificate automation service:

- Verifies the details within certificate requests.
- Monitors and reports on certificates under management throughout their lifetime.
- Identifies certificates that are in use but not under management and brings those discovered certificates into the management service.
- Automates the issue and renewal of certificates wherever possible and appropriate

Auto-enrolment

Auto-enrolment is a Windows-specific protocol that allows Microsoft Windows devices to internally request certificates to a domain. This protocol not only covers renewal but also new requests as the client is informed of the need to request a certificate when it joins a domain through Group Policy. Figure 1 outlines the Auto-enrolment process below.

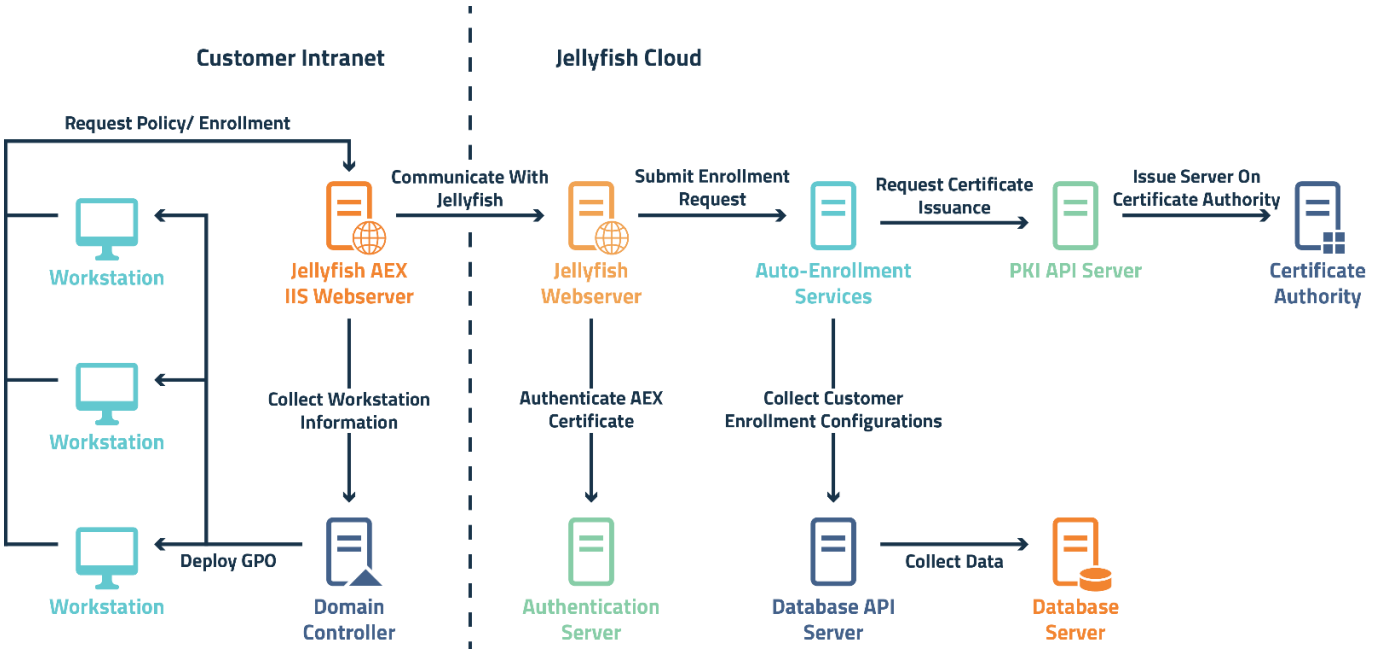


Figure 1 - Auto-Enrolment Overview

Certificate Automation

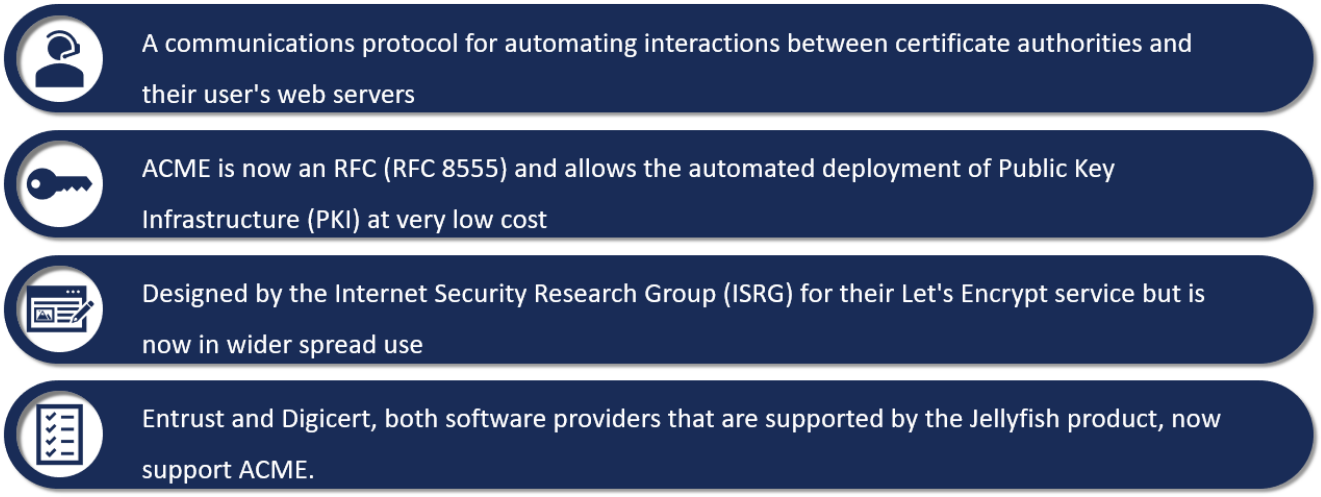
Fact Sheet

The older way Cogito Group's auto-enrolment service worked was by allowing a domain to believe a Microsoft CA is local to its environment, even if that is not the case. While this worked well, it did have some issues related to needing to support DCOM, which means numerous ports need to be made available for this solution to work.

The Cogito Group auto-enrolment feature has recently been upgraded from supporting an older MS-WCCE protocol through DCOM, to Microsoft's new approach of MS-XCEP and MS-WSTEP. This new, improved service is more secure, reliable, and available. The backend service instance is highly available, replacing the older model's protocol limited 1-to-1 client-server relationship. Embedded, secure channel communications replace the need for other forms of encryption such as VPNs etc. The ability to filter all components of received requests against defined certificate policies is another advantage provided by the auto-enrolment service. The ability only need one port to be open through a firewall and for that port to by default be the standard HTTPS port of 443 is also a benefit to some organisations.

ACME Protocol

Automatic Certificate Management Environment (ACME) Protocol



The ACME protocol is used to enable the automatic enrolment of certificates for webservers. ACME allows a client to request certificates using signed JSON messages sent over HTTPS. The ACME server will verify that the client owns the requested domains by using either a HTTP or DNS based challenge.

Several free and open-source ACME clients exist. The most popular of which, Certbot, can be configured to automatically install and renew certificates for Apache, Nginx, and other webservers.

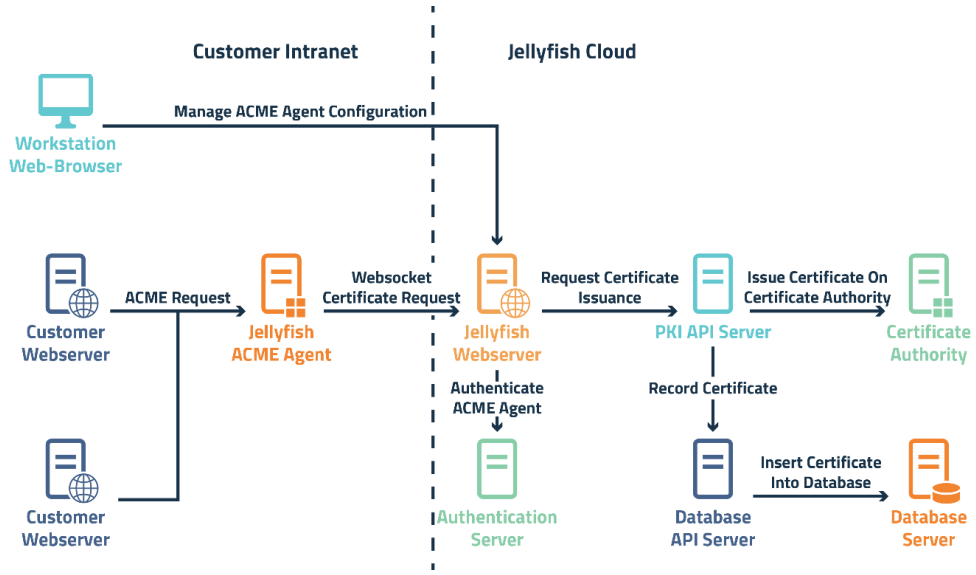


Figure 3 - ACME Integrations

ACME+

ACME+ is a Cogito Group extension to the ACME protocol which allows issuance of different types of Certificates, whereas the standard ACME protocol is limited to certificates for webservers.

When operating in ACME+ mode, the server can be configured to use other forms of trust and validation rather than relying on a certificate's identifiers that must be based on a DNS name in the event one is not available. This mode is intended to allow for the automated issuance of certificates using convenient and familiar tools.

Functionality of ACME+

- ACME+ adds the ability to use the ACME protocol as a basis for certificate types other than TLS certificates
- AMCE+ allows for domain validation to be turned off where required.
- ACME+ replaces our existing “store and forward” capability with a standard protocol approach:
    - this is where a certificate is requested and delivered through a store and forward mechanism for client devices that are disconnected from the CA they're to request the certificate from
    - this allows domains that are disconnected from a CA to still have a level of automation with certificate requests.
- ACME+ will store automated requests for transfer to another network where the CA resides.
    - It enables requests to be automatically bulk submitted and returned for transfer back to the originating disconnected network.
    - The requests can then be automatically picked up by the clients that have requested

Store and Forward

In situations where the Cogito Group ACME server is entirely disconnected from the issuing certificate authority, pending requests may be copied from the server and manually issued. Once issued, these certificates can be automatically distributed by the server. This enables a high degree of automation in highly secure or otherwise segregated networks.

Cogito's ACME+ ensures full implementation of the ACME server for the automated approval and issuance of certs using the ACME Protocol described in RFC 8555

SCEP

Simple Certificate Enrolment Protocol (SCEP) is the primary method of automatic enrolment for certificates MS Intune managed devices, Linux based devices, and many other network devices. SCEP is a protocol often used by devices with limited capabilities to obtain certificates. The standardised SCEP procedure is outlined in Figure 2 below. The SCEP service offers renewals after configuration, but in the case of Microsoft Intune, can also issue new device requests. SCEP is an RFC (RFC 8894) standard that defines how a network connected device can remotely request a certificate from a Certificate Authority (CA).

The process involves a three step ‘handshake’ in which the device:

1. Determines the capabilities of the SCEP server.
2. Verifies the authenticity of the servers SCEP certificate.
3. Submits a CSR for issuance to the CA.

MS Intune also offers the ability to use the NDES protocol instead of SCEP, but this method is becoming less popular due to a number of limitations with this connection method. Cogito used to provide an NDES based service but this has been retired in favour of the SCEP service.

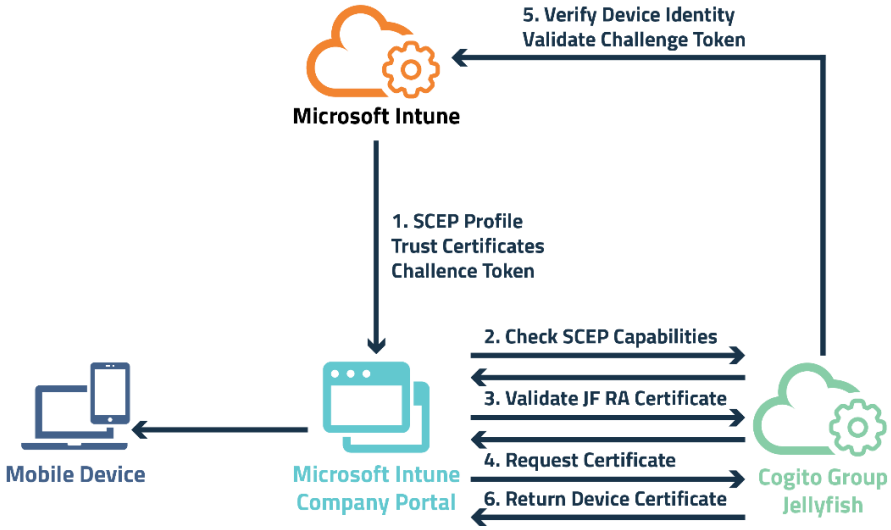


Figure 2 - SCEP Intune Verification Process

ITSM Automation

Information Technology Service Management (ITSM) allows applications such as Service Now or BMC Remedy to enable existing service management tools to provide the same or a similar process to users requesting certificates. The service allows clients to submit a ticket, go through the processes within the ITSM tool for that workflow, and deliver a certificate directly back into the ticket that was submitted.

Polling

The Polling feature enables the gathering of certificates from a CA directly. This can be used to bring certificates not issued through Jellyfish under management or as a transition to Jellyfish mechanism for existing PKI deployments. Where this can also be useful is where an ADCS CA is specified that issues certificates directly. In this instance poling allows for these certificates to be brough under management so that an accurate count of certificates and all of their attributes. This in turn allows for them to be searched, revoked and reported on. They can also be exported. Importantly, it enables users to be able to determine where the certificates they created originated from.

Discovery

The Jellyfish discovery tool is different from the enrolment protocols mentioned above. It is also different from Polling. The discovery tool is used to discover existing certificates and keys within an environment to bring them under management quickly and effectively. The Jellyfish Discovery Services Module includes certificate discovery tools to perform discovery of certificates in use within the targeted networks. Networks are scanned to identify any devices operating on them, and the devices are then scanned to determine any certificates present. Details of discovered certificates and devices are stored within the Jellyfish data store, allowing reports to be generated on data relating to the discovery run.

The discovery tool captures this data by interrogating stores such as the Windows Machine certificate stores and Java Keystores for what certificates and keys they are storing. This allows for

these keys and certificate to be brought under more active management. It allows for a significant reduction in unknown certificates. It also allows for rouge or unapproved PKIs and Key Generation tools to be identified. This process will poll servers, services, and applications to attempt to detect the use of certificates within the network. These will then be registered within the Jellyfish application. As the responsible entity for these certificates may not be known, these certificates are reported to Jellyfish administrators to ensure that action can be taken to determine the person or group responsible for their management.

REST API

Cogito Group's Jellyfish REST API allows integrations of other products through a programmatic interface, which can be viewed in Figure 4. The API calls are supplied to customers in the event of a custom app, but many applications and devices are already provided for. The Jellyfish portal itself uses these calls meaning anything you can do in the web portal, you can do through the JF REST API.

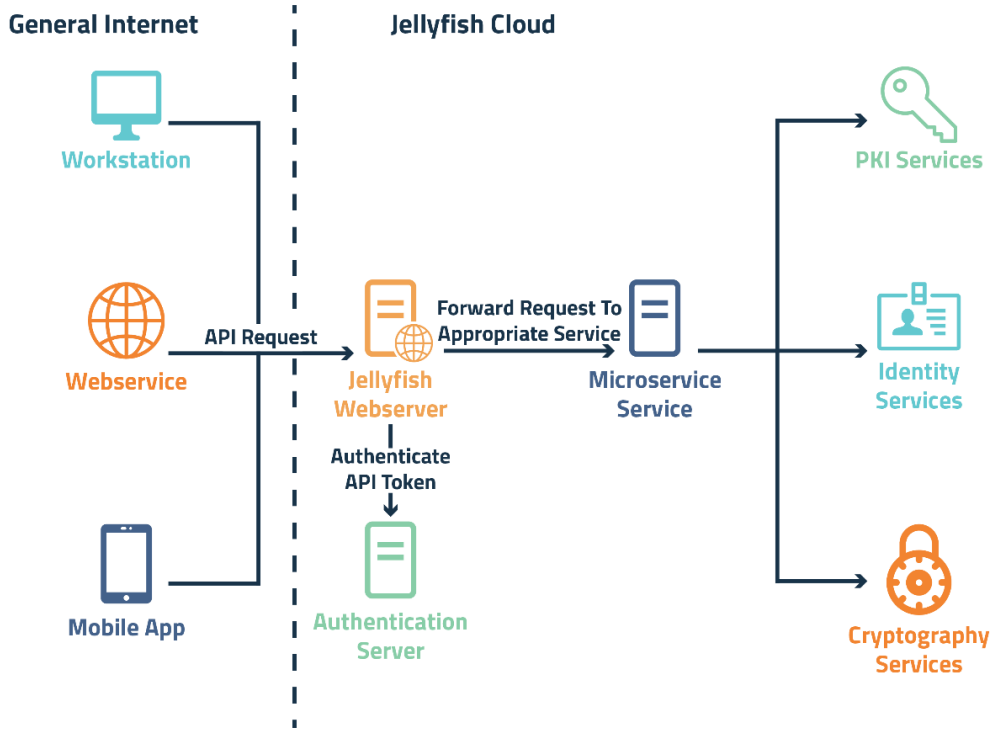


Figure 4 - Rest API Overview

Jellyfish Portal

While not an automated means of registering for a certificate, the Jellyfish portal can take numerous custom requests and fulfil them. However, Jellyfish's greatest strength is reporting. This can be an individual email to a user for an impending certificate expiry or running a report on the number of registration officers active between the requested timeframes. The search and report function has full Boolean search capability allowing you to run simple or very complex searches, such as finding any certificates with a first name: John, last name: Brown - but not preferred name of Brownie - that expire between 1/12/2022 and 1/01/2023, and have a certificate usage of digital signing only.

Certificate Automation

Fact Sheet

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.