Fact Sheet

Cogito Group

Certificate Automation

The Certificate Automation service provided by Cogito Group serves to prevent certificate outages and make life easier for its users. Most certificates are automated, but users will receive notifications about the expiry of any non-automated certificates. The Cogito Group certificate automation service:

- Simplifies the requesting and issuing of certificates.
- 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.

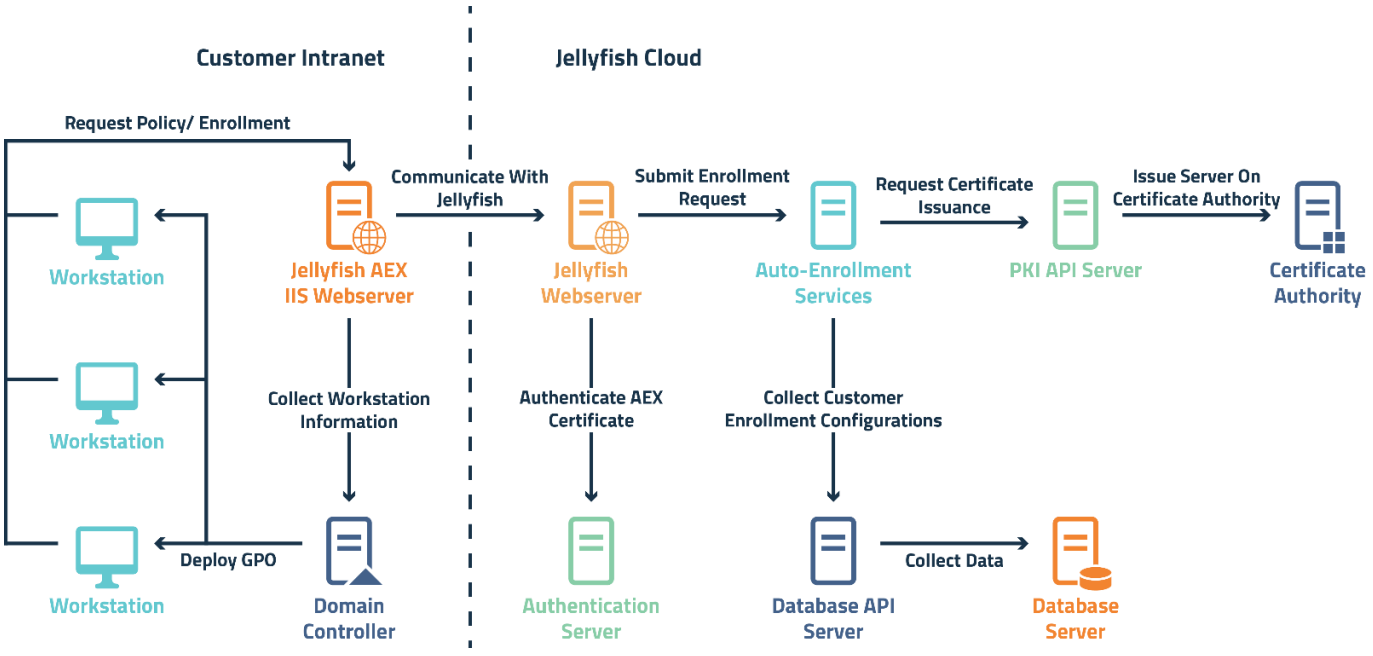

Figure 1 - Auto-Enrolment Overview

The components of Cogito Group's auto-enrolment service allow a domain to believe a Microsoft CA is local to its environment, even if that is not the case. A Microsoft ADCS CA is not even required to respond to the requests.

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 backend. HA, for instance, replaces a 1-for-1 client-server relationship. Embedded, secure channel communications replace the need for other forms of encryption. The ability to filter all components of received requests against defined certificate policies is another advantage provided by the auto-enrolment service.

ACME

The Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating interactions between certificate authorities and their user's web servers, as displayed in Figure 3. ACME is now an RFC (RFC 8555) and allows the automated deployment of Public Key Infrastructure (PKI) at very low cost. It was designed by the Internet Security Research Group (ISRG) for their Let's Encrypt service but is now in wider spread use. Entrust and Digicert, both software providers that are supported by the Jellyfish product, now support ACME.

Cogito Group was one of the first providers to support ACME v2. You can use Jellyfish to access both Let's Encrypt and Digicert externally trusted certificates.

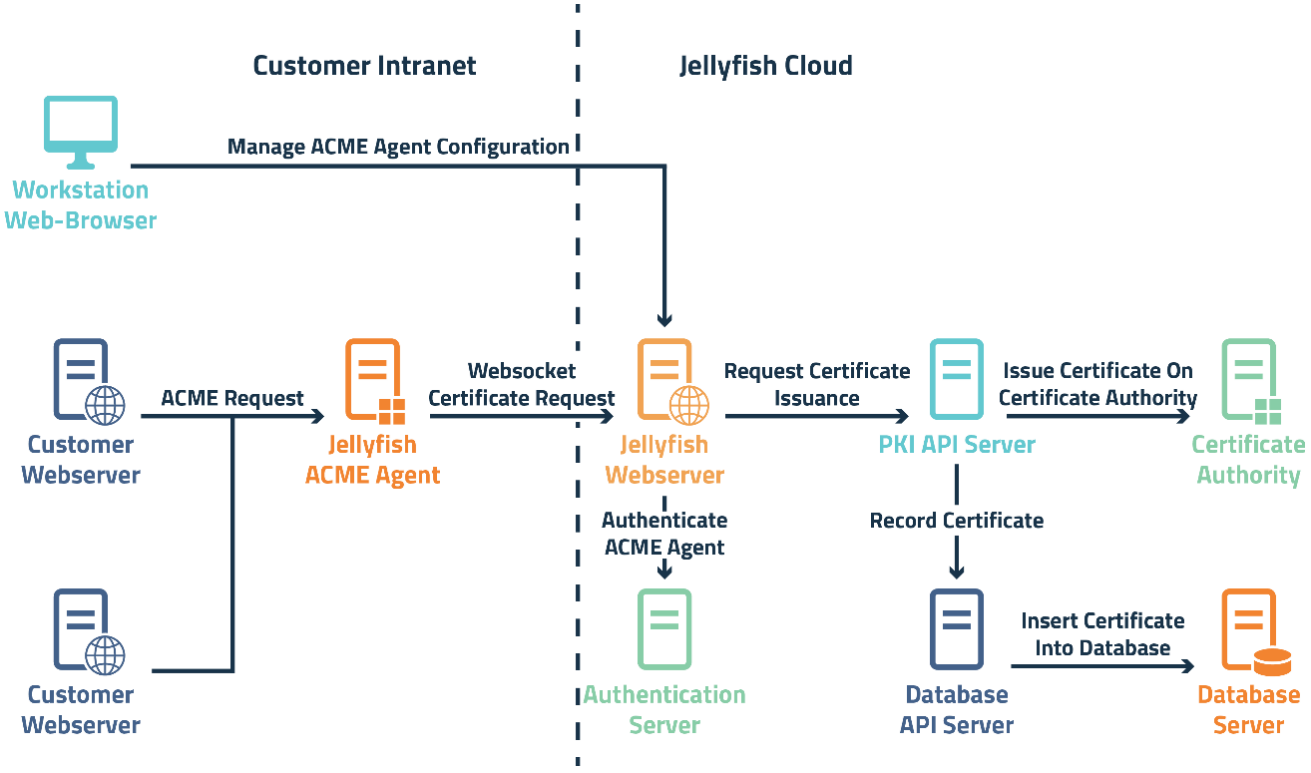

Figure 3 - ACME Integrations

SCEP

Simple Certificate Enrolment Protocol (SCEP) is the primary method of automatic enrolment for certificates on devices that use MS Intune, Linux, or many other networks. 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.

You can also connect using an NDES server, but this method is becoming less popular.

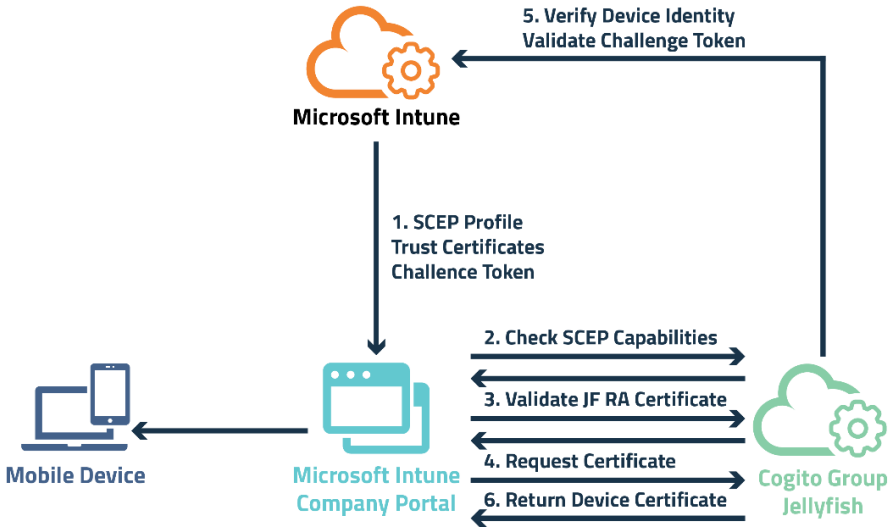

Figure 2 - SCEP Intune Verification Process

ITSM

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.

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.

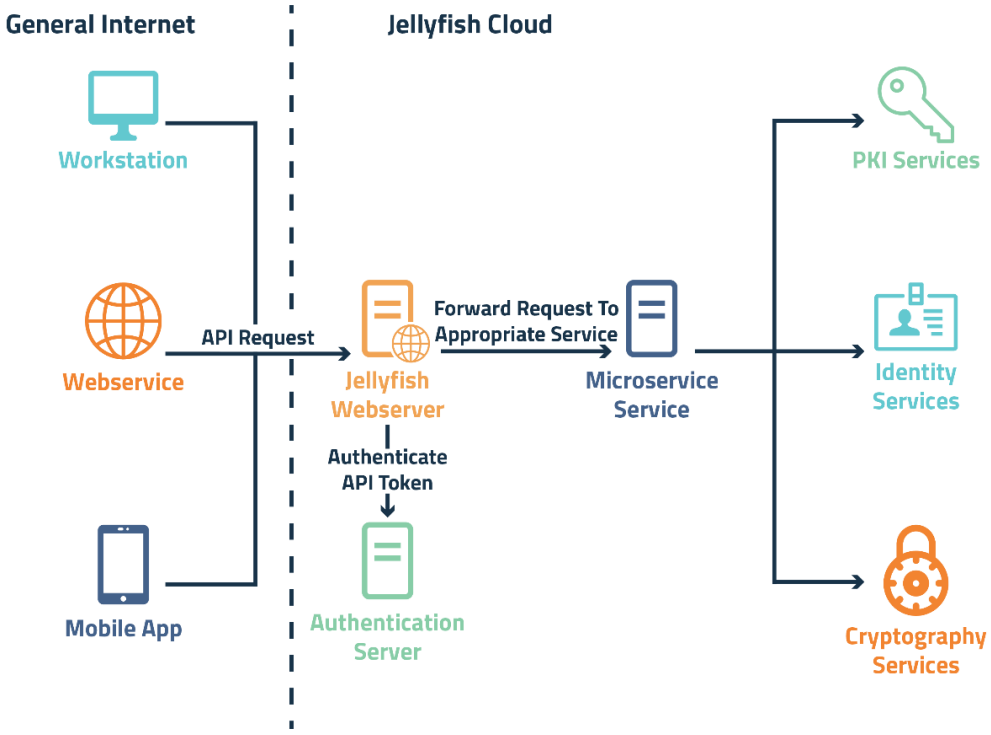

Figure 4 - RestAPI Overview

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 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.

Discovery

The Jellyfish discovery tool is different from the enrolment protocols mentioned above. The discovery tool is used to discover existing certificates 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 also provides the ability to scan and determine certificates within Windows Machine certificate stores and Java Keystores. To bring under management unknown certificates, or certificates that weren't managed by Jellyfish processes during issuance, Cogito Group provides a discovery service. 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.

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.