

ACME+

The next generation of Certificate Automation - introducing ACME+

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 when running in ACME.
- 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 issuance and renewal of certificates wherever possible and appropriate

ACME+ Functionality Enhancements



Enhanced Communication

ACME clients (eg Certbot) can talk to Jellyfish for the purposes of certificate enrolment and renewal

Validate Ownership

Jellyfish to validate ownership of domains through ACME and report on the current active ACME clients and their registered domains

Store and Forward CSRs

Using ACME+ to "store and forward" pending CSRs on a network entirely separated from Jellyfish.

Add Other Identifiers





Extending the ACME protocol to allow the issuance of certificates with identifiers other than DNS names (an email address)

ACME+ Roadmap 2022+

Jellyfish's CMDB capability will integrate the data from devices and servers into the greater device information listings

About the ACME Protocol

Automatic Certificate Management Environment (ACME) Protocol

-  A communications protocol for automating interactions between certificate authorities and their user's web servers
-  ACME is now an RFC (RFC 8555) and allows the automated deployment of Public Key Infrastructure (PKI) at very low cost
-  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.

The ACME protocol is used to enable the automatic enrolment of certificates for web servers. 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 web servers.

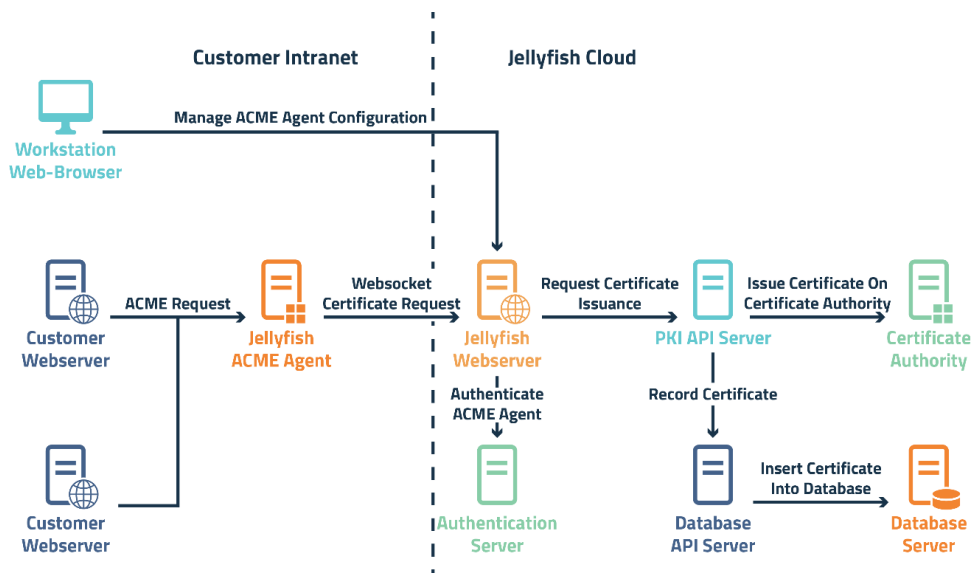


Figure 3 - ACME Integrations

Introducing ACME+

ACME+ is a Cogito Group extension to the ACME protocol which allows issuance of Certificates with arbitrary identifiers, whereas the standard ACME protocol is limited to certificates for web servers.

When operating in ACME+ mode, the server does not validate the certificate's identifiers. 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
- ACME+ 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 disconnected domains.
 - this allows domains that are disconnected from a CA to still automate 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.

ACME+

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



Agent for deployment

An agent is available for deployment on the customer networks (Linux or Windows)



Easy Installation

The agent communicates with Jellyfish over a HTTPS endpoint



Deployment

Within the Customer environment or the Jellyfish aaS environment



RFC 8555

The ACME service meets all security and operational requirements of RFC 8555 to ensure the service is secure

Integrity

ACME+ enrolment process ensures the integrity of the solution.



Integrity

The enrolment process will ensure the integrity of the solution



Identifier

Only an entity that controls and identifier can get an authorisation for that identifier



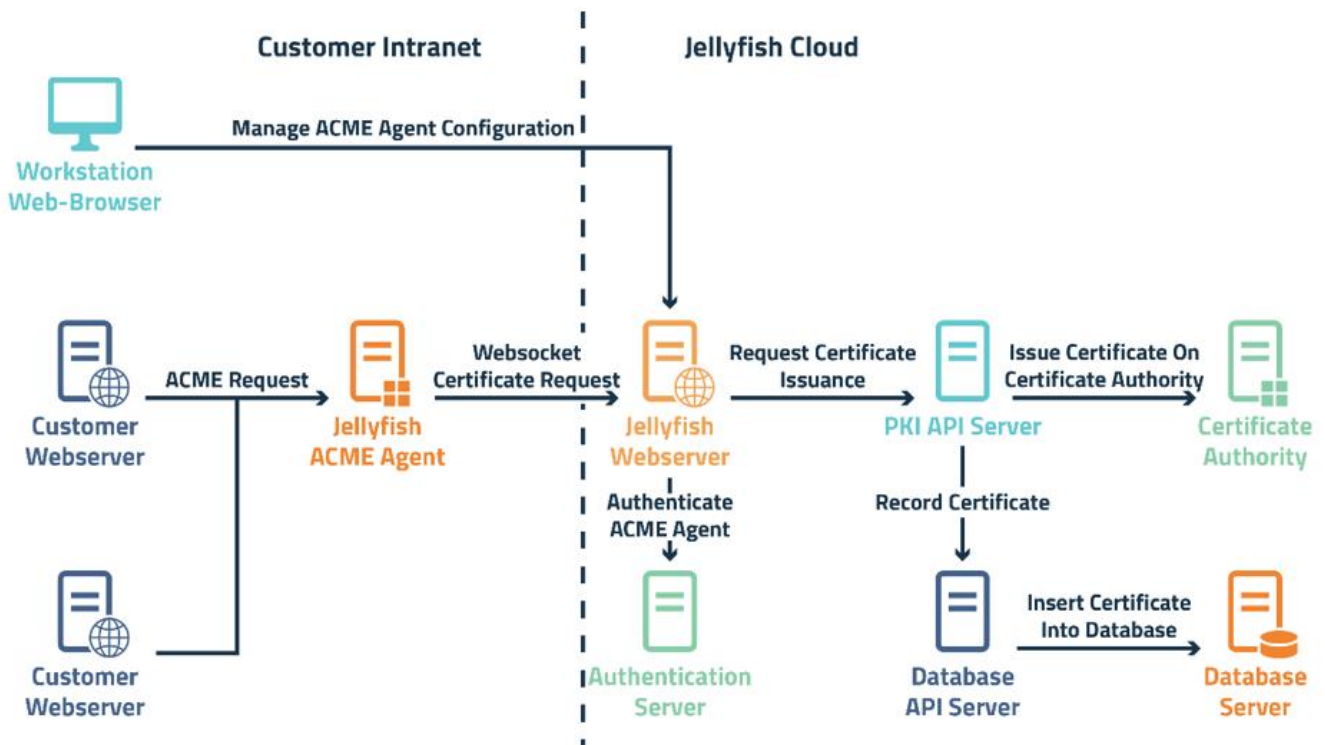
Authorisation

Once authorised an accounts key's authorisations cannot be improperly used by another account.

ACME+ Design Overview

- The ACME protocol is used to enable the automatic certificates for webservers
- Primarily used by LetsEncrypt to enable domain validation (DV) and certificate enrolment/renewal for publicly facing websites
- Design covers ACME+ support within Jellyfish
- Provides the ability to proxy the ACME protocol for any CA supported
- ACME+ in Jellyfish enhances functionality

Jellyfish ACME+ Integrations



High level design

As illustrated in the diagram above, the high level design outlines:

- The ACME endpoints listed in the RFC8555 standard are implemented in Jellyfish in ACME+.
- They provide endpoints accessible through the PKI microservice for the purposes of ACME
- These are forwarded onto:
 - the database (for storing the account ID's of the ACME clients) or
 - the CA microservice (for obtaining the certificates from the CSR).
- Once an ACME client has been registered, it's account ID will be stored in the Database
- It will be able to request certificates for the server until the configured expiry time for the server is up.
- The ACME client's registered domain and the machine it is representing is monitorable within Jellyfish through the menu

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.