Fact Sheet

Cogito Group

Polling

The next generation of Certificate Automation - introducing Polling

Cogito's Certificate Automation Service Polling Feature enables users to determine origin of certificates.

The Jellyfish Polling feature enables the gathering of certificates from a CA directly. This can be used to:

- bring certificates not issued through Jellyfish under management;
- as a transition to Jellyfish certificate management mechanism for existing PKI deployments;
- where CA has issued certificates directly from the interface;
- as a redundancy check or reconciliation tool to ensure other mechanisms do not miss anything; or
- as a transition of CA types into Leviathan CA, which is a performance and scale oriented CA built into Jellyfish.

The use of Jellyfish polling allows these certificates to benefit from management allowing them to be searched, revoked and reported on. They can also be easily exported.

Jellyfish polling enables users to be able to determine where the certificates they created originated from. It also allows an organisation to continue to use existing issuing methods when they introduce Jellyfish rather than requiring the customer to transition all processes to Jellyfish specific registration and automation processes in order to see all issued certificates. This is a key differentiator to other software which requires all issuances to be done through their end points in order to be able to manage all issued certificates.

What problems does the Polling feature solve?

Polling onboards certificates into the Jellyfish environment that were not issued through part of the Jellyfish solution.

These might be:

- certificates that were manually issued from a CA;
- certificates issued on a CA prior to Jellyfish being implemented; or
- certificates from offline or retired Certificate Authorities.

This is particularly useful when you are onboarding to the Jellyfish solution, or when you bring new CAs in that were previously unmanaged or managed with another software.

It is also useful as where there has been a disaster recover event. In this instance it can be used to recover lost certificates from a backup or when the Jellyfish database services experience interruption.

How does Polling work?

Polling works for both on-premise and SaaS cloud system

Polling works differently depending on the CA type. For instance when used with AD CS, polling works on Active Directory, by querying certificates directly using the Microsoft Native certificate database interfaces. For UniCERT Jellyfish Polling uses UPI where installed or direct DB integration where this is not an option and the REST API when doing this for EJBCA for instance.

As much Jellyfish relevant data is extracted as possible and fed into the Jellyfish solution for analysis, search, and reporting.

Polling can be used in both on-premise deployments and as part of a SaaS cloud system.

Using polling for SaaS is particularly useful when customers have an older CA and want to switch to a Jellyfish CA while still retaining all the information from their old CA for historic record purposes.

Polling Features

- Ability to capture all certificates from any source within Microsoft Active Directory.
- Ability to control how far back polling will search, and from which serial number to begin with. Rollback to re-poll a CA a second time (without causing duplications in Jellyfish), resumption to continue from where it has left off, complete reset of progress to poll a CA as if it has not been seen before.
- Ability for enhanced licensing capabilities. Given templates from the CA are configured in Jellyfish, relationships to templates CAs, and costs will persist in Jellyfish as if they were a native Jellyfish cert.
- Use of the powerful Jellyfish search to find certificates with matching criteria.
- Use of the Jellyfish notification system to keep you up to date on the lifecycle of your Jellyfish certificates.

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.