Fact Sheet

Cogito Group

AD CS

Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) is a Microsoft product that provides services for issuing and managing digital certificates used in software security systems that employ public key technologies.

AD CS provides digital certificates, they can be used for authentication of computer, user, device, or documents on and across a network. Digital certificates provide:

- Confidentiality through encryption
- Integrity through digital signatures
- Authentication by associating certificate keys with computer, user, or device accounts on a computer network
- Non repudiation

AD CS has full support in the Jellyfish ecosystem. Jellyfish can connect, issue, and manage certificates within an AD CS public key infrastructure (PKI). Jellyfish can even poll existing AD CS instances and create offline and online reports on its certificate usage. Jellyfish makes using AD CS easy and automates many of the more difficult and tedious tasks of managing an AD CS PKI. When you're ready to graduate from an AD CS PKI deployment, Jellyfish has a collection of tools for exporting, cataloguing, and bringing under management the assets previously managed by AD CS.

Key features

Jellyfish augments and extends the following AD CS functionality:

- **Certification Authorities**: Root and Subordinate Certificate Authorities (CAs) are used to issue certificates to users, computers, and services, and to manage certificate validity.
- **Web Enrollment**: Web Enrollment allows users to connect to a CA with a Web browser to request certificates and retrieve certificate revocation lists (CRLs).
- **Online Responder**: The Online Responder service decodes revocation status requests for specific certificates, evaluates the status of these certificates, and sends back a signed response containing the requested certificate status information.
- **Network Device Enrollment Service**: The Network Device Enrollment Service allows routers and other network devices that don't have domain accounts to obtain certificates.

- **TPM key attestation:** Lets the certification authority verify the private key is protected by a hardware-based TPM and that the TPM is one that the CA trusts. TPM key attestation prevents the certificate from being exported to an unauthorized device and can bind the user identity to the device.
- **Certificate Enrollment Policy Web Service:** The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate enrollment policy information.
- **Certificate Enrollment Web Service**: Certificate Enrollment Web Service enables users and computers to perform certificate enrollment through a web service. Together with the Certificate Enrollment Policy Web Service, this enables policy-based certificate enrollment when the client computer isn't a member of a domain or when a domain member isn't connected to the domain.
- **Automatic Enrollment**: The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate automatically through Microsofts AutorEnrolment protocols. Jellyfish allows this to be extended to other protocols natively such as ACME and SCEP.

Benefits of Active Directory Certificate Services

- **Cheap:** the AD CS role is available in the Windows Server operating system. This makes it a good choice for organisations with an investment in Windows servers. It also makes the use of the platform cheap and readily available as the role can be included on existing servers alongside other roles.
- **Simple:** as the platform has limited extensibility, it can be easy to set up and operate. This is great for basic requirements but can limit growth where the capability needs to do more over time or where scale and reliability are key considerations.
- **Active Directory Domain Services Integration:** the platform integrates with Active Directory Domain Services (AD DS). While this is an upside, it is also a downside. To get the most out of the platform's security and integration features (i.e., using an Enterprise, not Standalone deployment) you must have AD DS available to AD CS.

Drawbacks of Active Directory Certificate Services

- **Does Not Support High Availability (HA):** AD CS is not intended to be used to provide high availability, redundancy, or fail over technology for a Certificate Authority. The intended solution to the problems HA solves is instead to deploy and maintain multiple concurrent Certificate Authorities and deploy and manage Root Trust, CRLs, and OCSP responders for each. This is not scalable solution and introduces moving parts that cause reliability issues.

- **Mature but Outdated**: The database behind AD CS is the JET (or ESENT) Database. It's only remaining active use is within Active Directory, where services such as AD CS rely on a Database Engine still sitting at v4.0 more than 20 years later. AD CS itself last saw a major update as part of the release of the Microsoft Server 2008 operating system. A minor update was released in Microsoft Server 2012. Since the 2012 release it has effectively stayed stagnant since.
- **Not the right Database for the Job:** AD CS is based on the JET (or ESENT) Database. JET was the basis for many Microsoft products namely being the Database behind Microsoft Access. JET is a linear scaling, single threaded, iterative database. The technology is old, slow, and not a good choice for searching and managing certificates. Microsoft has discontinued it's use in newer applications.
- **Limited Recovery Options:** the limited recovery options of the JET Database Engine has a significant impact on a Certificate Authority and the wider PKI capability. Compared to modern database it severely lacks in backup and recovery. No replication support makes disk backup's the only redundancy solution. This risks the CA losing track of some certificates in a recovery event making revocation of those certificates impossible.
- **Performance Issues at Scale:** at over 1 million issued certificates AD CS becomes noticeably slower. At 2 million issued certificates AD CS at times becomes unresponsive and at 4 million it is effectively so slow as to be functionally stopped. The throughput of AD CS is limited by the key size, a strong RSA key with the length of 4096 severely limits the numbers of requests that can be processed per second. With the advent of Internet of Things (IoT) and the ubiquity of certificate-based security, a modern CA is expected to be able to perform at far higher numbers of certificates under management.

For more analysis on the Pros, Cons, and trade-offs of AD CS: read through Cogito Group's analysis of the technology in our AD CS - Pros and Cons whitepaper

AD CS

Fact Sheet

Jellyfish and Active Directory Certificate Services (AD CS)

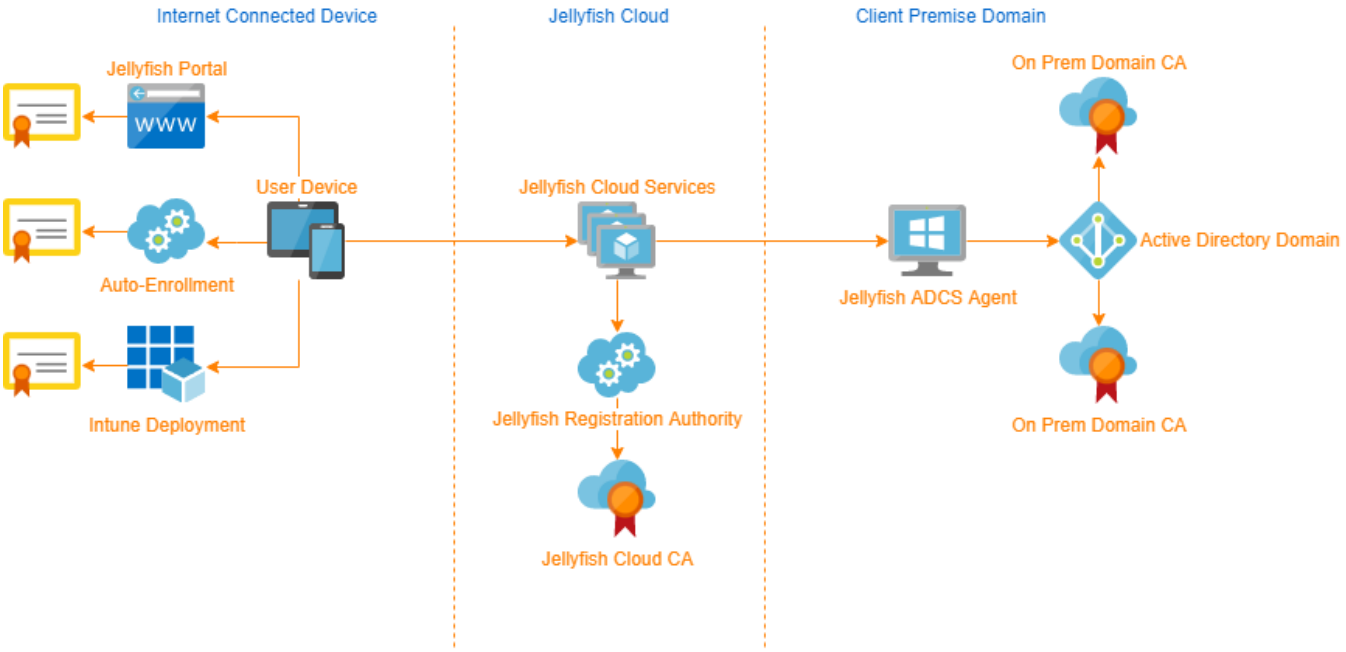
Bring the power and flexibility of the Jellyfish system to your existing PKI infrastructure.

AD CS limits the potential of your PKI. An aging and increasingly obsolete certificate enrolment system, AD CS adds little value to a public key infrastructure other than the ability to issue and revoke certificates.

Jellyfish builds on-top of an existing AD CS deployment by merging, consolidating, and enhancing the management technology available to administrators and reporters. When integrating AD CS with a Jellyfish deployment, operators have access to issue certificates from any pre-existing templates and authorities directly from a portable and easily accessible web portal. Reports can view, track, and gain insight into when these certificates are issued, consumed, expire and build relationships between users, devices, and credentials.

Jellyfish augments and enhances the limited feature set of an AD CS deployment. Access to automation tools for automating request and delivery of certificates, enhancements to certificate request and approval workflows, and lifecycle management and expiry notifications are all possible when AD CS collaborates with the Jellyfish system.

Jellyfish can also assist a customer to move away from AD CS to a larger more robust option when the time is right to do so.



What can Jellyfish do that ADCS does not?

- Improved Certificate cataloguing: *including subject alternative names, extended key usages, and many more extensions.*
- Superior Certificate search**:** *search for any certificate with a wide variety of terms at speeds up to 100x faster than AD CS.*

- Autoenrollment: *the full suite of Jellyfish auto-enrollment plugins are made available to AD CS including SCEP, AEX, ACME+, and more.*
- Reporting, monitoring, and alerting: *Jellyfish grants insights into an entire PKI at a glance, this includes certificates distributed by AD CS.*

The benefits of certificates under Jellyfish management?

The Jellyfish certificate management database is a thorough store of not only all information defined within a certificate, but the Jellyfish toolset builds relationships between these certificates and the users, devices, smartcards, and applications that consume these certificates.

AD CS relies on old technology. The certificates are stored in a JET Blue (ESENT) database, which does not index certificates in any useful way, and cannot be used to enable certificate analytics or search. Jellyfish can copy this data out of an existing ESENT database and store it in the Jellyfish certificate search indexes, enabling search on all fields of a certificate to enable certificate discovery not possible with AD CS. Jellyfish then uses this data to power reporting and insight technology to display real time certificate consumption information on the Jellyfish dashboard and reporting pages.

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.