White Paper

Cogito Group

AD CS. The Good, Bad and Ugly

About AD CS

Microsoft Active Directory Certificate Services (also known as AD CS originally called Certificate Services) is a platform that was first bundled as a Role in Microsoft Server 2000. It is a common choice for organisations seeking a simple and cheap Certificate Authority (CA) and wider, but small-scale Public Key Infrastructure (PKI) capability. This document discusses the pros and cons of the platform.

The Good

Mature

Certificate Services was introduced as a role in Server 2000. It has had updates in Server 2003, 2008 and 2012. It has been well tested with many small-scale deployments. It has had some minor bug fixes in 2016 with the formal introduction of additional smartcard capability, but realistically the smartcard capability is related to the operating system updates designed for smartcard use. The product has not been updated in any meaningful way since Server 2012 or circa the year 2011.

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. A common deployment method is to install the Role on a Domain Controller for instance. Cogito recommend against this approach as it can have security implications as described below.

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.

AD CS. The Good, Bad and Ugly

The Bad and the Outright Ugly

Does Not Support High Availability (HA)

While you can cluster the operating system that has the AD CS role installed, Windows operating system clustering requires centralised storage. This eliminates geo diverse redundancy as an option and limits zero trust options.

One solution is to have two CAs on different sites, each issuing a certificate with the same details for every device. This solves the problem of a CA going down but introduces additional complexity of having to maintain 2 separate trust chains. It also makes fault finding harder since the duplicated certificates could have different expiration dates and extensions since it will have used different templates.

While two CAs does provide failover, it falls short as a High Availability solution. The primary concern is certificate revocation. While a CA is in a failed state it is impossible to revoke certificates issued by that CA. This introduces a security risk where peer applications will continue to validate compromised certificate until the failed CA is restored. It also introduces a second concern of revocation request not being picked once the CA is recovered. This limitation is not ideal as often revocations can be time critical, given they can involve key compromise and privilege withdrawal. This opens an organisation up to security risks related to not having true HA.

AD CS also has issues when it is locally clustered using a single or multiple HSMs (Hardware Security Module). On a transition to the failover clustered machine, some HSMs in some configurations can reject what is ostensibly a 2nd machine try to connect to the HSM, making a secure service far less reliable. An example is where M of N using physical tokens on a HSM to achieve a higher level of compliance is required such as FIPS 140-2 Level 3.

Mature, but No Real Updates or Feature Additions in More Than a Decade

The database behind AD CS is the JET Database. JET version 4.0 first introduced in Access 2000 has had no feature updates since it was introduced and went end of life as a dedicated Database solution in 2004. It's only remaining active use is within Active Directory, where services such as AD CS rely on a Database Engine still siting at v4.0 more than 20 years later. Microsoft Jet Database Engine v4.0 SP8+ as part of Windows Vista/7/2008. This makes it difficult to operate, backup, or recover the CAs state. Further limiting HA or replication options.

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 in terms of features but did receive some minor bug fixes in Server 2016.

White Paper

Cogito Group

AD CS. The Good, Bad and Ugly

Not an Enterprise Database Product by Today's Standards

AD CS is based on the JET (or Jet) Blue Database. JET was the basis for many Microsoft products namely being the Database behind Microsoft Access. JET was originally released in 1992 and ceased active support from Microsoft as a separate product in 2004. While it has continued to be used in products such as AD CS, which is supported by Microsoft as part of their newer operating systems, it is no longer specified in newer products.

JET is not as robust as more modern server-based database products, particularly in multi-user scenarios. It lacks the locking mechanism required to serve multiple connections and has no deadlock resolution strategies.

The inability of JET to support multiple access could also be the reason behind the limitation of AD CS with regards to one CA per operating system instance.

Age of the product and the lack of regular or extensive updates is also a consideration here with many older products being far more capable than JET now.

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 becomes unresponsive and at 4 million it is effectively so slow as to be functionally stopped. A certificate within the AD CS system requires 32KB of disk space, and requires this block to be checked during every startup operation. A system with 4 million requires 128GB of certificates be sifted through on every system restart. 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.

AD CS. The Good, Bad and Ugly

There are also issues with an AD CS solution where there is a need for many CAs. AD CS is limited to only one CA per operating system, leaving the solution unable to scale. To take just one metric, the minimum memory for Windows Server 2022 operating with desktop experience is 2 Gigabytes (2GB). The throughput of AD CS is directly linked to the quantity of RAM available; Microsoft recommend a minimum deployment of 4GB. We would suggest that better performance is achieved with at least 8GB per server operating system running a single CA. In comparison Cogito's own Leviathan CA product has been tested to use 1.4GB with 100,000 CAs installed and running.

No Real Certifications for the CA platform

Microsoft has claimed that the product has certifications such as Common Criteria. This is based on the Operating System itself having Common Criteria certification. Microsoft has contended that because the capability is bundled in the Operating System this means that the certification extends to also accredit the AD CS CA platform. Microsoft's own Common Criteria certifications web page does not adequately describe the certification status of the AD CS product. Microsoft's own documentation on this page such as the Windows 11/10/Server 2022 Security Target references a the US Government NIAP Protection Profile for General Purpose Operating Systems v 4.2.1 not the more relevant Protection Profile for Certification Authorities v2.1. While a vendor must choose a protection profile lest they go through the same process multiple times, the fact is that AD CS is incapable of meeting the Certification Authorities protection profile requirements in some areas. An example is that it lacks support for the securely encrypted Full-Request syntax of the Certificate Management over Cryptographic Message Syntax (CMC) specification.

This gives the impression of being in a similar vein to claims by Microsoft of their Azure HSMs being FIPS 140-2 Level 3 'capable'. While it is certainly true that the HSMs they use are capable of Level 3, they operate them in FIPS 140-2 Level 2 compliance. Claiming NIST FIPS 140-2 Level 3 for services that operate at Level 2 is at best misleading.

One CA per Operating System

Each CA must be put on a separate Virtual Machine (VM). By contrast most other products are capable of operating multiple CAs per Operating System. At small scale this is not an issue but if the needs become more complex this can cause issues such as VM resourcing. AD CS has no support for containerization or Kubernetes deployments, further limiting the options for deployments at scale.

AD CS. The Good, Bad and Ugly

Limited Management Capabilities

ADCS is often paired with Certificate Lifecycle Management (CLM) software such as the Jellyfish Certificate Lifecycle Management capability simply because no native capability exists to interact with or discover issued certificates in a meaningful way. There is no search or report capability on certificates or on the devices or users they're issued to. The only two methods to search the certificate store is to scroll through the entries or attempt to query the JET database directly through a scripting language, making large volumes of certificates virtually impossible to search through without a substantial technical knowledge of the system. This can make key security enforcing functionality almost impossible to achieve without additional tools. A good example of this is it is extremely difficult to find and revoke a specific certificate with larger certificate numbers. There is no batch capabilities such as batch issuance or revocation, and certificate functions are only handled linearly with no asynchronous capability, making operations on large quantities of certificates time consuming.

Limited Automation Capabilities

AD CS has limited support for wider PKI protocols. Support includes AEP and NDES (a proprietary subset of the SCEP protocol). AD CS cannot support newer methods such as ACME, CMP, EST or API based requests. And the AD CS methods to replace values defined in a CSR is limited to CLI intervention, excluding many advanced features from inclusion in the industry standard CMC method for such operations. This severely limits the options for an AD CS CA to respond to and issue certificates to non-Microsoft based services or devices. Again options such as the Jellyfish Certificate Lifecycle Management capability are often used to overcome this limitation, but this reduces the two key advantages of AD CS being cost and simplicity.

Limited Registration Authority Capability in the Form of Network Device Enrolment Service (NDES)

While Network Device Enrolment Service (NDES) is considered by Microsoft to be a Registration Authority (RA), unlike other PKI products it is very limited in its RA capabilities. Cogito does not consider NDES to be an RA product, but rather just a SCEP agent to AD CS. The NDES implementation of SCEP is also so limited as to require additional software deployments to allow access for cloud platforms to access it's capabilities. One task Cogito would consider essential for an RA product is to maintain information about all requests received for processing by a CA. This gives two key advantages. The first is richer information about the registrations that have occurred to issue certificates, including information about the registrant itself. The second benefit of a true RA product is that on a failure of the CA itself, even if not all certificates issued can be recovered, the RA can provide information on what passed through it to determine what certificates were issued, but no longer appear in the CA's Database, allowing the risk around this loss to be better managed.

AD CS. The Good, Bad and Ugly

Limited Extensibility

AD CS has limited capacity to issue certificates through its Graphical Interface, only the ability to submit a Certificate Request (CSR) is available. However even CSR submission is limited only to CSRs that include the Microsoft specification for Certificate Template information. A common circumvention for this requirement is to submit the CSR using the CLI tool CertReq.

AD CS by default does not allow modifications typically performed by an Enrollment Agent during certificate submission. A common PKI operation required of a CA is to add additional Subject Alternative Name information to the request, an operation not supported by AD CS out of the box. AD CS does have the ability to enable this modification, but it is done through manual configuration of the Host Machine's Registry,however the enablement of these registry settings exposes the CA to security vulnerabilities. The CLI submission required to alter a certificate during submission is not protected by an Enrollment Agent certificate as is the industry standard for CSR modification.

Many facets of a CSR cannot be altered in any way by an AD CS CA, severely limiting the options for including information in a certificate not already embedded by the CSR's originator. A problem particularly notable when combined with the limited support for modern enrollment platforms, resulting in windows machines generating CSRs lacking information that is not possible to be appended by the CA.

Security Due to Common Deployment Methods

Due to the nature of the service being another role on a server and that it is often deployed by non-PKI experts, it is often deployed in ways that can cause security risks. An example is that AD CS is often deployed on existing services such as DCs. While this is convenient, it can cause a large risk to the organisation. Another issue is that AD CS and AD DS are codependent services. This can create a chicken or egg situation when deployed together. It creates the potential for an AD DS certificate expiring, preventing AD CS from issuing a replacement certificate.

Other common poor deployment methods involve:

- No segregation of the AD CS services from other services.
- Deployment without security enforcing capability such as HSMs. This makes a key security enforcing function within an environment open to relatively unsophisticated attacks.
- Deployment of a single Root and Issuing CA.
- Deployment of a Root CA that is not offline.

- Deployment of the service without good physical and logical controls and no enterprise grade support in place for backups, vulnerability management or updates in place. An example is Cogito still often find legacy implementations installed on a desktop server under an employee's desk.
- No backup or recovery strategy, or a strategy that does not account for the limitations of the JET database

Works Only on Windows Server Operating Systems

As a role of Windows Server, the platform can only be deployed on Windows Server operating systems and only one CA can be deployed per server. The key automatic enrolment protocol is a Microsoft proprietary protocol, not a standard based protocol, that is almost exclusively only supported on Microsoft platforms. This excludes many devices and applications. Further to this, to get the most out of AD CS it also needs to be deployed in Enterprise mode which requires a Microsoft AD Domain to store the certificate templates that will be used by AD CS.

AD CS is Not Currently Supported by Azure Key Vault

While this may change, AD CS uses the CNG (Crypto Next Generation)/KSP (Key Service Provider) API to access HSMs through a PKCS #11 compliant interface. Unfortunately, Azure Key Vault does not currently offer a PKCS #11 interface. This means that the far more expensive option of dedicated HSMs must be specified if the AD CS instance is to be used within Azure. This removes a key benefit around the cost effectiveness of the platform.

AD CS Does Not Support Cloud Platforms or a Multi-Cloud Strategy

Many organisations are moving or have moved to cloud services, and many have a multi-cloud strategy. AD CS was conceived well before cloud and does not provide good support for these strategies.

AD CS does not have native support for any of the Azure Cloud functionality. All cloud based interactions with AD CS are done through deployment of additional Microsoft Software such as the Certificate Connector for Microsoft Intune. The software Microsoft provides to solve cloud facing issues is a revolving door of different solutions and implementations as they try to solve the problems AD CS has with the modern cloud workspace.

Google Cloud Platform (GCP) will not support the deployment of AD CS that utilises the Google Cloud HSM as the Google Cloud HSM has the same issues as the Azure Key Vault in that it does not provide a PKCS#11 interface that can be utilised by the AD CS CA.

AWS will support the deployment of AD CS on an EC2 VM within their environment with a connection to a AWS Cloud HSM cluster. The AWS Cloud HSM cluster is hosted within a shared HSM

and keys are only accessible to the AWS tenant. You can add extra HSMs to the AWS Cloud HSM cluster within the same region or in a separate region up to a default maximum of 6 per region. The keys stored within the AWS Cloud HSM are non-exportable

None of the solutions offered by the major cloud vendors provide the ability to move between cloud providers without the requirement to create new CAs because you will not be able to transfer your keys.

Conclusion

AD CS is a good choice for what it was intended to do. That is to provide certificates in simple, small Microsoft only environments where budget is the overriding consideration. AD CS fails where it is pressed into service for more complex and larger deployments. Its simplicity in these environments encourages poor security choices and where it does not have the flexibility and capability to meet a diverse range of requirements, where availability, reliability, scale, and non-Microsoft product support are considerations.

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.

Cogito specifically developed the Jellyfish Certificate Lifecycle Management capability as part of the wider Jellyfish platform to address some of the limitations of the Microsoft AD CS platform. Later, Cogito also developed Leviathan CA to overcome the remaining issues around scale, reliability and product support issues of the AD CS platform.