

CERTIFICATE SERVICES (AD CS).



Active Directory Certificate Services issues credentials for users, devices, and services. **Protect who can obtain a certificate, which identity it represents, and where its private key can be used.**

- CERTIFICATE TEMPLATE PERMISSIONS
- ENROLLMENT RELAY DEFENSE
- STRONG IDENTITY MAPPING
- REVOCATION READINESS

01 THE MECHANISM

Templates Define Issuance

Enterprise certification authorities (CAs) use templates stored in Active Directory to set enrollment rules, allowed uses, and identity fields. **Enrollment rights and permission to edit a template are different powers.** Review both, plus approvals and publication.

The Private Key Proves Possession

A certificate binds a public key to an identity; authentication requires proof using the corresponding private key. **The public certificate alone is not the secret.** Protect private keys on endpoints and the CA signing keys behind trust.

Valid Issuance Can Be Abused

Weak templates or enrollment protections can produce certificates an attacker controls. **A valid CA signature does not prove the request was legitimate.** Authentication also depends on permitted use, trust, validity, revocation, and account mapping.

02 THE FLOW

The Intended Certificate Lifecycle

EXPECTED

1

Request: an authorized client submits a public key and enrollment request. The template limits who may enroll and how identity is established.

2

Issue: the CA checks enrollment permissions, template policy, and required approvals, then signs a certificate for the validated identity and key.

3

Authenticate: the client proves private-key possession. The verifier checks certificate policy and account mapping; the application applies its access rules.

The Enrollment Relay Attack Path

ABUSED

1

An attacker relays a victim's NTLM authentication to an **unprotected web enrollment endpoint** that accepts it. This is the ESC8 attack class.

2

If the victim may enroll in a suitable authentication template, the CA can issue a certificate **for that victim using an attacker-controlled key.**

3

The attacker uses the certificate and private key to authenticate as the victim **where validation and mapping accept it.** The victim's privileges determine the reach.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Template Governance	Limit enrollment and write permissions; remove unused published templates. Review authentication uses, subject-name rules, and approval requirements.
Enrollment Protection	Require HTTPS and Extended Protection for Authentication (EPA) on web enrollment; retire unnecessary endpoints and NTLM. Require RPC packet privacy.
CA & Key Protection	Treat CA administration as highly privileged. Protect signing keys, backups, and host access; use appropriate hardware protection and separate roles.
Mapping & Revocation	Verify strong certificate-to-account mapping on domain controllers. Maintain certificate revocation lists (CRLs), status services, and tested recovery procedures.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Template Scans Only	No	Finds risky settings, but not every stolen key or abuse of an otherwise legitimate enrollment path.
Enrollment Counts Only	No	Normal autoenrollment creates volume; one malicious request can be enough. Counts lack identity and template context.
CA Logs Only	No	Shows recorded issuance, but not all endpoint key theft or later authentication. Off-CA forgery may bypass the issuance log.
Endpoint Alerts Only	No	Covers observed host behavior but can miss template changes, enrollment relay, and certificates used from elsewhere.
PKI + Identity Correlation	No	Join issuance, template changes, and authentication. Check coverage and investigate context; no single signal proves or excludes abuse.

CERTIFICATE SERVICES (AD CS).

CONSTRAIN · VERIFY · REVOKE

05

PROGRAM OPERATIONS

Inventory the full issuance path.

Assign owners to CAs, templates, enrollment services, and relying applications. Record certificate purpose, lifetime, renewal, and private-key protection.

Collect and correlate CA auditing.

Track requests (4886), issuance (4887), and template changes (4899/4900). Join requester, template, serial number, and subsequent authentication where available.

Validate hardening with real clients.

Test EPA, RPC privacy, template restrictions, and strong mapping against required enrollment and sign-in flows; retire exceptions with an owner and deadline.

Contain issuance and certificate use.

Stop the abused path, preserve evidence, revoke affected certificates, and publish fresh revocation data. Verify relying-party behavior and terminate affected sessions separately.

06

CONTROL MAPPING

ESC1 / ESC4

Template identity and permissions: constrain supplied identities, authentication purposes, enrollment rights, and who can change template policy.

ESC8 / ESC11

Enrollment relay defenses: HTTPS plus required EPA for web enrollment; enforced packet privacy for RPC enrollment.

KB5014754

Strong certificate mapping: validate certificates against the intended account using supported strong mappings, rather than trusting a supplied name alone.

ATT&CK T1649

Authentication certificate theft or forgery: secure private keys and CA infrastructure; correlate abnormal enrollment, key access, and certificate use.

07

WHAT THIS DOES NOT SOLVE

Compromised Endpoints

A protected CA does not stop abuse of a **private key** or **active session** on a compromised client.

CA Signing-Key Exposure

A stolen signing key can enable **forgery outside normal issuance**. Recovery must address CA trust, not only a single leaf certificate.

Revocation Delays

Publishing a CRL does not make every verifier update instantly. **Caching and status-check behavior** affect containment.

Excessive Access

Correct authentication does not fix **overbroad application or directory permissions** granted to the authenticated account.

08

MYTHS VS. REALITY

MYTH

“Resetting the password revokes its certificates.”

REALITY

A password reset does not invalidate a separate certificate credential. **Revoke affected certificates and address active sessions** as part of containment.

MYTH

“HTTPS alone prevents enrollment relay.”

REALITY

TLS encrypts the connection. **Required EPA provides the additional relay protection**; also remove unnecessary NTLM and enrollment services.

MYTH

“Fixing a template cancels old certificates.”

REALITY

A template change governs issuance policy. **Previously issued certificates need separate review and revocation** where they remain dangerous.

MYTH

“A trusted certificate proves legitimate enrollment.”

REALITY

The CA signature proves who signed the certificate. **A misconfigured or relayed request can still obtain a valid signature**.

MYTH

“Strong mapping makes every AD CS path safe.”

REALITY

Mapping binds a certificate to an account. **It does not repair compromised keys, CA administration, or every enrollment path**.

09

SPEAK THE PROGRAM — KEY TERMS

CA

A **certification authority** signs certificates. Its key and the trust placed in it underpin certificate acceptance.

CERTIFICATE TEMPLATE

An enterprise CA policy defining **enrollment permissions, certificate purpose, identity fields, and issuance requirements**.

EKU & SAN

Extended Key Usage identifies allowed purposes; **Subject Alternative Name** carries names. Neither replaces secure account mapping.

EPA

Extended Protection for Authentication binds authentication to the intended service or channel to resist relay attacks.

STRONG MAPPING

A secure association between a certificate and an account, such as a **validated SID binding or explicit strong mapping**.

CRL & OCSP

A **Certificate Revocation List** lists revoked certificates; **Online Certificate Status Protocol** provides certificate-status responses.