TRUVALD · ADCS SECURITY

Twenty-five years.

Why the default certificate templates in every ADCS install are the foundation of most ESC findings.

That's how long the default certificate templates on your ADCS install have been frozen at schema V1. User, Computer, WebServer, Smartcard Logon, Domain Controller, most of them. Defined for Windows 2000, unchanged since, and you cannot modify them. Permissions, EKUs, cryptographic options, all locked in amber.

Quick version timeline for reference:

- **V1** — Windows 2000 / Server 2003 Standard
- **V2** — Windows Server 2003 Enterprise (editable, still legacy crypto)
- **V3** — Windows Server 2008 (CNG, SHA-2, ECC)
- **V4** — Windows Server 2012 (key attestation, renewal with same key)

The screenshot below is from a real ADCS forest. Count the schema versions. Most of what ships in the box is still V1.

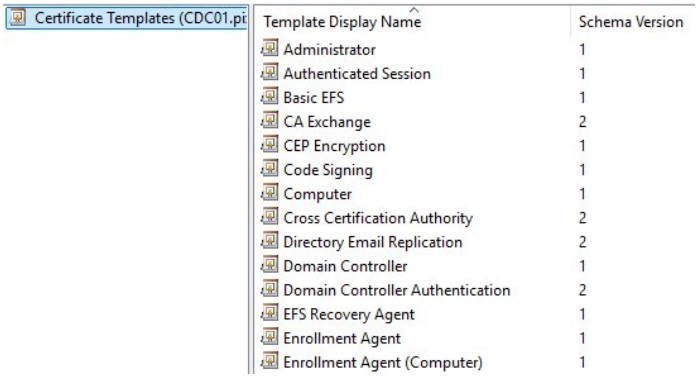

Figure 1. Certificate Templates console. Most defaults remain at schema V1.

When security folks say "don't use the default templates," they're not being fussy. They mean the schema itself is the problem. ESC15, the EKUwu attack, works specifically because V1 templates don't enforce the constraints later versions do. A WebServer certificate becomes a client-auth certificate with nothing more than enrollment rights. The template can't defend against it because the V1 schema doesn't have the field newer versions use to lock it down.

The fix isn't complicated. Duplicate. V4 ideally, V3 minimum. Then harden the duplicate.

The defaults were always the starting point. They were never the answer.

So, when's the last time you actually checked which default templates are still published on your CAs?

From the field

Most environments still publish at least three or four default templates. Usually User, Computer, Web Server, and Workstation Authentication. Sometimes Domain Controller. Always for a "reason" that nobody on the current team remembers. The pattern is consistent enough across PKI assessments that it has become a starting-line checklist item. Nobody publishes them on purpose. They just never get cleaned up.