Szablony, automatyczna rejestracja i silne mapowanie certyfikatów

Poziom: zaawansowany

Dotyczy: AD CS (CA-Zielona na dc01, docelowo Zielona-CA01 na ca01), szablony w wersji Windows Server 2016, GPO automatycznej rejestracji, Windows 11, NPS, Certificate Connector na conn01, KB5014754 w stanie na październik 2026

Czas: ~60 min

Szablon mówi urzędowi, komu i jaki certyfikat wolno wydać, a automatyczna rejestracja sprawia, że komputery i użytkownicy dostają go i odnawiają bez naszego udziału. Od lutego 2025 roku kontroler domeny przyjmuje do logowania tylko certyfikaty silnie powiązane z kontem, więc źle zaprojektowany szablon przestaje być tylko ryzykiem, a staje się awarią. Wracamy tu przy każdym nowym rodzaju certyfikatu, przy przenosinach urzędu i gdy NPS zaczyna odrzucać laptopy.

ZAŁOŻENIA SCENARIUSZA

komputery biura i laptopy handlowców są w domenie `ad.zielona.example`, część z nich także w Intune. NPS dla Wi-Fi i VPN stoi dziś na `dc02`, docelowo na `nps01` i `nps02` (propozycja z planu segmentacji); szablon `ZielonaNPS` działa tak samo w obu miejscach. Do czasu przenosin szablony publikujemy na `CA-Zielona`, a nazwy techniczne zostają te same na `ca01`.

Skróty użyte na tej stronie (24)

Skrót	Co znaczy
ACME	Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

Skrót	Co znaczy
EAP-TLS	EAP z TLS: uwierzytelnianie certyfikatem użytkownika albo urządzenia zamiast hasła
EJBCA	Enterprise JavaBeans Certificate Authority: otwarty urząd certyfikacji firmy Keyfactor z interfejsem WWW i obsługą wielu protokołów rejestracji, wersja Community bezpłatna
EKU	Extended Key Usage: pole w certyfikacie mówiące, do czego wolno go używać, na przykład wyłącznie do uwierzytelniania serwera
ESC	Escalation (numeracja SpecterOps): oznaczenie znanych dróg od zwykłego konta do przejęcia domeny przez źle ustawione AD CS, od ESC1 do ESC16
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
LDAPS	LDAP szyfrowany TLS, zwykle port 636
NPS	Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi
NTAuth	magazyn NTAuth (NT Authentication): lista urzędów w konfiguracji lasu AD, których certyfikaty mogą służyć do logowania do domeny
PKCS	Public Key Cryptography Standards: rodzina standardów kryptograficznych, tu chodzi o profil certyfikatu importowanego razem z gotowym kluczem prywatnym
RPC	Remote Procedure Call: sposób, w jaki programy wywołują funkcje na innym komputerze w sieci; kontrolery domeny używają go między innymi do replikacji
SCEP	Simple Certificate Enrollment Protocol: protokół, którym urządzenie samo prosi urząd certyfikacji o wystawienie certyfikatu
SHA1	starsza, dziś uznawana za słabą funkcja skrótu kryptograficznego
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta
SKI	Subject Key Identifier: skrót klucza publicznego zapisany w certyfikacie, jeden z silnych sposobów powiązania certyfikatu z kontem w altSecurityIdentities
TPM	Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów
UPN	User Principal Name: login w formie adresu, np. jan.nowak@zielona.example
URI	ogólny adres zasobu w internecie, część adresu URL bez samej domeny
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii

Fiszka

Polecenia `Add-CATemplate`, `Remove-CATemplate` i `Get-CATemplate` wykonujemy w PowerShellu na serwerze urzędu kontem z prawem zarządzania urzędem (CA Administrator). Szablony duplikujemy

i zmieniamy w konsoli `certtmpl.msc` kontem z grupy `GG_PKI_Szablony`, a polecenia po stronie klienta na komputerze albo jako użytkownik.

TYLKO ODCZYT

Lista szablonów opublikowanych na urzędzie: Get-CATemplate

```
Get-CATemplate | Format-Table Name, DisplayName, Oid
```

Pokazuje tylko szablony, które ten urząd wydaje. Szablon istnieje w lesie raz, a każdy urząd sam decyduje, czy go publikuje.

Przykład (skrót):

```
Name                      DisplayName
----                      -----------
ZielonaWWW                Zielona WWW (serwery)
ZielonaUzytkownik-Intune  Zielona uzytkownik Intune
WebServer                 Web Server
Machine                   Computer
```

Wiersze `WebServer` i `Machine` to szablony domyślne w wersji 1, które kreator opublikował przy instalacji `CA-Zielona`. Zastępujemy je kopiami i zdejmujemy z urzędu.

TYLKO ODCZYT

Duplikowanie szablonu: konsola Certificate Templates

```
certtmpl.msc → prawy przycisk na szablonie źródłowym (np. Computer) → Duplicate Template
→ Compatibility: Certification Authority Windows Server 2016, Certificate recipient
Windows 10 / Windows Server 2016
→ General: Template display name „Zielona Komputer”, nazwa techniczna ZielonaKomputer,
Validity period 1 year, Renewal period 6 weeks
→ Cryptography: Key Storage Provider, RSA 2048, wybrane dostawcy: Microsoft Platform
Crypto Provider, Microsoft Software Key Storage Provider
→ Subject Name: Build from this Active Directory information, DNS name
→ Security: Domain Computers: Read, Enroll, Autoenroll
→ Superseded Templates: Computer, Workstation Authentication
```

Kopia dostaje numer wersji schematu 4, więc nie dotyczy jej ESC15 (szablony w wersji 1 z nazwą w żądaniu). Pola „nazwa techniczna” (Template name) nie da się zmienić po

utworzeniu, więc wpisujemy ją bez spacji i polskich znaków od razu.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: okno Properties of New Template, zakładka Subject Name z zaznaczonym Build from this Active Directory information i polem DNS name, a w tle lista szablonów z ZielonaKomputer.

◫ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

◫ ZMIENIA SYSTEM

Publikacja szablonu na urzędzie: Add-CATemplate

```
Add-CATemplate -Name "NazwaSzablonu" -Force
```

Od tej chwili urząd wydaje certyfikaty z tego szablonu każdemu, kto ma do niego prawo Enroll. Kopiowanie szablonu nic nie zmienia, dopóki go nie opublikujemy, więc szablon możemy spokojnie przygotować dzień wcześniej.

◫ ZMIENIA SYSTEM

Zdjęcie szablonu z urzędu: Remove-CATemplate

```
Remove-CATemplate -Name "NazwaSzablonu" -Force
```

Urząd przestaje wydawać certyfikaty z tego szablonu, ale już wydane działają do końca ważności. Tak wycofujemy szablony domyślne w wersji 1 i tak, przy przenosinach, przełączamy wydawanie ze starego urzędu na nowy.

◫ ZMIENIA SYSTEM

Włączenie automatycznej rejestracji w GPO: Certificate Services Client - Auto-Enrollment

```
gpmc.msc → GPO „Zielona Certyfikaty” podłączone do domeny
→ Computer Configuration → Policies → Windows Settings → Security Settings → Public Key Policies
→ Certificate Services Client - Auto-Enrollment → Configuration Model: Enabled
```

```
→ zaznaczone: Renew expired certificates, update pending certificates, and remove
revoked certificates
→ zaznaczone: Update certificates that use certificate templates
→ to samo w User Configuration → Policies → Windows Settings → Security Settings →
Public Key Policies
```

Jedno GPO dla komputerów i użytkowników. Samo GPO nie wydaje niczego: komputer albo użytkownik dostanie certyfikat tylko z szablonu, w którym ma prawo Autoenroll.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

ZMIENIA SYSTEM

Wymuszenie automatycznej rejestracji: certutil -pulse

```
gpupdate /force
certutil -pulse
certutil -pulse -user
```

Komputer domyślnie sprawdza szablony przy starcie i co osiem godzin. `certutil -pulse` uruchamia sprawdzenie od razu dla komputera, a z `-user` dla zalogowanego użytkownika.

gpupdate = group policy update: wymuś odświeżenie GPO · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

ZMIENIA SYSTEM

Ręczna rejestracja komputera z szablonu: certreq -enroll

```
certreq -enroll -machine -q NazwaSzablonu
```

Komputer prosi urząd o certyfikat z podanego szablonu bez kreatora. Używamy przy serwerach, którym nie chcemy dawać prawa Autoenroll, na przykład przy pierwszym certyfikacie NPS.

Przykład:

```
Active Directory Enrollment Policy
  {9D5C2B7A-...}
  ldap:
```

```
Request ID: 1187
Certificate retrieved(Issued) Issued
```

NPS = Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi · **certreq** = narzędzie Windows do tworzenia i wysyłania żądań certyfikatów (CSR) do CA

TYLKO ODCZYT

Sprawdzenie certyfikatów komputera z szablonem: Get-ChildItem Cert:\LocalMachine\My

```
Get-ChildItem Cert:\LocalMachine\My | Select-Object Subject, Issuer, NotAfter,
@{n='Szablon';e={($_.Extensions | Where-Object { $_.Oid.Value -eq '1.3.6.1.4.1.311.21.7'
}).Format(0)}}
```

Wypisuje certyfikaty komputera z wystawcą, datą wygaśnięcia i informacją o szablonie, z którego pochodzą (rozszerzenie `1.3.6.1.4.1.311.21.7`).

Przykład (skrót):

```
Subject  : CN=ws-ksiegowosc01.ad.zielona.example
Issuer   : CN=CA-Zielona, DC=ad, DC=zielona, DC=example
NotAfter : 14.11.2027 08:12:40
Szablon  : Template=Zielona Komputer(1.3.6.1.4.1.311.21.8....), Major Version
Number=100, Minor Version Number=2
```

TYLKO ODCZYT

Sprawdzenie rozszerzenia SID w certyfikacie: certutil -dump

```
certutil -dump NazwaPliku.cer | Select-String -Pattern "1.3.6.1.4.1.311.25.2" -Context
0,3
```

Rozszerzenie z identyfikatorem `1.3.6.1.4.1.311.25.2` niesie SID konta, dla którego wydano certyfikat. Urząd Enterprise dodaje je sam do certyfikatów z szablonów, w których nazwa pochodzi z Active Directory. Brak wyniku przy certyfikacie do logowania oznacza, że kontroler odrzuci go, chyba że konto ma silne mapowanie jawne.

SID = w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii

poleceń

□□ TYLKO ODCZYT

Zdarzenia silnego mapowania na kontrolerze: Get-WinEvent 39, 40, 41

```
Get-WinEvent -ComputerName NazwaKontroleraDC -FilterHashtable @{LogName='System';
ProviderName='Microsoft-Windows-Kerberos-Key-Distribution-Center'; Id=39,40,41} -
MaxEvents 50 -ErrorAction SilentlyContinue | Select-Object TimeCreated, Id, Message
```

Zdarzenie 39 oznacza certyfikat, którego nie da się silnie powiązać z kontem, a 41 certyfikat z SID innego konta; w trybie pełnego wymuszania oba to odrzucone logowanie. Zdarzenie 40 (certyfikat starszy niż konto) KB5014754 opisuje dla trybu zgodności, którego od 9 września 2025 nie da się włączyć, więc dziś spodziewamy się głównie 39 i 41. Dokumentacja podaje źródło zdarzeń jako `Kdcsvc`, więc nazwę dostawcy sprawdzamy w podglądzie zdarzeń na naszym kontrolerze.

□□ **SID** = w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta

□□ ZMIENIA SYSTEM

Silne mapowanie jawne dla certyfikatu bez SID: Set-ADUser altSecurityIdentities

```
Set-ADUser -Identity nazwa_usera -Add
@{altSecurityIdentities="X509:<I>NazwaWystawcy<SR>NumerSeryjny"}
```

> (gdzie `NazwaWystawcy` to nazwa urzędu w odwróconej kolejności, na przykład `DC=example,DC=zielona,DC=ad,CN=CA-Zielona`, a `NumerSeryjny` to numer seryjny certyfikatu; przykłady administratorów i KB5014754 pokazują numer w odwróconej kolejności bajtów, więc sprawdzamy wpis na koncie testowym!)

Wiąże konkretny certyfikat z kontem typem `X509IssuerSerialNumber`, który Microsoft uznaje za silny. Używamy tylko dla pojedynczych wyjątków, na przykład certyfikatu z urządzenia, które nie umie przyjąć rozszerzenia SID.

□□ **SID** = w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników · **CN** =

Common Name: główna nazwa w certyfikacie, np. adres serwera

KLIKAMY W INTERFEJSIE

Wymiana certyfikatów na wszystkich komputerach: Reenroll All Certificate Holders

```
certtmpl.msc → prawy przycisk na szablonie (np. ZielonaKomputer) → Reenroll All Certificate Holders
```

Podnosi główny numer wersji szablonu, więc przy najbliższej automatycznej rejestracji każdy posiadacz certyfikatu z tego szablonu prosi o nowy, nawet jeśli stary jest jeszcze długo ważny. Używamy po zmianie szablonu i przy przenosinach na nowy urząd, zawsze najpierw na grupie pilotażowej.

Z życia wzięte

Z ŻYCIA WZIĘTE

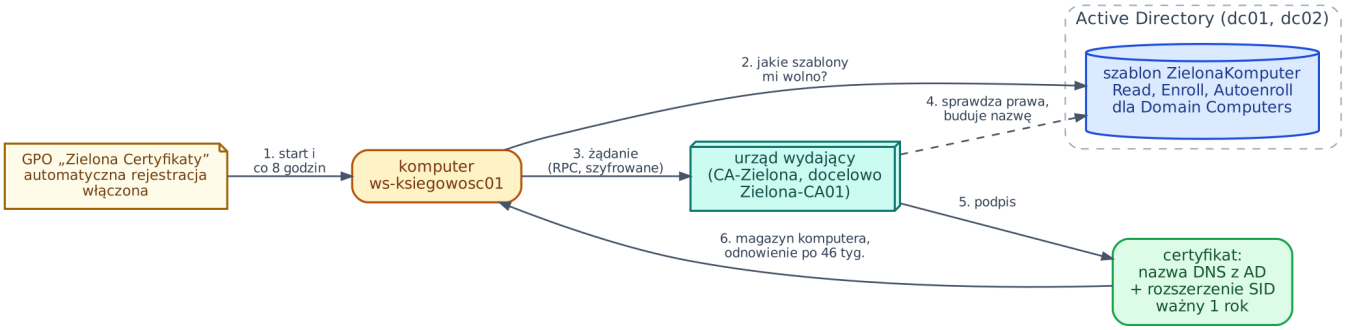
Poniedziałek, 7:40, luty 2025. Pięć laptopów magazynu w Swarzędzu nie łączy się z Wi-Fi, a Marek dzwoni, że skanery „widzą sieć, a laptopy nie”. W dzienniku `dc02` są zdarzenia 39: certyfikaty komputerów pochodzą z szablonu, który ktoś przed laty ustawił na nazwę podawaną w żądaniu, żeby wystawiać je ręcznie, więc nie mają rozszerzenia SID. Wtorkowa aktualizacja kontrolerów włączyła pełne wymuszanie i NPS przestał przyjmować te certyfikaty. Tomek publikuje szablon `ZielonaKomputer` z nazwą z Active Directory, a po `certutil -pulse` laptopy wracają do sieci przed przerwą śniadaniową.

Jak to działa

Rozwiń: jak to działa pod spodem

Szablon, uprawnienie, GPO: trzy klucze do certyfikatu

Komputer dostaje certyfikat automatycznie tylko wtedy, gdy spełnione są trzy warunki: GPO włącza automatyczną rejestrację, szablon jest opublikowany na urzędzie, a konto komputera (albo jego grupa) ma w szablonie prawa Read, Enroll i Autoenroll. Brak któregokolwiek oznacza ciszę: żadnego błędu, po prostu brak certyfikatu.



Rysunek 1. Automatyczna rejestracja w Zielonej: GPO włącza klienta rejestracji, komputer czyta z AD szablony i swoje uprawnienia, wysyła żądanie do urzędu przez RPC, urząd buduje nazwę z AD, dodaje rozszerzenie SID i odsyła certyfikat, a komputer odnawia go sam po 46 tygodniach (kliknięcie otwiera pełny rozmiar)

Pojęcie: szablon certyfikatu. Obiekt w konfiguracji lasu, który opisuje rodzaj certyfikatu: do czego służy (EKU), skąd bierze nazwę, jak długo jest ważny, jaki klucz ma mieć i kto może o niego prosić. Szablony w wersji 1 (domyślne, wbudowane) nie dają się zmieniać; zawsze pracujemy na ich kopiach.

Pojęcie: automatyczna rejestracja (autoenrollment). Usługa Windows, która przy starcie i co osiem godzin sprawdza, do których szablonów komputer albo użytkownik ma prawo Autoenroll, i sama prosi o brakujące albo kończące się certyfikaty. Działa tylko w domenie, z łącznością do kontrolera i urzędu, dlatego laptopy poza biurem dostają certyfikaty z Intune.

Szablony Zielonej

Szablon (nazwa techniczna)	Kopia szablonu	Dla kogo	Nazwa podmiotu	Zastosowanie (EKU)	Ważność	Jak trafia

`ZielonaKomputer`	Computer	grupa Domain Computers	z AD, nazwa DNS	uwierzytelnianie klienta i serwera	1 rok	automatycznie
`ZielonaKontroler`	Kerberos Authentication	grupa Domain Controllers	z AD, nazwa DNS i domena	klient, serwer, logowanie kartą, uwierzytelnianie KDC	1 rok	automatycznie, zastępuje Domain Controller, Domain Controller Authentication i Kerberos Authentication
`ZielonaNPS`	RAS and IAS Server	grupa RAS and IAS Servers	z AD, nazwa DNS	klient i serwer	1 rok	automatycznie na serwerach NPS
`ZielonaUzytkownik`	User	grupy `GG_VPN_Uzytkownicy` i `GG_WiFi_Uzytkownicy`	z AD, UPN w SAN	uwierzytelnianie klienta	1 rok	automatycznie na komputerach w biurze
`ZielonaUzytkownik-Intune`	User	tylko konto komputera `conn01$`	w żądaniu	uwierzytelnianie klienta	1 rok	profil PKCS w Intune
`ZielonaWWW`	Web Server	grupa `GG_PKI_Wnioskodawcy` (administratorzy)	w żądaniu, z zatwierdzeniem menedżera	tylko uwierzytelnianie serwera	1 rok	ręcznie: `certreq`, OpenSSL

Zasady, które łączą wszystkie szablony:

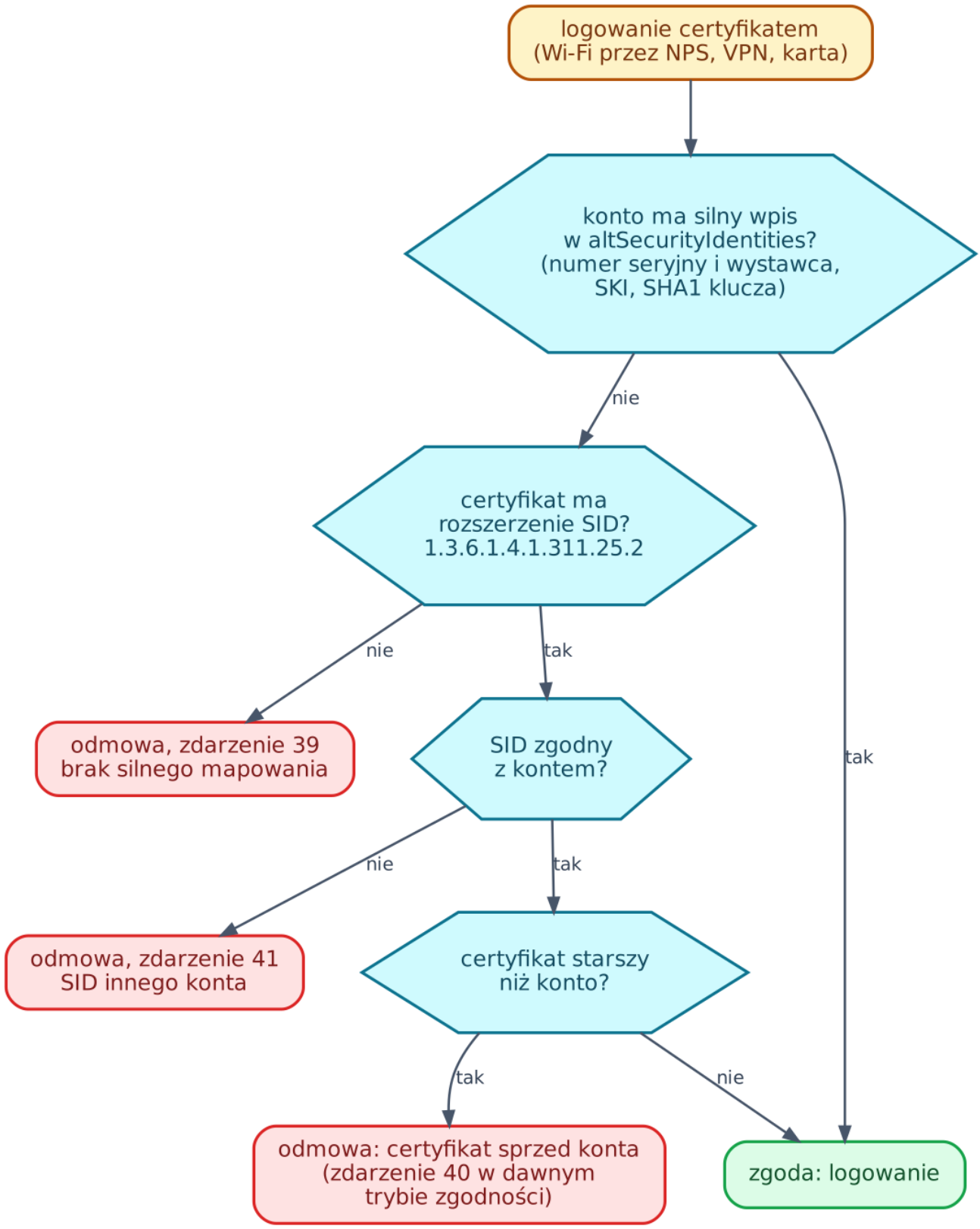
1. Nazwa z Active Directory wszędzie, gdzie się da. Tylko takie certyfikaty dostają rozszerzenie SID automatycznie.
2. Nazwa w żądaniu tylko z jednym zastosowaniem: uwierzytelnianie serwera. Szablon z nazwą w żądaniu i uwierzytelnianiem klienta to ESC1, chyba że prawo Enroll ma wyłącznie jedno konto techniczne (jak `conn01$`) i to konto jest w warstwie 0.
3. Prawa Enroll i Autoenroll dla grup, nigdy dla Authenticated Users ani Domain Users w szablonach do logowania.
4. Klucz komputera w TPM, gdy komputer go ma (Microsoft Platform Crypto Provider), z możliwością zapasowego dostawcy programowego dla maszyn wirtualnych bez wirtualnego TPM.
5. Odnowienie na 6 tygodni przed końcem, żeby urlop ani zakaz zmian nie zostawiły nikogo bez certyfikatu.

Szablon `ZielonaWWW` istnieje już na `CA-Zielona` i opisuje go strona Generowanie certyfikatów: OpenSSL i urząd certyfikacji Windows, a `ZielonaUzytkownik-Intune` strona Certyfikaty, Wi-Fi i VPN z Intune: Certificate Connector czy Cloud PKI.

Silne mapowanie certyfikatów: co zmieniło KB5014754

Gdy ktoś loguje się certyfikatem (Wi-Fi z EAP-TLS przez NPS, VPN, karta, Windows Hello z certyfikatem), kontroler domeny musi ustalić, do którego konta należy certyfikat. Przez lata wystarczało, że w certyfikacie była nazwa UPN albo DNS pasująca do konta. W 2022 roku pokazano, że to za mało: kto mógł zmienić UPN albo nazwę DNS swojego konta komputera, mógł dostać certyfikat, który kontroler uznawał za certyfikat kontrolera domeny (CVE-2022-26923, zwane Certifried).

> **Pojęcie: silne mapowanie.** Powiązanie certyfikatu z kontem, którego nie da się podrobić zmianą nazwy. Microsoft uznaje za silne: rozszerzenie SID w certyfikacie albo jawny wpis w atrybucie `altSecurityIdentities` konta typu numer seryjny z wystawcą, identyfikator klucza (SKI) albo skrót SHA1 klucza publicznego. Słabe są wpisy oparte tylko na nazwie podmiotu albo adresie e-mail.



Rysunek 2. Jak kontroler domeny decyduje o certyfikacie w trybie pełnego wymuszania: najpierw szuka silnego mapowania jawnego w altSecurityIdentities, potem rozszerzenia SID; SID

zgodny z kontem i certyfikat młodszy niż konto dają zgodę, SID innego konta zdarzenie 41 i odmowę, brak obu zdarzenie 39 i odmowę (kliknięcie otwiera pełny rozmiar)

Data	Co się stało
10 maja 2022	poprawki dla CVE-2022-26923 i CVE-2022-26931: urzędy Enterprise zaczynają dodawać rozszerzenie SID, kontrolery w trybie zgodności (zdarzenia ostrzegawcze)
11 kwietnia 2023	koniec możliwości wyłączenia mechanizmu
11 lutego 2025	kontrolery bez ustawionego klucza rejestru przechodzą w pełne wymuszanie
9 września 2025	koniec obsługi klucza `StrongCertificateBindingEnforcement`: trybu zgodności nie da się już włączyć
październik 2026	stan obecny: każdy kontroler z bieżącymi poprawkami odrzuca certyfikaty bez silnego mapowania; w dzienniku zmian KB nie ma nowych wpisów z 2026 roku

Dla Zielonej oznacza to trzy sprawdzenia, które robimy przed każdym nowym szablonem do logowania i po każdych przenosinach:

1. Certyfikat ma rozszerzenie `1.3.6.1.4.1.311.25.2` (fiszka z `certutil -dump`), albo konto ma silne mapowanie jawne.
2. Konto istniało przed wydaniem certyfikatu: po odtworzeniu konta z kosza albo po założeniu konta od nowa wydajemy nowy certyfikat.
3. Na urzędzie nie ma wyłączonego rozszerzenia SID (`DisableExtensionList`, ESC16) ani szablonów z flagą `CT_FLAG_NO_SECURITY_EXTENSION` (ESC9), co sprawdza strona o hartowaniu.

Certyfikaty z Intune dostają SID inaczej: SCEP przez zmienną `{{OnPremisesSecurityIdentifier}}` w polu URI, a PKCS przez wpis `EnableSidSecurityExtension` na serwerze łącznika. Obie drogy opisuje strona o Intune; w październiku 2026 to wciąż jedyne miejsca, w których certyfikat do logowania powstaje z nazwą podawaną w żądaniu i nadal przechodzi przez kontroler.

Droga bez Microsoftu

Bez domeny Windows nie ma ani szablonów, ani magazynu NTAuth, ani silnego mapowania w tym sensie. Odpowiednik szablonu to zasady urzędu (w step-ca: provisionery z ograniczeniami nazw i czasu ważności, w EJBCA: profile certyfikatu i profile podmiotu), a odpowiednik automatycznej rejestracji to klient, który sam prosi i odnawia.

Zadanie	Droga Microsoftu	Droga bez Microsoftu

certyfikat komputera w biurze	szablon `ZielonaKomputer` i GPO	MDM z profilem SCEP (np. do step-ca albo EJBCA)
certyfikat serwera linuksowego	`certreq` z OpenSSL, szablon `ZielonaWWW`	`certmonger` z FreeIPA na `ipa01` albo klient ACME do step-ca
certyfikat użytkownika do Wi-Fi	szablon `ZielonaUzytkownik` albo profil PKCS z Intune	profil SCEP z MDM, a RADIUS (FreeRADIUS) sprawdza pola certyfikatu według własnych reguł
powiązanie certyfikatu z kontem	rozszerzenie SID, `altSecurityIdentities`	reguła RADIUS albo aplikacji: UPN, adres e-mail albo identyfikator z katalogu (LDAP, Keycloak), a ochrona przed podmianą nazwy leży po stronie urzędu, który nie pozwala wnioskodawcy wpisać dowolnej nazwy

Częste błędy

Objaw	Przyczyna	Co robimy
Komputer nie dostaje certyfikatu, brak błędów	brak prawa Autoenroll w szablonie, szablon nieopublikowany albo GPO niepodłączone	`Get-CATemplate` na urzędzie, zakładka Security szablonu, `gpresult /r` na komputerze, dziennik Application, źródło CertificateServicesClient-AutoEnrollment
NPS odrzuca certyfikat, na kontrolerze zdarzenie 39	certyfikat bez rozszerzenia SID: szablon z nazwą w żądaniu albo wydany przed majem 2022	szablon z nazwą z AD i `Reenroll All Certificate Holders`; dla wyjątku `altSecurityIdentities`
Odmowa logowania certyfikatem po odtworzeniu albo ponownym założeniu konta	certyfikat starszy niż obiekt konta	nowy certyfikat dla odtworzonego konta (`certutil -pulse -user` po zalogowaniu)
Certyfikat z `ZielonaWWW` ma tylko CN, bez SAN	wniosek bez SAN albo szablon budujący nazwę z AD	wniosek z `san.cnf` albo `request.inf` z SAN, sprawdzenie `certutil -dump` przed wdrożeniem
Po zmianie szablonu stare certyfikaty dalej mają stare ustawienia	zmiana szablonu działa tylko na nowe wnioski	`Reenroll All Certificate Holders` po pilotażu
Komputery mają po dwa certyfikaty, z `Machine` i z `ZielonaKomputer`	szablon nie zastępuje starego (Superseded Templates)	dopisujemy stare szablony w zakładce Superseded Templates, stare zdejmujemy z urzędu
Laptop w terenie od miesięcy bez nowego certyfikatu	automatyczna rejestracja wymaga łączności z urzędem	certyfikat z Intune (PKCS albo SCEP) dla urządzeń, które rzadko widzą biuro

Ćwiczenia

1. Ola prosi o szablon, w którym jej zespół sam wpisze nazwę serwera i dostanie certyfikat „do wszystkiego”, bo tak szybciej. Co odpowiadamy i co proponujemy?

Odpowiedź

Szablon z nazwą w żądaniu i szerokim zastosowaniem (uwierzytelnianie klienta albo Any Purpose) to ESC1 i ESC2: pozwala wystawić certyfikat na dowolne konto, także administratora. Proponujemy `ZielonaWWW` (tylko uwierzytelnianie serwera, zatwierdzenie menedżera) albo, dla serwerów linuksowych zespołu, ACME z `acme01` ograniczonym do nazw `*.zielona.example`.

1. Po wtorkowych poprawkach w lutym 2025 Wi-Fi magazynu przestało działać tylko dla laptopów z certyfikatem sprzed 2022 roku. Dlaczego akurat dla nich?

Odpowiedź

Certyfikaty wydane przed poprawkami z maja 2022 roku nie mają rozszerzenia SID, bo urząd zaczął je dodawać dopiero po aktualizacji. Pełne wymuszanie od 11 lutego 2025 roku odrzuca je przy braku silnego mapowania jawnego. Nowsze certyfikaty z szablonów z nazwą z AD mają SID i przechodzą.

1. Dlaczego szablon `ZielonaUzytkownik-Intune` z nazwą w żądaniu i uwierzytelnianiem klienta nie jest ESC1 w rozumieniu Zielonej, a ten sam szablon z prawem Enroll dla Domain Users byłby?

Odpowiedź

Prawo Enroll ma tylko konto komputera `conn01$`, a `conn01` jest w warstwie 0, więc wpisać dowolną nazwę może tylko łącznik Intune, który robi to według profilu. Z prawem Enroll dla Domain Users każdy pracownik mógłby poprosić o certyfikat z UPN administratora domeny i zalogować się nim.

1. Gdzie szukamy przyczyny, gdy nowy kontroler `dc03` nie ma certyfikatu do LDAPS po tygodniu?

Odpowiedź

Sprawdzamy, czy szablon `ZielonaKontroler` jest opublikowany na urzędzie, czy grupa Domain Controllers ma w nim Read, Enroll i Autoenroll, i czy GPO automatycznej rejestracji obejmuje jednostkę Domain Controllers. Potem `certutil -pulse` na `dc03` i dziennik Application ze źródłem CertificateServicesClient-AutoEnrollment.

Powiązane: Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA · Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza · Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona · Certyfikaty, Wi-Fi i VPN z Intune: Certificate Connector czy Cloud PKI · EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt

Źródła: (odczyt 20 do 26.10.2026) · support.microsoft.com, KB5014754 „Certificate-based authentication changes on Windows domain controllers” (10.05.2022, 11.04.2023, 11.02.2025, 9.09.2025; rozszerzenie `1.3.6.1.4.1.311.25.2`; zdarzenia 39, 40, 41; typy mapowania silnego i słabego; bit `0x00080000` w `msPKI-Enrollment-Flag`) · learn.microsoft.com, „Certificate templates” i „Configure certificate autoenrollment” · learn.microsoft.com, `Add-CATemplate`, `Remove-CATemplate`, `Get-CATemplate` · learn.microsoft.com, „certreq -enroll” i „certutil -pulse” · learn.microsoft.com, „Use a PKCS certificate profile” (`EnableSidSecurityExtension`) i „Use SCEP certificate profiles” (`{{OnPremisesSecurityIdentifier}}`) · trustedsec.com, „EKUwu: Not just another AD CS ESC” (szablony w wersji 1, poprawka 12.11.2024)

Revision #2
Created 2026-10-26 14:06:00 UTC by Tomasz Konieczny
Updated 2026-10-26 14:28:21 UTC by Tomasz Konieczny