Utrzymanie i zmiana

Przenosiny z dc01, hartowanie AD CS, certyfikaty publiczne i ACME.

- Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona
- Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza
- Certyfikaty publiczne i ACME: Let's Encrypt z DNS-01, skracanie ważności i step-ca

Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona

Poziom: zaawansowany

Dotyczy: CA-Zielona na dc01 (Windows Server 2022), Zielona-Root-CA na ca-root01 i Zielona-CA01 na ca01 (Windows Server 2025), NPS, fw01 (FortiOS 7.6), conn01 z Certificate Connector, Intune, serwery linuksowe i kontenery z LDAPS

Czas: ~2 h pracy rozłożonej na dziesięć tygodni

Przenosiny urzędu to nie kopiowanie bazy na nowy serwer, tylko wymiana zaufania w całej firmie: najpierw każde urządzenie zaczyna ufać nowemu urzędowi, potem nowy urząd przejmuje wydawanie, a stary dożywa w spokoju do wygaśnięcia ostatniego certyfikatu. Tak robione przenosiny nie mają ani jednej chwili, w której coś musi się zepsuć. Wracamy tu w styczniu 2027, po zakazie zmian, i przy każdej przyszłej wymianie urzędu.

ZAŁOŻENIA SCENARIUSZA

nowa hierarchia ma inne nazwy niż stary urząd (`Zielona-Root-CA` i `Zielona-CA01` obok `CA-Zielona`), więc oba urzędy działają równolegle. Wariant „ta sama nazwa na nowym serwerze” (kopia bazy i klucza, `Restore-CARoleService`) opisuje dokumentacja Microsoftu o migracji AD CS; nie wybieramy go, bo przenosi na nowy serwer jednopoziomowy urząd z kluczem, który przez lata leżał w kopiach kontrolera. NPS stoi na `dc02`; gdy wcześniej powstaną `nps01` i `nps02`, ten sam krok robimy na nich.

Skróty użyte na tej stronie (18)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

Skrót	Co znaczy
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
AIA	Authority Information Access: miejsce w certyfikacie, które mówi, skąd pobrać certyfikat urzędu, który go podpisał
CD	Continuous Delivery/Deployment: automatyczne wdrażanie zbudowanego kodu
CDP	CRL Distribution Point: adres w certyfikacie, pod którym urząd publikuje listę unieważnionych certyfikatów
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
EAP	Extensible Authentication Protocol: rodzina metod uwierzytelniania, dzięki której VPN albo Wi-Fi mogą pytać o hasło albo o certyfikat na wiele różnych sposobów
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
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
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS
XML	eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Fiszka

Polecenia na urzędach wykonujemy w PowerShellu jako administrator urzędu, polecenia na `fw01` w CLI FortiOS, na linuksach w bash z sudo. Kolejność faz jest ważniejsza niż same polecenia: zaufanie przed wydawaniem, wydawanie przed wycofaniem.

ZMIENIA SYSTEM

Lista ważnych certyfikatów starego urzędu: certutil -view

```
certutil -config "dc01.ad.zielona.example\CA-Zielona" -view -restrict "Disposition=20" -
out "RequestID,RequesterName,CommonName,NotAfter,CertificateTemplate" csv > C:\Temp\CA-
Zielona-wydane.csv
Import-Csv C:\Temp\CA-Zielona-wydane.csv | Where-Object { [datetime]$_.'Certificate
Expiration Date' -gt (Get-Date) } | Sort-Object { [datetime]$_.'Certificate Expiration
Date' } | Format-Table
```

Pierwsze polecenie zapisuje wszystkie wydane i nieunieważnione certyfikaty (stan 20), drugie wybiera te, które jeszcze nie wygasły, i sortuje po dacie. Nagłówki kolumn w pliku zależą od języka systemu, więc przed filtrowaniem zaglądamy do pierwszej linii pliku. To lista, którą odhaczamy w fazach 3 do 5.

Przykład (skrót):

```
Request ID Requester Name       Issued Common Name             Certificate Expiration
Date Certificate Template
---------- --------------       ------------------
--------------------------- --------------------
214        ZIELONA\jan.kowalski vpn.zielona.example            03.10.2027
08:22            ZielonaWWW
1032       ZIELONA\WS-MAG07$    ws-mag07.ad.zielona.example    11.08.2027
06:01            Machine
```

certutil = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

ZMIENIA SYSTEM

Dodanie nowego urzędu głównego do zaufanych na linuksie: update-ca-trust

```
sudo cp zielona-root-ca.crt /etc/pki/ca-trust/source/anchors/zielona-root-ca.crt
sudo update-ca-trust
trust list --filter=ca-anchors | grep -A2 "Zielona-Root-CA"
```

Komendy można wykonać jako blok. Dopisujemy nowy urząd obok starego `CA-Zielona.crt`, niczego nie usuwając. Kontenery z własnym magazynem zaufania (Gitea, Graylog, Jenkins,

MailCow, Argo CD) dostają plik tak, jak opisuje strona logowania z AD każdej aplikacji.

Przykład:

```
pkcs11:id=%3A%1F...;type=cert
    type: certificate
    label: Zielona-Root-CA
```

CD = Continuous Delivery/Deployment: automatyczne wdrażanie zbudowanego kodu · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **cp** = copy: skopiuj · **update-ca-trust** = update CA trust: odświeżenie systemowego magazynu zaufanych urzędów certyfikacji w Rocky Linux · **trust** = p11-kit trust: pokaż i zmień systemowy magazyn zaufanych certyfikatów na Linuksie

ZMIENIA SYSTEM

Import urzędu do zaufanych na FortiGate: execute vpn certificate ca import

```
execute vpn certificate ca import tftp NazwaPliku.cer AdresSerweraTftp
```

Wgrywa publiczny certyfikat urzędu na `fw01`. Robimy to dwa razy: dla `Zielona-Root-CA` i dla `Zielona-CA01`, bo FortiGate przy sprawdzaniu certyfikatów klientów nie zawsze pobiera brakujące ogniwa spod adresu AIA. Nazwy, które FortiOS nada certyfikatom (`CA_Cert_N`), zapisujemy w zgłoszeniu.

AIA = Authority Information Access: miejsce w certyfikacie, które mówi, skąd pobrać certyfikat urzędu, który go podpisał

ZMIENIA SYSTEM

Dopuszczenie nowego urzędu przy logowaniu certyfikatem na FortiGate: config user peer

```
config user peer
    edit "NazwaProfiluPeer"
        set ca "NazwaCertyfikatuCA"
    next
end
```

Profil peer wskazuje urząd, którego certyfikaty klientów FortiGate przyjmuje. Na czas przenosin potrzebujemy przyjmowania certyfikatów z obu urzędów, więc zakładamy drugi profil dla `Zielona-CA01` i dopisujemy go do grupy użytkowników VPN obok starego. Dokładną składnię dla naszej wersji FortiOS sprawdzamy w dokumentacji Fortinet przed zmianą.

VPN = Virtual Private Network: szyfrowany tunel do sieci firmowej

ZMIENIA SYSTEM

Profil zaufanego certyfikatu dla nowej hierarchii: Intune

```
Microsoft Intune admin center → Devices → Manage devices → Configuration → Create → New policy
→ Platform: Windows 10 and later → Profile type: Templates → Trusted certificate
→ profil 1: plik Zielona-Root-CA.cer, Destination store: Computer certificate store - Root
→ profil 2: plik Zielona-CA01.cer, Destination store: Computer certificate store - Intermediate
→ Assignments: te same grupy co profile Wi-Fi, VPN i PKCS
```

Dwa nowe profile dokładamy obok istniejącego `Zielona-Zaufany-CA-Zielona`, którego nie usuwamy do końca przenosin.

ZMIENIA SYSTEM

Przełączenie wydawania szablonu na nowy urząd: Add-CATemplate i Remove-CATemplate

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

Pierwsze polecenie wykonujemy na `ca01`, drugie na `dc01`, w tej kolejności i w odstępie co najmniej jednej replikacji. Przez chwilę oba urzędy wydają ten sam szablon i to jest w porządku: klient wybiera któryś z nich.

ZMIENIA SYSTEM

Wydłużenie listy unieważnień starego urzędu: certutil -setreg CA\CRLPeriodUnits

```
certutil -setreg CA\CRLPeriodUnits 4
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
Restart-Service certsvc
certutil -crl
```

Komendy można wykonać jako blok, na `dc01`, gdy `CA-Zielona` przestaje wydawać cokolwiek. Lista ważna miesiąc zostawia zapas na dłuższą przerwę `dc01`, a urząd dalej publikuje ją sam. Starych certyfikatów nie unieważniamy hurtem: wygasają same albo wymieniamy je w fazach.

CA = Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

OSTROŻNIE · NIEODWRACALNE

Usunięcie roli urzędu z kontrolera: Uninstall-AdcsCertificationAuthority

```
Uninstall-AdcsCertificationAuthority -Force
Uninstall-WindowsFeature ADCS-Cert-Authority, ADCS-Web-Enrollment
```

Komendy można wykonać jako blok, ale tylko w fazie 6, po sprawdzeniu listy z pierwszej fiszki i po wykonaniu kopii urzędu, którą przechowujemy jeszcze rok. Usuwa urząd z `dc01`; jego certyfikaty, które gdzieś jeszcze zostały, przestaną przechodzić sprawdzenie unieważnienia, gdy wygaśnie ostatnia lista.

OSTROŻNIE · NIEODWRACALNE

Usunięcie starego urzędu z magazynu NTAuth: certutil -viewdelstore

```
certutil -viewdelstore "ldap:///CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=ad,DC=zielona,DC=example?cACertificate?base?obj
ectClass=certificationAuthority"
```

Otwiera okno z urzędami w NTAuth i pozwala usunąć wybrany. Usuwamy wyłącznie `CA-Zielona`, po fazie 6: od tej chwili żaden certyfikat z tego urzędu nie zaloguje nikogo do domeny. Resztę obiektów (AIA, CDP, Enrollment Services, Certification Authorities) sprzątamy w `pkiview.msc`, menu Action, Manage AD Containers.

NTAuth = magazyn NTAuth (NT Authentication): lista urzędów w konfiguracji lasu AD, których certyfikaty mogą służyć do logowania do domeny · **AIA** = Authority Information Access: miejsce w certyfikacie, które mówi, skąd pobrać certyfikat urzędu, który go podpisał · **CDP** = CRL Distribution Point: adres w certyfikacie, pod którym urząd publikuje listę unieważnionych certyfikatów · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń · **CN** = Common Name: główna nazwa w certyfikacie, np. adres serwera · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

Zanim zaczniemy

Z ŻYCIA WZIĘTE

Środa, 9:30, styczeń. Tomek proponuje zrobić wszystko w jedno popołudnie: „zdejmiemy szablony ze starego, opublikujemy na nowym, i po sprawie". Pytamy, co stanie się z Gitea, która ufa tylko plikowi `CA-Zielona.crt`, gdy `dc01` dostanie nowy certyfikat LDAPS z `Zielona-CA01`. Tomek przez chwilę liczy w głowie aplikacje z logowaniem z AD, dochodzi do siedmiu i proponuje sam, żeby zaufanie rozdać tydzień wcześniej.

Wymaganie	Jak sprawdzamy
hartowanie `CA-Zielona` zrobione przed zakazem zmian	strona Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza, zgłoszenie zamknięte do 14.11.2026
nowa hierarchia działa	weryfikacja ze strony Budowa hierarchii: urząd główny offline ca-root01 i urząd wydający ca01
szablony skopiowane z tymi samymi nazwami technicznymi	`Get-CATemplate` na `dc01` i lista w GLPI, strona Szablony, automatyczna rejestracja i silne mapowanie certyfikatów
lista wydanych certyfikatów starego urzędu	pierwsza fiszka, plik w zgłoszeniu
lista miejsc, które ufają tylko plikowi `CA-Zielona.crt`	inwentarz ze strony Inwentarz certyfikatów i częste problemy: wygasła CRL, łańcuch, SAN, alarm w Zabbixie
grupa pilotażowa: komputery i konta zespołu IT	grupa `GG_PKI_Pilot` w AD i w Entra ID
terminy poza zakazem zmian, Patch Tuesday i zamknięciem miesiąca	kalendarz zmian w GLPI

Kolejność faz



Rysunek 1. Przenosiny w sześciu fazach: hartowanie starego urzędu do 14 listopada 2026, budowa 19 stycznia 2027, rozdanie zaufania 2 lutego, komputery i kontrolery 16 lutego, NPS, fw01 i Intune 2 marca, użytkownicy i koniec wydawania ze starego urzędu 16 i 23 marca, wycofanie CA-Zielona po wygaśnięciu ostatniego certyfikatu (kliknięcie otwiera pełny rozmiar)

Faza	Termin (wtorek, okno 17:00 do 20:00)	Co robimy	Co może się zepsuć
0	do 14.11.2026	hartowanie `CA-Zielona`, kopia klucza i bazy, inwentarz	nic, zmiany na starym urzędzie
1	19.01.2027	budowa `ca-root01` i `ca01`	nic, nowy urząd nic nie wydaje
2	2.02.2027	rozdanie zaufania: AD (już po budowie), Intune, linuksy, kontenery, `fw01`, profile Wi-Fi i VPN	nic, tylko dokładamy zaufanie
3	16.02.2027	szablony `ZielonaKomputer` i `ZielonaKontroler` na `ca01`, pilotaż, potem wszyscy	LDAPS w aplikacjach, które pominęliśmy w fazie 2
4	2.03.2027	`ZielonaNPS`, certyfikat bramy VPN na `fw01` z `ZielonaWWW`, `conn01` i profil PKCS dla `ca01`	Wi-Fi i VPN, jeśli profil klienta nie ufa nowemu urzędowi
5	16.03 i 23.03.2027	`ZielonaUzytkownik`, certyfikat inspekcji SSL z ceremonii, `ZielonaWWW` tylko z `ca01`; 23.03 ostatnie szablony zdjęte z `CA-Zielona`	ręcznie wydane certyfikaty serwerów, o których nikt nie pamiętał
6	po wygaśnięciu albo wymianie ostatniego certyfikatu (najpóźniej marzec 2028)	wycofanie `CA-Zielona`, sprzątanie AD, `dc01` bez AD CS	stare certyfikaty spoza inwentarza

Patch Tuesday w 2027 roku wypada 12 stycznia, 9 lutego i 9 marca, a zamknięcie miesiąca to trzy ostatnie dni robocze, dlatego terminy przeskakują o tydzień.

Przebieg

Faza 2: zaufanie przed wydawaniem

> **Pojęcie: przenosiny przez równoległe urzędy.** Sposób wymiany urzędu, w którym stary i nowy działają jednocześnie, a klienci ufają obu. Każdy klient przechodzi na nowy urząd przy najbliższym odnowieniu albo wymuszonej wymianie, a stary urząd znika dopiero wtedy, gdy nie zostaje po nim ani jeden potrzebny certyfikat.

1. Sprawdzamy na stacji pilotażowej, że `Zielona-Root-CA` jest w magazynie Root, a `Zielona-CA01` w Intermediate (po `gpupdate /force`).
2. W Intune dokładamy dwa profile zaufanego certyfikatu (fiszka) dla wszystkich grup z profilami Wi-Fi, VPN i PKCS.
3. W profilu Wi-Fi z Intune i w GPO Wi-Fi dla komputerów w biurze dopisujemy `Zielona-Root-CA` w polu zaufanych urzędów dla certyfikatu serwera (Root certificates for server validation), obok `CA-Zielona`. Bez tego kroku faza 4 odetnie Wi-Fi.
4. W profilu VPN (EAP XML) dopisujemy odcisk `Zielona-Root-CA` obok odcisku `CA-Zielona` w liście zaufanych urzędów serwera.
5. Na każdym linuksie i w każdym kontenerze z listy inwentarza dodajemy `Zielona-Root-CA` (fiszka z `update-ca-trust`), w Jenkinsie do magazynu Javy, w Argo CD do konfiguracji certyfikatów.
6. Na `fw01` importujemy oba certyfikaty urzędów i zakładamy drugi profil peer.
7. Sprawdzamy z `docker01`, `mon01` i `pg01`: `openssl verify -CAfile /etc/pki/tls/certs/ca-bundle.crt` na certyfikacie testowym z `ca01` daje `OK`.

Faza 3: komputery i kontrolery

1. Publikujemy `ZielonaKomputer` i `ZielonaKontroler` na `ca01`, z prawem Autoenroll tymczasowo tylko dla `GG_PKI_Pilot` i jednego kontrolera (`dc03`, gdy istnieje, inaczej `dc02`).
2. Na komputerach pilotażu `certutil -pulse`, sprawdzamy wystawcę nowych certyfikatów, Wi-Fi, VPN i logowanie.
3. Sprawdzamy LDAPS na kontrolerze pilotażowym ze wszystkich aplikacji z logowaniem z AD (test logowania w Gitea, NetBoksie, Graylogu, GLPI, Zabbixie, Jenkinsie i PostgreSQL na `pg01`).

4. Po dniu bez zgłoszeń przywracamy prawa Domain Computers i Domain Controllers w szablonach na `ca01`, zdejmujemy oba szablony z `dc01` i robimy `Reenroll All Certificate Holders`.

Faza 4: NPS, brama VPN i Intune

1. Na serwerze NPS `certreq -enroll -machine -q ZielonaNPS`, w konsoli NPS (Network Policies, Constraints, Authentication Methods, EAP Types, Microsoft: Smart Card or other certificate, Edit) wybieramy nowy certyfikat. Pierwszy test z laptopa pilotażowego, potem z laptopa spoza pilotażu, który ma tylko profil z fazy 2.
2. Dla `fw01` wystawiamy certyfikat `vpn.zielona.example` z `ZielonaWWW` na `ca01` (klucz powstaje na `fw01` albo w `certreq`, jak na stronie Błąd 13801: certyfikat bramy VPN, EKU i SAN), importujemy go i przełączamy w `phase1-interface`. Stary certyfikat zostaje na `fw01` do fazy 6.
3. Na `conn01` niczego nie instalujemy od nowa: łącznik obsługuje każdy urząd Enterprise w lesie. Tworzymy nowy profil PKCS z `Certification authority: ca01.ad.zielona.example` i `Certification authority name: Zielona-CA01`, przypisujemy go grupie pilotażowej, a po teście wszystkim; stary profil PKCS usuwamy z przypisań, gdy nowe certyfikaty są na urządzeniach. Szablon `ZielonaUzytkownik-Intune` publikujemy na `ca01` z prawami dla `conn01$` przed utworzeniem profilu.

Faza 5: użytkownicy, inspekcja i ręczne certyfikaty

1. `ZielonaUzytkownik` na `ca01`, zdjęcie z `dc01`, `Reenroll All Certificate Holders` po pilotażu.
2. Na ceremonii marcowej `ca-root01` podpisuje żądanie urzędu inspekcji SSL z `fw01` (projekt w Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA); w profilu `ssl-ssh-profile` wskazujemy nowy certyfikat.
3. Z listy z pierwszej fiszki wybieramy certyfikaty z `ZielonaWWW` i innych szablonów ręcznych, wystawiamy nowe z `ca01` (Lore, Traefik, Perforce, `fw01`, drukarki z panelem WWW) i wpisujemy w inwentarz datę wymiany.
4. 23.03 zdejmujemy z `CA-Zielona` wszystkie pozostałe szablony i wydłużamy jego listę unieważnień (fiszka). Od tej chwili stary urząd nic nie wydaje.

Faza 6: wygaszenie CA-Zielona

1. Raz w miesiącu porównujemy listę ważnych certyfikatów starego urzędu z inwentarzem. Certyfikat bez odpowiednika z `ca01` wymieniamy.

2. Gdy lista jest pusta albo zawiera tylko certyfikaty już wymienione: ostatnia kopia urzędu (strona o hartowaniu), wycofanie roli z `dc01`, usunięcie `CA-Zielona` z NTAuth i kontenerów AD, zdjęcie profilu `Zielona-Zaufany-CA-Zielona` w Intune, usunięcie `CA-Zielona.crt` z linuksów i kontenerów, usunięcie starego profilu peer i certyfikatów na `fw01`.
3. Od tej chwili `dc01` jest zwykłym kontrolerem i można go wycofać według strony Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie.

Weryfikacja

```
Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Issuer -like "*Zielona-CA01*" } |
Select-Object Subject, NotAfter
certutil -config "ca01.ad.zielona.example\Zielona-CA01" -view -restrict "Disposition=20" -out
"CertificateTemplate" csv | Group-Object | Select-Object Count, Name
```

Pierwsze polecenie na kilku komputerach i kontrolerach pokazuje certyfikaty z nowego urzędu, drugie na urzędzie liczy wydane certyfikaty według szablonu. Po fazie 5 liczba certyfikatów z `ZielonaKomputer` na `ca01` powinna odpowiadać liczbie komputerów w domenie.

Na kontrolerze w tygodniu po każdej fazie zaglądamy do zdarzeń 39, 40 i 41 (strona o szablonach), a w Graylogu do odrzuceń NPS (zdarzenie 6273).

Wycofanie zmian

Do fazy 5 każdy krok jest odwracalny jednym poleceniem, bo stary urząd działa, a klienci mu ufają:

Faza	Wycofanie
2	nic nie trzeba wycofywać; dodatkowe zaufanie nie przeszkadza
3	`Add-CATemplate` na `dc01`, `Remove-CATemplate` na `ca01`, `certutil -pulse` na komputerach; certyfikaty z `ca01` mogą zostać
4	w konsoli NPS i na `fw01` wybieramy z powrotem stary certyfikat, w Intune przywracamy przypisanie starego profilu PKCS
5	szablony z powrotem na `dc01`, lista unieważnień z powrotem na tydzień

Faza	Wycofanie
6	brak prostego wycofania: odtworzenie `CA-Zielona` z kopii (`Restore-CARoleService`) na nowym serwerze z tą samą nazwą, dlatego do fazy 6 nie spieszymy się

Gdy coś nie zadziała

Objaw	Przyczyna	Co robimy
Gitea, Graylog albo `pg01` nie logują użytkowników po fazie 3	kontroler ma nowy certyfikat LDAPS, a aplikacja ufa tylko `CA-Zielona.crt`	dodajemy `Zielona-Root-CA` do magazynu aplikacji, do czasu poprawki szablon `ZielonaKontroler` wyłączony dla tego kontrolera
Laptopy łączą się z Wi-Fi w biurze, ale nie poza pilotażem	profil Wi-Fi nie ma nowego urzędu w zaufanych dla serwera	wracamy w NPS do starego certyfikatu, poprawiamy profil w Intune i GPO, czekamy na synchronizację
VPN: błąd 13801 po wymianie certyfikatu bramy	klient nie ufa `Zielona-Root-CA` albo nowy certyfikat nie ma SAN	sprawdzamy profil zaufanego certyfikatu i SAN według strony o błędzie 13801
FortiGate odrzuca certyfikaty użytkowników z `ca01`	brak drugiego profilu peer albo brak certyfikatu `Zielona-CA01` na bramie	import obu certyfikatów urzędów, profil peer, `diagnose debug application fnbamd -1` w czasie próby
Profil PKCS z `ca01` w stanie Error	szablon nieopublikowany na `ca01` albo `conn01$` bez Read i Enroll	`Get-CATemplate` na `ca01`, zakładka Security szablonu
Po wycofaniu `CA-Zielona` drukarka skanująca do udziału przestaje działać	ręczny certyfikat spoza inwentarza	nowy certyfikat z `ZielonaWWW`, wpis do inwentarza

□□ Ćwiczenia

1. Dlaczego faza 2 nie może iść po fazie 4?

Odpowiedź

W fazie 4 NPS i `fw01` dostają certyfikaty z nowego urzędu. Laptop, który jeszcze mu nie ufa, odrzuci certyfikat serwera NPS i bramy VPN, więc Wi-Fi i VPN przestaną działać. Najpierw każdy klient musi ufać nowemu urzędowi, dopiero potem serwery mogą się nim przedstawiać.

1. W fazie 6 na liście starego urzędu zostały trzy certyfikaty komputerów magazynu ważne do sierpnia 2027, a komputery mają już certyfikaty z `ca01`. Czy możemy wycofać `CA-`

`Zielona` w kwietniu?

Odpowiedź

Tak, jeśli upewnimy się, że te komputery używają już nowych certyfikatów (stare są tylko zbędnym zapasem w magazynie). Dla porządku można je unieważnić i opublikować ostatnią listę przed wycofaniem. Wycofujemy po ostatniej kopii urzędu, którą trzymamy jeszcze rok.

1. Tomek pyta, czemu nie unieważnimy od razu wszystkich certyfikatów `CA-Zielona` po fazie 5, „żeby było czysto”. Co odpowiadamy?

Odpowiedź

Hurtowe unieważnienie wyłącza w jednej chwili wszystko, czego nie wymieniliśmy, a lista z pierwszej fiszki nie obejmuje urządzeń spoza domeny, z którymi coś mogło się zdarzyć. Wygaszanie przez wygaśnięcie albo wymianę po kolei daje zgłoszenia pojedynczo, a nie lawinę naraz.

Powiązane: Budowa hierarchii: urząd główny offline ca-root01 i urząd wydający ca01 · Szablony, automatyczna rejestracja i silne mapowanie certyfikatów · 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 · Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie · Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć

Źródła: (odczyt 20 do 26.10.2026) · learn.microsoft.com, „certutil” (`-view -restrict`, `-out ... csv`, `-viewdelstore`, `-setreg CA\CRLPeriodUnits`) · learn.microsoft.com, `Uninstall-AdcsCertificationAuthority`, `Add-CATemplate`, `Remove-CATemplate`, `Restore-CARoleService` · learn.microsoft.com, „Active Directory Certificate Services migration guide” (wariant z tą samą nazwą) · learn.microsoft.com, „Use a PKCS certificate profile” (Certificate Connector obsługuje urzędy Enterprise w lesie) · docs.fortinet.com, FortiOS 7.6 CLI Reference, `execute vpn certificate ca import` i `config user peer` (składnię sprawdzamy dla naszej wersji) · directaccess.richardhicks.com, wpisy o migracji AD CS (październik 2026)

Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza

Poziom: zaawansowany

Dotyczy: AD CS na Windows Server 2022 (CA-Zielona na dc01) i 2025 (ca01, ca-root01), szablony certyfikatów, IIS, Graylog, Microsoft Defender for Identity, Locksmith 2026.1, PSPKIAudit, Certify

Czas: ~90 min

Źle ustawiony urząd certyfikacji to najkrótsza droga od zwykłego konta do administratora domeny, a badacze opisali już szesnaście takich dróg. Ta strona tłumaczy je bez żargonu, pokazuje, jak sprawdzić każdą z nich w Zielonej, i zbiera to, co robimy zawsze: uprawnienia, audyt zdarzeń urzędu i kopię klucza z bazą. Wracamy tu przed audytem, raz na kwartał przy przeglądzie i po każdej zmianie szablonu.

ZAŁOŻENIA SCENARIUSZA

hartujemy dzisiejszy `CA-Zielona` na `dc01` przed zakazem zmian, we wtorek 3 listopada 2026 (kopia i audyt możemy włączyć wcześniej, bo niczego nie psują). Te same ustawienia dostaje `ca01` przy budowie. Defender for Identity jest opisany jako opcja: wymaga licencji, której Zielona dziś nie ma, a czujnik na serwerze urzędu daje dodatkowe oceny.

Skróty użyte na tej stronie (23)

Skrót	Co znaczy
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

Skrót	Co znaczy
CSV	w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami
EPA	Extended Protection for Authentication: ochrona w Windows i IIS, która wiąże logowanie z konkretnym połączeniem TLS i utrudnia przekazanie logowania NTLM (relay)
ESC	Escalation (numeracja SpecterOps): oznaczenie znanych dróg od zwykłego konta do przejęcia domeny przez źle ustawione AD CS, od ESC1 do ESC16
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
HSM	Hardware Security Module: sprzętowy moduł, w którym klucz urzędu powstaje i zostaje na zawsze; system prosi moduł o podpis, ale klucza nie da się skopiować
HTTP	Hypertext Transfer Protocol: protokół stron WWW
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
IIS	Internet Information Services: serwer WWW wbudowany w Windows Server
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
NTAuth	magazyn NTAuth (NT Authentication): lista urzędów w konfiguracji lasu AD, których certyfikaty mogą służyć do logowania do domeny
NTLM	NT LAN Manager: starszy od Kerberos sposób logowania w sieciach Windows przez wyzwanie i odpowiedź, podatny na przekazywanie i użycie skrótu hasła; Microsoft zapowiedział jego domyślne wyłączenie
PKI	Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów
PSPKI	moduł PowerShell PKI (autor Vadims Podāns): polecenia do zarządzania AD CS, na którym opiera się PSPKIAudit
README	Read Me: plik tekstowy z opisem projektu, wykresu lub szablonu, czytany jako pierwszy
RPC	Remote Procedure Call: sposób, w jaki programy wywołują funkcje na innym komputerze w sieci; kontrolery domeny używają go między innymi do replikacji
SAN	w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta
UPN	User Principal Name: login w formie adresu, np. jan.nowak@zielona.example
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS

Fiszka

Polecenia odczytu wykonujemy kontem domenowym z prawem odczytu konfiguracji lasu, z osobnej stacji administracyjnej. Polecenia zmieniające urząd wykonujemy na serwerze urzędu kontem `.t0` z rolą CA Administrator. Karty czerwone dotyczą kopii klucza: plik kopii ma taką wartość jak sam urząd.

◫◫ ZMIENIA SYSTEM

Przegląd urzędu i szablonów: Invoke-Locksmith -Mode 0

```
Install-Module -Name Locksmith -Scope CurrentUser
Invoke-Locksmith -Mode 0
```

Locksmith (autor Jake Hildreth) przegląda wszystkie urzędy i szablony w lesie i wypisuje znalezione błędy z numerem ESC. Tryb 0 tylko pokazuje tabelę, tryb 1 dokłada przykładowe poprawki, tryby 2 i 3 zapisują wynik do pliku CSV. Trybu 4, który sam poprawia ustawienia, nie używamy: każdą poprawkę robimy jako zmianę w GLPI. Najnowsza wersja w galerii PowerShell w październiku 2026 to 2026.1.4.1426 ze stycznia 2026; obok rozwija się moduł Locksmith2 (wydanie stabilne z 7 października 2026), który sprawdzimy przy kolejnym przeglądzie.

Przykład (skrót):

```
Technique Name               Issue
--------- ----               -----
ESC6      CA-Zielona         EDITF_ATTRIBUTESUBJECTALTNAME2 is enabled on the CA.
ESC8      CA-Zielona         HTTP enrollment is enabled.
ESC4      WebServer          Authenticated Users has Write permissions.
```

◫◫ **ESC** = Escalation (numeracja SpecterOps): oznaczenie znanych dróg od zwykłego konta do przejęcia domeny przez źle ustawione AD CS, od ESC1 do ESC16 · **CSV** = w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami · **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

◫◫ TYLKO ODCZYT

Szablony z nazwą podawaną w żądaniu: Get-ADObject msPKI-Certificate-Name-Flag

```
Get-ADObject -SearchBase "CN=Certificate Templates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=ad,DC=zielona,DC=example" -LDAPFilter "(msPKI-
```

```
Certificate-Name-Flag:1.2.840.113556.1.4.803:=1)" -Properties msPKI-Template-Schema-
Version, pKIExtendedKeyUsage | Format-Table Name, msPKI-Template-Schema-Version,
pKIExtendedKeyUsage
```

Wypisuje szablony, w których wnioskodawca sam podaje nazwę (flaga `ENROLLEE_SUPPLIES_SUBJECT`), z wersją schematu i zastosowaniami klucza. To kandydaci do ESC1 (z uwierzytelnianiem klienta) i ESC15 (wersja schematu 1).

Przykład:

```
Name                    msPKI-Template-Schema-Version pKIExtendedKeyUsage
----                    ----------------------------- ------------------
WebServer                                           1 {1.3.6.1.5.5.7.3.1}
ZielonaWWW                                          4 {1.3.6.1.5.5.7.3.1}
ZielonaUzytkownik-Intune                            4 {1.3.6.1.5.5.7.3.2}
```

□□ **CN** = Common Name: główna nazwa w certyfikacie, np. adres serwera · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

□□ **TYLKO ODCZYT**

Odczyt flag zasad urzędu: certutil -getreg policy\EditFlags

```
certutil -getreg policy\EditFlags
```

Szukamy w wyniku wiersza `EDITF_ATTRIBUTESUBJECTALTNAME2`. Jego obecność oznacza, że każdy, kto może poprosić o jakikolwiek certyfikat, może dopisać w żądaniu dowolną nazwę w SAN (ESC6).

Przykład (skrót):

```
  EditFlags REG_DWORD = 15014e (1376590)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
```

□□ **SAN** = w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

□□ **ZMIENIA SYSTEM**

Wyłączenie dowolnej nazwy w żądaniu: certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2

```
certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2
Restart-Service certsvc
```

Komendy można wykonać jako blok. Po restarcie usługi urząd ignoruje atrybut `san:` w żądaniach. Certyfikaty z SAN wystawiamy wyłącznie z szablonów, w których nazwę podaje się w żądaniu, a które mają tylko uwierzytelnianie serwera i zatwierdzenie menedżera (`ZielonaWWW`).

SAN = w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

ZMIENIA SYSTEM

Wymuszenie szyfrowania żądań RPC: certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST

```
certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST
Restart-Service certsvc
```

Komendy można wykonać jako blok. Urząd odrzuca żądania przez RPC bez szyfrowania pakietów, co zamyka przekaźnik NTLM do interfejsu RPC (ESC11). Windows od dawna szyfruje te żądania sam, więc problem mogą mieć tylko stare urządzenia albo skrypty; sprawdzamy w dzienniku po zmianie.

RPC = Remote Procedure Call: sposób, w jaki programy wywołują funkcje na innym komputerze w sieci; kontrolery domeny używają go między innymi do replikacji · **CA** = Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty · **NTLM** = NT LAN Manager: starszy od Kerberos sposób logowania w sieciach Windows przez wyzwanie i odpowiedź, podatny na przekazywanie i użycie skrótu hasła; Microsoft zapowiedział jego domyślne wyłączenie · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

TYLKO ODCZYT

Sprawdzenie wyłączonych rozszerzeń: certutil -getreg policy\DisableExtensionList

```
certutil -getreg policy\DisableExtensionList
```

Jeśli na liście jest `1.3.6.1.4.1.311.25.2`, urząd nie dodaje rozszerzenia SID do żadnego certyfikatu (ESC16), więc kontrolery odrzucą certyfikaty do logowania albo, przy słabym mapowaniu jawnym, przyjmą podrobione. Lista powinna być pusta.

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

ZMIENIA SYSTEM

Usunięcie rejestracji przez WWW: Uninstall-AdcsWebEnrollment

```
Get-WindowsFeature ADCS-* | Where-Object Installed | Format-Table Name, DisplayName
Uninstall-AdcsWebEnrollment -Force
Uninstall-WindowsFeature ADCS-Web-Enrollment
```

Komendy można wykonać jako blok. Strona `/certsrv` przyjmuje logowanie NTLM po HTTP, więc napastnik w sieci może przekazać do niej uwierzytelnienie kontrolera domeny i dostać jego certyfikat (ESC8). W Zielonej nikt z niej nie korzysta: komputery mają automatyczną rejestrację, a administratorzy `certreq`. Gdy rejestracja przez WWW jest kiedyś potrzebna, to tylko po HTTPS z ochroną EPA i bez NTLM.

WWW = World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS · **NTLM** = NT LAN Manager: starszy od Kerberos sposób logowania w sieciach Windows przez wyzwanie i odpowiedź, podatny na przekazywanie i użycie skrótu hasła; Microsoft zapowiedział jego domyślne wyłączenie · **HTTP** = Hypertext Transfer Protocol: protokół stron WWW · **HTTPS** = HTTP zabezpieczony szyfrowaniem TLS · **EPA** = Extended Protection for Authentication: ochrona w Windows i IIS, która wiąże logowanie z konkretnym połączeniem TLS i utrudnia przekazanie logowania NTLM (relay)

TYLKO ODCZYT

Odczyt uprawnień do urzędu: certutil -getreg CA\Security

```
certutil -getreg CA\Security
```

Pokazuje, kto ma prawa Manage CA i Issue and Manage Certificates. Prawo Manage CA pozwala zmienić flagi urzędu, a Issue and Manage Certificates zatwierdzić dowolne żądanie, więc oba prawa mają tylko konta warstwy 0 (ESC7).

Przykład (skrót):

```
Allow    Enroll  NT AUTHORITY\Authenticated Users
Allow    Certificate Manager  ZIELONA\GG_PKI_Menedzerowie
Allow    CA Administrator  ZIELONA\GG_PKI_Administratorzy
Allow    CA Administrator  ZIELONA\Domain Admins
Allow    CA Administrator  ZIELONA\Enterprise Admins
```

CA = Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

TYLKO ODCZYT

Odczyt uprawnień do szablonu: Get-Acl AD:

```
(Get-Acl "AD:CN=NazwaSzablonu,CN=Certificate Templates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=ad,DC=zielona,DC=example").Access | Where-
Object { $_.ActiveDirectoryRights -match "Write|GenericAll|ExtendedRight" } | Format-
Table IdentityReference, ActiveDirectoryRights, ObjectType
```

Wypisuje konta i grupy, które mogą zmienić szablon albo z niego korzystać. Prawa zapisu (`WriteProperty`, `WriteDacl`, `WriteOwner`, `GenericAll`) poza administratorami warstwy 0 to ESC4: ktoś może przerobić szablon na podatny i z niego skorzystać.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie · **CN** = Common Name: główna nazwa w certyfikacie, np. adres serwera · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

ZMIENIA SYSTEM

Włączenie audytu urzędu: certutil -setreg CA\AuditFilter

```
certutil -setreg CA\AuditFilter 127
auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
Restart-Service certsvc
```

Komendy można wykonać jako blok. `127` włącza wszystkie siedem kategorii audytu urzędu: start i zatrzymanie, kopię, wnioski, unieważnienia, ustawienia bezpieczeństwa, pobranie klucza archiwalnego i zmianę konfiguracji. Bez `auditpol` urząd zbiera zdarzenia, ale system ich nie zapisuje.

CA = Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń · **auditpol** = audit policy: odczyt i zmiana zaawansowanych zasad audytu Windows

◫◫ OSTROŻNIE · NIEODWRACALNE

Kopia klucza i bazy urzędu: Backup-CARoleService

```
$haslo = Read-Host -AsSecureString -Prompt "Haslo kopii urzedu"
Backup-CARoleService -Path "SciezkaKopii\baza-i-klucz" -Password $haslo
reg export "HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration"
"SciezkaKopii\konfiguracja-urzedu.reg" /y
Get-CATemplate | Export-Csv "SciezkaKopii\szablony.csv" -NoTypeInformation
Copy-Item C:\Windows\CAPolicy.inf "SciezkaKopii\" -ErrorAction SilentlyContinue
```

Komendy można wykonać jako blok. Powstaje plik `.p12` z kluczem urzędu zabezpieczonym hasłem, kopia bazy, eksport ustawień z rejestru, lista opublikowanych szablonów i plik zasad. Hasło trzymamy w Vaultwardenie i w kopercie w sejfie, a samą kopię na zaszyfrowanym nośniku poza siecią, nigdy na udziale ani w zwykłym repozytorium `bkp01` dostępnym dla warstwy 1.

◫◫ **reg** = registry: narzędzie wiersza poleceń do odczytu i zmiany rejestru Windows, na przykład reg query · **HKLM** = HKEY_LOCAL_MACHINE: gałąź rejestru Windows z ustawieniami całego komputera, a nie pojedynczego użytkownika

◫◫ OSTROŻNIE · NIEODWRACALNE

Odtworzenie urzędu z kopii: Restore-CARoleService

```
Restore-CARoleService -Path "SciezkaKopii\baza-i-klucz" -Password (Read-Host -
AsSecureString -Prompt "Haslo kopii urzedu") -Force
```

Wgrywa klucz i bazę na serwer z zainstalowaną rolą urzędu o tej samej nazwie (instalacja z istniejącym kluczem). Używamy tylko przy odtwarzaniu po awarii albo w ćwiczeniu na odizolowanej maszynie testowej; przed użyciem czytamy aktualną dokumentację odtwarzania AD CS, bo zależy od typu urzędu i dostawcy klucza.

◫◫ **AD CS** = Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji

Z życia wzięte

◫◫ Z ŻYCIA WZIĘTE

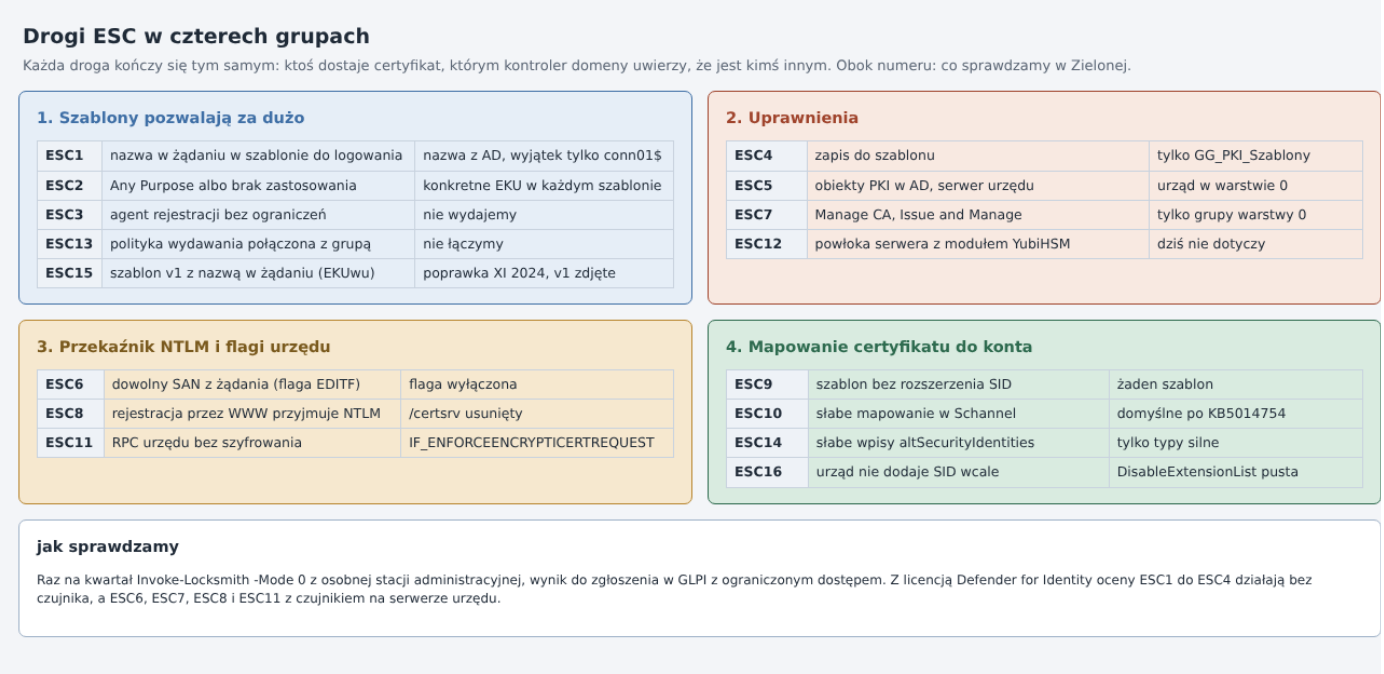
> Czwartek, 11:00. Ola, przeglądając wyniki skanera podatności, pokazuje nam stronę `http://dc01/certsrv`, której nikt w zespole IT nie używał od lat. Tego samego dnia Locksmith zgłasza na `CA-Zielona` ESC6 i ESC8: ktoś kiedyś włączył flagę dowolnej nazwy w SAN, żeby wystawić certyfikat bramy VPN, i nie wyłączył jej z powrotem, a rejestracja przez WWW przyszła z kreatora. Razem dawały drogę od dowolnego konta w sieci do certyfikatu kontrolera domeny. Po południu zgłoszenie w GLPI ma trzy zmiany na najbliższy wtorek i jedną notatkę: strona o błędzie 13801 dostaje poprawkę.

Jak to działa

Rozwiń: jak to działa pod spodem

Szesnaście dróg po ludzku

Wszystkie drogi ESC sprowadzają się do jednego: ktoś dostaje certyfikat, którym kontroler domeny uwierzy, że jest kimś innym, albo zmienia urząd tak, żeby taki certyfikat dostać. Numerację wprowadził w 2021 roku raport „Certified Pre-Owned” (ESC1 do ESC8), a kolejne numery dopisali inni badacze do ESC16 w 2025 roku.



Rysunek 1. Drogi ESC w czterech grupach: szablony, które pozwalają podać cudzą nazwę albo zbyt wiele zastosowań; uprawnienia do szablonów, urzędu i obiektów PKI; przekaźnik NTLM

do stron WWW i RPC urzędu; słabe albo wyłączone mapowanie certyfikatu do konta; dla każdej grupy co sprawdzamy w Zielonej (kliknięcie otwiera pełny rozmiar)

Numer	Po ludzku	Jak sprawdzamy	Co robimy w Zielonej
ESC1	szablon do logowania, w którym wnioskodawca sam wpisuje, kim jest	`Get-ADObject` z flagą nazwy w żądaniu, Locksmith	nazwa z AD w szablonach do logowania; wyjątek tylko dla `conn01$`
ESC2	szablon „do wszystkiego” (Any Purpose albo bez zastosowania)	Locksmith, kolumna `pKIExtendedKeyUsage`	każdy szablon ma konkretne zastosowania
ESC3	szablon agenta rejestracji pozwala prosić o certyfikaty w cudzym imieniu	Locksmith	nie wydajemy szablonów Enrollment Agent; gdyby były potrzebne, z ograniczeniami agentów na urzędzie
ESC4	ktoś niepowołany może zmienić szablon	`Get-Acl` na szablonie, Locksmith	zapis szablonów tylko dla `GG_PKI_Szablony` i administratorów lasu
ESC5	ktoś niepowołany może zmienić obiekty PKI w AD albo sam serwer urzędu	Locksmith, przegląd lokalnych administratorów urzędu	urząd w warstwie 0, kontener Public Key Services bez nadmiarowych praw
ESC6	urząd przyjmuje dowolną nazwę w SAN z żądania	`certutil -getreg policy\EditFlags`	flaga wyłączona na stałe
ESC7	ktoś niepowołany ma prawo Manage CA albo Issue and Manage Certificates	`certutil -getreg CA\Security`	tylko grupy warstwy 0
ESC8	strona rejestracji przez WWW przyjmuje przekazane logowanie NTLM	`Get-WindowsFeature ADCS-*`	rejestracja przez WWW usunięta
ESC9	szablon z wyłączonym rozszerzeniem SID	Locksmith (flaga `CT_FLAG_NO_SECURITY_EXTENSION`)	żaden szablon nie ma tej flagi
ESC10	słabe mapowanie certyfikatu w Schannel na kontrolerze	wartość `CertificateMappingMethods` na kontrolerach	domyślne ustawienie po KB5014754 (0x18), bez zmian ręcznych
ESC11	interfejs RPC urzędu przyjmuje żądania bez szyfrowania	`certutil -getreg CA\InterfaceFlags`	`IF_ENFORCEENCRYPTICERTREQUEST` włączone
ESC12	dostęp do powłoki serwera z modułem YubiHSM daje użycie klucza urzędu	przegląd, gdy kiedyś wybierzemy taki moduł	dziś nie dotyczy

Numer	Po ludzku	Jak sprawdzamy	Co robimy w Zielonej
ESC13	szablon z polityką wydawania powiązaną z grupą daje uprawnienia tej grupy	Locksmith	nie łączymy polityk wydawania z grupami
ESC14	słabe jawne mapowanie w `altSecurityIdentities` albo prawo jego zapisu	przegląd kont z tym atrybutem	tylko typy silne, zapis atrybutu tylko dla warstwy 0
ESC15	szablon w wersji 1 z nazwą w żądaniu pozwala dopisać dowolne zastosowanie (EKUwu, CVE-2024-49019)	`msPKI-Template-Schema-Version` równe 1	poprawka z 12 listopada 2024 na urzędzie, szablony w wersji 1 zdjęte z urzędu
ESC16	urząd w ogóle nie dodaje rozszerzenia SID	`certutil -getreg policy\DisableExtensionList`	lista pusta

> **Pojęcie: przekaźnik NTLM (NTLM relay).** Atak, w którym napastnik nakłania komputer (na przykład kontroler domeny) do zalogowania się u siebie, a to logowanie natychmiast przekazuje dalej, do usługi, która przyjmuje NTLM. Usługa myśli, że rozmawia z kontrolerem. Dlatego strony i interfejsy urzędu, które przyjmują NTLM bez ochrony kanału, są tak groźne.

Uprawnienia: kto co może

Uprawnienie	Kto w Zielonej	Gdzie ustawiamy
lokalny administrator `ca01` i `dc01`	konta `.t0`	grupy z ograniczonym członkostwem w GPO warstwy 0
CA Administrator (Manage CA)	`GG_PKI_Administratorzy` (konta `.t0` obu administratorów)	konsola urzędu, zakładka Security
Certificate Manager (Issue and Manage Certificates)	`GG_PKI_Menedzerowie` (te same osoby, ale osobna grupa, żeby dało się rozdzielić)	konsola urzędu, zakładka Security
zmiana szablonów	`GG_PKI_Szablony`	uprawnienia kontenera Certificate Templates
Enroll w szablonach	grupy według tabeli na stronie o szablonach	zakładka Security szablonu
Read urzędu i Request Certificates	Authenticated Users (zostaje)	konsola urzędu

Zmiany w grupach `GG_PKI_*` alarmują w Graylogu tak samo jak zmiany w Domain Admins, opisane na stronie Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt.

Audyt: zdarzenia urzędu w Graylogu

Urząd z `AuditFilter 127` zapisuje zdarzenia w dzienniku Security, a agent wysyła je do Grayloga, do tego samego strumienia co zdarzenia kontrolerów.

Zdarzenie	Co znaczy	Alarm
4886, 4887	urząd przyjął żądanie, wydał certyfikat	raport dzienny; alarm, gdy nazwa podmiotu albo SAN wskazuje konto uprzywilejowane, a wnioskodawca nim nie jest
4888, 4889	żądanie odrzucone, żądanie czeka na zatwierdzenie	raport dzienny
4870	certyfikat unieważniony	każde
4882, 4885	zmiana uprawnień urzędu, zmiana filtra audytu	każde
4890, 4891, 4892	zmiana ustawień menedżera, konfiguracji albo właściwości urzędu	każde
4899, 4900	zmiana szablonu, zmiana uprawnień szablonu	każde
4876, 4877	początek i koniec kopii urzędu	raport: kopia była w tym miesiącu
5136 na kontrolerze dla obiektów w `CN=Public Key Services`	zmiana obiektów PKI w AD	każde

Odbiór zdarzeń opisują strony Graylog: codzienna praca z logami i strona o hartowaniu AD (strumień `ad-logowania`).

Kopia klucza i bazy

> **Pojęcie: kopia urzędu.** Dwie różne rzeczy w jednym: klucz prywatny urzędu (bez niego nowy serwer nie podpisze niczego jako ten urząd) i baza wydanych certyfikatów (bez niej nie unieważnimy niczego, co wydano). Kopia stanu systemu kontrolera zawiera obie, ale też całą resztę kontrolera, więc nie jest dobrym miejscem na klucz urzędu.

Zasady kopii w Zielonej:

1. Kopia urzędu wydającego co tydzień do katalogu na `ca01`, a stamtąd raz w miesiącu na zaszyfrowany nośnik w sejfie (baza zmienia się codziennie, klucz raz na kilka lat).
2. Kopia urzędu głównego na każdej ceremonii, na dwóch dyskach w dwóch lokalizacjach.
3. Kopia `CA-Zielona` przed hartowaniem i przed każdą fazą przenosin, przechowywana jeszcze rok po jego wycofaniu.
4. Odtworzenie ćwiczymy raz w roku na odizolowanej maszynie, z protokołem w GLPI, tak jak odtwarzanie AD na stronie Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM.

> ⚠ Klucza urzędu nigdy nie eksportujemy poza urząd, jego kopię i ewentualny moduł HSM. Usługa, która potrzebuje certyfikatu (Traefik, Nginx, `fw01`, aplikacja Java), dostaje własny certyfikat serwera wystawiony przez urząd, a do zaufania tylko publiczny plik `.crt` urzędu. Plik o nazwie `CA-Zielona.key` na serwerze aplikacji oznacza albo klucz urzędu (wtedy urząd jest przejęty i stawiamy nowy), albo źle nazwany klucz certyfikatu serwera (wtedy zmieniamy nazwę, żeby nikt się nie pomylił). Stronę Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01 poprawiamy w tym duchu: Traefik dostaje certyfikat serwera, na przykład `wildcard-zielona.crt` z kluczem.

Oceny w Defender for Identity

Microsoft Defender for Identity ocenia konfigurację AD CS w Secure Score w dwóch grupach. Oceny szablonów działają dla każdego klienta z AD CS w lesie, a oceny samego urzędu wymagają czujnika Defender for Identity na serwerze urzędu (strona dokumentacji zaktualizowana 7 sierpnia 2026).

Ocena	Numer	Wymaga czujnika na urzędzie
użytkownicy mogą poprosić o certyfikat dla dowolnego konta	ESC1	nie
zbyt szerokie zastosowania w szablonie	ESC2	nie
źle ustawiony szablon agenta rejestracji	ESC3	nie
źle ustawione uprawnienia i właściciel szablonu	ESC4	nie

Ocena	Numer	Wymaga czujnika na urzędzie
podatne ustawienie urzędu	ESC6	tak
źle ustawione uprawnienia urzędu	ESC7	tak
niezabezpieczone strony rejestracji przez WWW	ESC8	tak
brak wymuszenia szyfrowania RPC	ESC11	tak

Licencję Defender for Identity porównuje strona Licencje i porównanie: Defender for Business, Endpoint P1 i P2 oraz odpowiedniki; Zielona jej dziś nie ma, więc tę samą listę sprawdzamy raz na kwartał Locksmithem. Część ocen ma w dokumentacji oznaczenie wersji zapoznawczej, więc listę porównujemy z portalem przed każdym przeglądem.

Narzędzia: tylko do audytu własnego środowiska

Narzędzie	Kto rozwija	Do czego używamy	Uwagi
Locksmith	Jake Hildreth, galeria PowerShell	kwartalny przegląd ESC, tryby 0 do 3	otwarte oprogramowanie, tryb 4 tylko w laboratorium
PSPKIAudit (`Invoke-PKIAudit`)	GhostPack (SpecterOps)	drugie zdanie przy przeglądzie, przegląd bazy wydanych certyfikatów (`Get-CertRequest`)	wymaga modułu PSPKI i RSAT dla AD CS; wykrywa ESC1 do ESC8, nowszych numerów nie
Certify	GhostPack (SpecterOps)	tylko wyliczanie urzędów i szablonów w laboratorium albo na zlecenie audytora	narzędzie ofensywne: program antywirusowy je blokuje, polecenia wydające certyfikaty pomijamy
Defender for Identity	Microsoft	stała ocena w Secure Score	wymaga licencji

> ⚠ Narzędzia do szukania ESC uruchamiamy wyłącznie we własnej domenie, z osobnej stacji administracyjnej, z wpisem w GLPI i zgodą pana Zbigniewa na piśmie dla narzędzi ofensywnych. Raport to gotowa mapa ataku na domenę, więc trzymamy go w zgłoszeniu z ograniczonym dostępem, a nie na udziale. W cudzym środowisku (u klienta, u dostawcy) tych narzędzi nie używamy

> bez umowy.

Droga bez Microsoftu

Urzędy spoza świata Microsoftu nie mają ESC w tym sensie, bo nie mają szablonów AD ani NTAuth, ale mają te same rodzaje błędów: zbyt szerokie zasady wydawania, zbyt wielu administratorów i brak kopii klucza.

Zabezpieczenie	step-ca	EJBCA Community	FreeIPA z Dogtag
kto może wnioskować o jakie nazwy	zasady (`policy`) z listą dozwolonych nazw na urzędzie i w każdym provisionerze	profile podmiotu i profile certyfikatu	profile certyfikatów i reguły `caacl`
administratorzy	osobni administratorzy urzędu, provisionery z hasłem albo tokenem	role i reguły dostępu	role IPA, grupa administratorów
klucz urzędu	plik z hasłem, moduł HSM przez PKCS#11 albo usługa KMS (obraz z przyrostkiem `-hsm`)	moduł HSM przez PKCS#11 albo programowo	baza NSS na serwerze IPA
audyt	dziennik usługi do Grayloga	dziennik audytu w bazie	dzienniki Dogtag
kopia	katalog konfiguracji, klucze i baza (BadgerDB albo PostgreSQL)	baza danych i magazyn kluczy	`ipa-backup`

Częste błędy

Objaw	Przyczyna	Co robimy
Po wyłączeniu ESC6 skrypt wystawiający certyfikaty z `san:` dostaje certyfikaty bez SAN	skrypt polegał na fladze	przestawiamy go na szablon `ZielonaWWW` z SAN w żądaniu (`request.inf` albo `san.cnf`)
Locksmith zgłasza ESC4 na szablonach domyślnych	uprawnienia z instalacji lasu sprzed lat	zdejmujemy domyślne szablony z urzędu, uprawnienia poprawiamy w szablonach, które zostają
W Graylogu brak zdarzeń 4886 i 4887	`AuditFilter` ustawiony, ale brak `auditpol` albo odwrotnie	oba polecenia z fiszki, `Restart-Service certsvc`, test wnioskiem `certreq`

Objaw	Przyczyna	Co robimy
Po wymuszeniu szyfrowania RPC stara drukarka nie odnawia certyfikatu	urządzenie wnioskuje bez szyfrowania	certyfikat dla drukarki ręcznie z `ZielonaWWW`, wpis w inwentarzu
Kopia urzędu leży na udziale `\\bkp01\kopie` z prawem odczytu dla działu IT	wygoda	przenosimy na nośnik w sejfie, w repozytorium zostaje tylko zaszyfrowana kopia z hasłem poza `bkp01`
Program antywirusowy usuwa `Certify.exe` ze stacji administratora	narzędzie ofensywne	do kwartalnego przeglądu używamy Locksmitha; Certify tylko w laboratorium z wyjątkiem w polityce

Ćwiczenia

1. Locksmith zgłasza na `CA-Zielona` jednocześnie ESC6 i ESC8. Dlaczego razem są groźniejsze niż osobno i co wyłączamy najpierw?

Odpowiedź

ESC8 pozwala napastnikowi przekazać logowanie kontrolera domeny do strony rejestracji i dostać certyfikat w imieniu kontrolera, a ESC6 pozwala w każdym żądaniu dopisać dowolną nazwę. Razem dają certyfikat z nazwą konta uprzywilejowanego bez żadnego uprawnienia. Najpierw wyłączamy flagę (jedno polecenie i restart usługi), potem usuwamy rejestrację przez WWW.

1. Dlaczego kopia stanu systemu `dc01` na `bkp01` nie wystarcza jako kopia urzędu?

Odpowiedź

Bo odtworzenie urzędu z kopii stanu systemu oznacza odtworzenie całego kontrolera, a klucz urzędu leży wtedy w repozytorium kopii razem z resztą danych, dostępny dla każdego, kto ma dostęp do kopii. Osobna kopia urzędu (`Backup-CARoleService`) z hasłem na nośniku w sejfie daje odtworzenie samego urzędu i lepiej chroni klucz.

1. Pan Wojtek pyta, jak udowodnimy, że nikt nie wystawił sobie certyfikatu z UPN prezesa. Co pokazujemy?

Odpowiedź

Zdarzenia 4887 z Grayloga za okres audytu z alarmem na nazwy kont uprzywilejowanych, przegląd bazy urzędu (`certutil -view` albo `Get-CertRequest` z PSPKI) filtrowany po UPN pana Zbigniewa, raport Locksmitha bez ESC1, ESC4, ESC6 i ESC8 oraz zgłoszenia w GLPI dla każdego ręcznie wystawionego certyfikatu.

1. W szablonie `WebServer` w wersji 1 prawo Enroll ma grupa Domain Computers. Który numer ESC dotyczy tej sytuacji i co robimy?

Odpowiedź

ESC15 (EKUwu): szablon w wersji 1 z nazwą w żądaniu pozwala dopisać do żądania zastosowanie uwierzytelniania klienta. Instalujemy poprawkę z listopada 2024 roku na urzędzie, zdejmujemy `WebServer` z urzędu i wydajemy certyfikaty serwerów z kopii w wersji 4 (`ZielonaWWW`) z prawem Enroll tylko dla administratorów.

Powiązane: Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA · Szablony, automatyczna rejestracja i silne mapowanie certyfikatów · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt · Błąd 13801: certyfikat bramy VPN, EKU i SAN · Generowanie certyfikatów: OpenSSL i urząd certyfikacji Windows · Graylog: codzienna praca z logami

Źródła: (odczyt 20 do 26.10.2026) · docs.specterops.io, „Escalation techniques” (ESC1 do ESC16) i „ESC11: NTLM relay to AD CS RPC interfaces” · trustedsec.com, „EKUwu: Not just another AD CS ESC” (8.10.2024, poprawka CVE-2024-49019 12.11.2024, szablony w wersji 1) · learn.microsoft.com, „Defender for Identity security posture assessments” (aktualizacja 7.08.2026: oceny szablonów bez czujnika, oceny urzędu z czujnikiem na serwerze AD CS) oraz strony ocen ESC4, ESC8 i ESC11 (część jako Preview) · dirteam.com, „What's New in Microsoft Defender for Identity in December 2023” (lista ocen AD CS) · powershellgallery.com, Locksmith 2026.1.4.1426 (4.01.2026) i Locksmith2 2026.10.70205 (7.10.2026) · README Locksmith (tryby 0 do 4) · it-connect.fr, „AD CS : auditer et analyser votre PKI avec PSPKIAudit” (3.10.2025, aktualizacja 20.05.2026: `Invoke-PKIAudit`, `Get-CertRequest`, wymagania, ESC1 do ESC8) · specterops.io, „Certify” · learn.microsoft.com, „certutil” (`-getreg`, `-setreg policy\EditFlags`, `CA\InterfaceFlags`, `CA\AuditFilter`), `Backup-CARoleService`, `Restore-CARoleService`, `Uninstall-AdcsWebEnrollment` · learn.microsoft.com, „Audit Certification Services” (zdarzenia 4868 do 4900) · support.microsoft.com, KB5014754 (`CertificateMappingMethods` 0x18)

Certyfikaty publiczne i ACME: Let's Encrypt z DNS-01, skracanie ważności i step-ca

Poziom: średnio

Dotyczy: Let's Encrypt, ACME (RFC 8555), certbot z wtyczką RFC 2136, Traefik na docker01, step-ca 0.30.2 na acme01 (10.20.10.128, opcja), Rocky Linux 9, harmonogram CA/Browser Forum SC081v3

Czas: ~50 min

Certyfikaty publiczne, którym ufa każda przeglądarka, od 15 marca 2026 roku żyją najwyżej 200 dni, od marca 2027 najwyżej 100, a od marca 2029 najwyżej 47. Przy takich liczbach ręczne odnawianie przestaje być możliwe, więc ta strona pokazuje automatyczne odnawianie protokołem ACME: publicznie z Let's Encrypt i walidacją przez DNS, a wewnętrznie z własnym urzędem ACME na step-ca. Wracamy tu przy każdej nowej usłudze widocznej z internetu i przed każdym progiem skracania ważności.

ZAŁOŻENIA SCENARIUSZA

strefa publiczna `zielona.example` jest u dostawcy DNS, który przyjmuje aktualizacje RFC 2136 z kluczem TSIG; gdy dostawca ma tylko własne API, używamy wtyczki certbota albo dostawcy w Traefiku dla tego API, a reszta strony się nie zmienia. Traefik na `docker01` już odnawia certyfikaty publiczne przez HTTP-01. `acme01` to propozycja: Rocky Linux 9 bez Dockera, step-ca jako urząd podrzędny `Zielona-Root-CA`, ograniczony do nazw w `zielona.example`.

Skróty użyte na tej stronie (29)

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

Skrót	Co znaczy
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
ARI	ACME Renewal Information: rozszerzenie protokołu ACME, w którym urząd podpowiada klientowi, kiedy odnowić certyfikat, także wcześniej po masowym unieważnieniu
B2B	business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DNS-01	sposób potwierdzenia domeny w ACME: urząd certyfikacji każe opublikować jednorazowy rekord TXT _acme-challenge i sprawdza go w DNS; działa bez portu 80 i pozwala na certyfikat wieloznaczny
DNS-PERSIST-01	nowa walidacja ACME ze stałym rekordem TXT _validation-persist, który nie zmienia się przy każdym odnowieniu (głosowanie CA/Browser Forum SC-088v3)
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
EPEL	Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów
HTTP-01	sposób potwierdzenia domeny w ACME: urząd certyfikacji pobiera jednorazowy plik z adresu /.well-known/acme-challenge/ na porcie 80 naszego serwera
IIS	Internet Information Services: serwer WWW wbudowany w Windows Server
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
OCSP	Online Certificate Status Protocol: sprawdzanie na żywo, czy certyfikat nie został unieważniony
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
RPM	RPM Package Manager: format paczek i narzędzie instalujące oprogramowanie w RHEL/Rocky, dnf korzysta z niego pod spodem
SCEP	Simple Certificate Enrollment Protocol: protokół, którym urządzenie samo prosi urząd certyfikacji o wystawienie certyfikatu
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS

Skrót	Co znaczy
TLS-ALPN-01	walidacja ACME, w której serwer pokazuje na porcie 443 specjalny certyfikat z tokenem urzędu (ALPN: Application-Layer Protocol Negotiation)
TSIG	Transaction Signature: podpis kluczem wspólnym, którym serwer DNS potwierdza, że aktualizację rekordu wysłał uprawniony klient, na przykład FortiGate w genericDDNS według RFC 2136
TXT	typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Polecenia wykonujemy w bash jako użytkownik z sudo: certbot na serwerze, który potrzebuje certyfikatu, step-ca na `acme01`. Zamiast `NazwaDomeny`, `NazwaSerwera`, `AdresSerweraDNS` i nazw kluczy wpisujemy własne wartości.

□□ ZMIENIA SYSTEM

Instalacja certbota z wtyczką RFC 2136: dnf install

```
sudo dnf install -y epel-release
sudo dnf install -y certbot python3-certbot-dns-rfc2136
```

Komendy można wykonać jako blok. Certbot i wtyczka pochodzą z repozytorium EPEL; nazwę pakietu wtyczki sprawdzamy w `dnf search certbot-dns`, gdy repozytorium ją zmieni.

□□ **RFC** = Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę ·**EPEL** = Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów ·**dnf** = Dandified YUM: menedżer pakietów RHEL/Rocky

□□ PLIK KONFIGURACYJNY

Plik z kluczem TSIG dla wtyczki: /etc/letsencrypt/rfc2136.ini

```
dns_rfc2136_server = AdresSerweraDNS
dns_rfc2136_port = 53
dns_rfc2136_name = NazwaKluczaTsig
dns_rfc2136_secret = SekretKluczaTsig
dns_rfc2136_algorithm = HMAC-SHA512
```

Plik daje prawo zmiany rekordów w strefie, więc ma prawa `600` i właściciela `root` (`sudo chmod 600 /etc/letsencrypt/rfc2136.ini`). Klucz TSIG u dostawcy ograniczamy, jeśli się da, do rekordów `_acme-challenge`.

TSIG = Transaction Signature: podpis kluczem wspólnym, którym serwer DNS potwierdza, że aktualizację rekordu wysłał uprawniony klient, na przykład FortiGate w genericDDNS według RFC 2136

ZMIENIA SYSTEM

Wystawienie certyfikatu z walidacją DNS-01: certbot certonly --dns-rfc2136

```
sudo certbot certonly --dns-rfc2136 --dns-rfc2136-credentials
/etc/letsencrypt/rfc2136.ini --dns-rfc2136-propagation-seconds 60 -d "NazwaDomeny" -d
"*.NazwaDomeny"
```

Certbot dopisuje w strefie rekord TXT `_acme-challenge`, czeka minutę na rozejście się zmiany, Let's Encrypt sprawdza rekord, a certbot go usuwa. Walidacja DNS-01 jest jedyną, która daje certyfikat z gwiazdką (`*.zielona.example`) i certyfikat dla nazwy, która nie jest osiągalna z internetu.

Przykład (skrót):

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/zielona.example/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/zielona.example/privkey.pem
This certificate expires on 2027-01-24.
```

DNS-01 = sposób potwierdzenia domeny w ACME: urząd certyfikacji każe opublikować jednorazowy rekord TXT _acme-challenge i sprawdza go w DNS; działa bez portu 80 i pozwala na certyfikat wieloznaczny · **TXT** = typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC · **certbot** = automatyczne certyfikaty Let's Encrypt

□□ TYLKO ODCZYT

Próba odnowienia bez wydawania: certbot renew --dry-run

```
sudo certbot renew --dry-run
```

Przechodzi całe odnowienie na serwerze testowym Let's Encrypt (staging), bez nowych certyfikatów i bez limitów. Robimy to po każdej zmianie w DNS, kluczu TSIG albo zaporze.

□□ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **TSIG** = Transaction Signature: podpis kluczem wspólnym, którym serwer DNS potwierdza, że aktualizację rekordu wysłał uprawniony klient, na przykład FortiGate w genericDDNS według RFC 2136 · **certbot** = automatyczne certyfikaty Let's Encrypt

□□ TYLKO ODCZYT

Sprawdzenie harmonogramu odnawiania: systemctl list-timers

```
systemctl list-timers | grep -i certbot
```

Pakiet z EPEL instaluje timer systemd, który dwa razy dziennie uruchamia `certbot renew`. Certbot odnawia certyfikat, gdy zostaje mniej niż jedna trzecia ważności, a przy kliencie z obsługą ARI wtedy, gdy wskaże to urząd (do sprawdzenia w naszej wersji certbota).

□□ **EPEL** = Extra Packages for Enterprise Linux: dodatkowe repozytorium pakietów dla RHEL i klonów · **ARI** = ACME Renewal Information: rozszerzenie protokołu ACME, w którym urząd podpowiada klientowi, kiedy odnowić certyfikat, także wcześniej po masowym unieważnieniu ·**systemctl** = system control: sterowanie usługami systemd

□□ ZMIENIA SYSTEM

Przeładowanie usługi po odnowieniu: --deploy-hook

```
sudo certbot reconfigure --cert-name NazwaDomeny --deploy-hook "systemctl reload nginx"
```

Zapisuje w konfiguracji odnowienia polecenie, które certbot wykona po każdym udanym odnowieniu. Bez tego usługa trzyma stary certyfikat w pamięci do restartu, a certyfikat na dysku jest już nowy. Polecenie `reconfigure` jest w nowszych wersjach certbota; w starszych dopisujemy `renew_hook` w pliku `/etc/letsencrypt/renewal/NazwaDomeny.conf`.

□□ **certbot** = automatyczne certyfikaty Let's Encrypt

PLIK KONFIGURACYJNY

Walidacja DNS-01 w Traefiku: certificatesresolvers.dnschallenge

```
command:
  - "--certificatesresolvers.le-dns.acme.email=it@zielona.example"
  - "--certificatesresolvers.le-dns.acme.storage=/acme/acme-dns.json"
  - "--certificatesresolvers.le-dns.acme.dnschallenge=true"
  - "--certificatesresolvers.le-dns.acme.dnschallenge.provider=rfc2136"
environment:
  RFC2136_NAMESERVER: "AdresSerweraDNS:53"
  RFC2136_TSIG_KEY: "NazwaKluczaTsig"
  RFC2136_TSIG_ALGORITHM: "hmac-sha512."
  RFC2136_TSIG_SECRET_FILE: "/run/secrets/tsig_secret"
```

Fragment usługi `traefik` w `compose.yaml` ze strony Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01: drugi resolver obok istniejącego HTTP-01. Nazwy zmiennych pochodzą z biblioteki lego, której używa Traefik; przed wdrożeniem sprawdzamy je w dokumentacji naszej wersji. Sekret trzymamy w pliku z Docker secrets albo `.env`, nie w `compose.yaml`.

DNS-01 = sposób potwierdzenia domeny w ACME: urząd certyfikacji każe opublikować jednorazowy rekord TXT _acme-challenge i sprawdza go w DNS; działa bez portu 80 i pozwala na certyfikat wieloznaczny · **HTTP-01** = sposób potwierdzenia domeny w ACME: urząd certyfikacji pobiera jednorazowy plik z adresu /.well-known/acme-challenge/ na porcie 80 naszego serwera

ZMIENIA SYSTEM

Instalacja step-ca na acme01: dnf install step-ca

```
sudo tee /etc/yum.repos.d/smallstep.repo >/dev/null <<'EOT'
[smallstep]
name=Smallstep
baseurl=https://packages.smallstep.com/stable/fedora/
enabled=1
repo_gpgcheck=0
gpgcheck=1
gpgkey=https://packages.smallstep.com/keys/smallstep-0x889B19391F774443.gpg
EOT
sudo dnf makecache && sudo dnf install -y step-cli step-ca
```

```
step-ca version
```

Komendy można wykonać jako blok. Repozytorium producenta podaje pakiety dla rodziny Fedora i RHEL. Najnowsza wersja, którą znaleźliśmy w październiku 2026, to 0.30.2 z 23 marca 2026; wersje starsze niż 0.30.0 mają krytyczną lukę w SCEP (CVE-2026-30836), więc nie instalujemy ich.

Przykład:

```
Smallstep CA/0.30.2 (linux/amd64)
Release Date: 2026-03-23 ...
```

RHEL = Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa · **SCEP** = Simple Certificate Enrollment Protocol: protokół, którym urządzenie samo prosi urząd certyfikacji o wystawienie certyfikatu · **tee** = zapisz strumień wejścia do pliku i jednocześnie wypisz go na ekran · **dnf** = Dandified YUM: menedżer pakietów RHEL/Rocky · **step-ca** = step certificate authority: otwarty urząd certyfikacji Smallstep z ACME, SCEP i własnymi provisionerami

ZMIENIA SYSTEM

Utworzenie urzędu step-ca: step ca init

```
step ca init --deployment-type standalone --name "NazwaUrzeduAcme" --dns "NazwaSerwera"
--address ":443" --provisioner "admin"
```

Tworzy konfigurację, własny urząd główny i urząd pośredni w `$(step path)`. Własny urząd główny zaraz usuniemy, bo podpisem dla `acme01` będzie `Zielona-Root-CA`; kreator jest potrzebny tylko po to, żeby powstały wszystkie pliki konfiguracji.

step = step CLI (Smallstep): narzędzie do certyfikatów, kluczy i zarządzania urzędem step-ca

OSTROŻNIE · NIEODWRACALNE

Podpięcie step-ca pod Zielona-Root-CA: step certificate create --csr

```
shred -u "$(step path)/secrets/root_ca_key"
cp zielona-root-ca.crt "$(step path)/certs/root_ca.crt"
step certificate create "NazwaUrzeduAcme" intermediate.csr intermediate_ca_key --csr --
kty RSA --size 3072
```

Komendy można wykonać jako blok. Usuwa klucz urzędu głównego wygenerowanego przez kreator, podmienia certyfikat główny na `Zielona-Root-CA` i tworzy klucz z żądaniem dla

urzędu pośredniego. Plik `intermediate.csr` jedzie na nośniku na ceremonię `ca-root01`, a podpisany certyfikat wraca jako `$(step path)/certs/intermediate_ca.crt` (klucz trafia do `$(step path)/secrets/intermediate_ca_key`).

shred = Linux: nadpisuj plik albo cały dysk wielokrotnie, żeby utrudnić odzyskanie danych, na SSD nie daje gwarancji · **cp** = copy: skopiuj · **step** = step CLI (Smallstep): narzędzie do certyfikatów, kluczy i zarządzania urzędem step-ca · **RSA** = Rivest, Shamir, Adleman: algorytm szyfrowania kluczem publicznym, którym Vaultwarden podpisuje tokeny sesji, stąd pliki rsa_key* w danych aplikacji

PLIK KONFIGURACYJNY

Ograniczenie nazw w urzędzie: policy w ca.json

```
"policy": {
  "x509": {
    "allow": {
      "dns": ["*.zielona.example", "*.ad.zielona.example"]
    },
    "allowWildcardNames": false
  }
}
```

Fragment pliku `$(step path)/config/ca.json`, wstawiony wewnątrz obiektu `authority` (tak wymaga dokumentacja Smallstep): step-ca wyda certyfikat wyłącznie dla nazw z listy i nie wyda certyfikatu z gwiazdką. To zabezpieczenie po stronie oprogramowania; twarde ograniczenie nazw w samym certyfikacie urzędu (name constraints) wymaga przygotowania na ceremonii i sprawdzamy je osobno.

ZMIENIA SYSTEM

Dodanie provisionera ACME: step ca provisioner add --type ACME

```
step ca provisioner add acme --type ACME
sudo systemctl restart step-ca
```

Od tej chwili `acme01` ma katalog ACME pod adresem `https://acme01.ad.zielona.example/acme/acme/directory`. Domyślna ważność certyfikatów step-ca to 24 godziny; dłuższą (na przykład 7 dni) ustawiamy w opcjach provisionera, a nazwy opcji sprawdzamy w `step ca provisioner add --help`. Usługę systemd zakładamy według dokumentacji „Running step-ca as a daemon”.

□□ **ACME** = Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku ·**step** = step CLI (Smallstep): narzędzie do certyfikatów, kluczy i zarządzania urzędem step-ca ·**systemctl** = system control: sterowanie usługami systemd

□□ ZMIENIA SYSTEM

Certyfikat z wewnętrznego ACME: certbot --server

```
sudo REQUESTS_CA_BUNDLE=/etc/pki/tls/certs/ca-bundle.crt certbot certonly --standalone
--server https://acme01.ad.zielona.example/acme/acme/directory -d "NazwaSerwera"
```

Ten sam certbot, inny urząd. `REQUESTS_CA_BUNDLE` wskazuje magazyn systemowy, w którym jest już `Zielona-Root-CA`, bo inaczej certbot nie zaufa samemu `acme01`. Walidacja HTTP-01 wymaga, żeby `acme01` dotarł do portu 80 serwera.

□□ **ACME** = Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku ·**HTTP-01** = sposób potwierdzenia domeny w ACME: urząd certyfikacji pobiera jednorazowy plik z adresu /.well-known/acme-challenge/ na porcie 80 naszego serwera

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Piątek, 15:50, marzec 2026. Ola zgłasza, że nowy certyfikat dla sklepu B2B kupiony u komercyjnego urzędu „jest za krótki”: zamówiła roczny, a dostała ważny 199 dni. Tomek sprawdza i wyjaśnia, że od 15 marca 2026 żaden publiczny urząd nie wyda dłuższego niż 200 dni, a za rok będzie to 100. Pan Zbigniew pyta, czy w takim razie co trzy miesiące ktoś będzie siedział nad certyfikatami. Odpowiadamy, że nie, i jeszcze w tym miesiącu sklep przechodzi na certyfikat z Let's Encrypt odnawiany przez ACME.

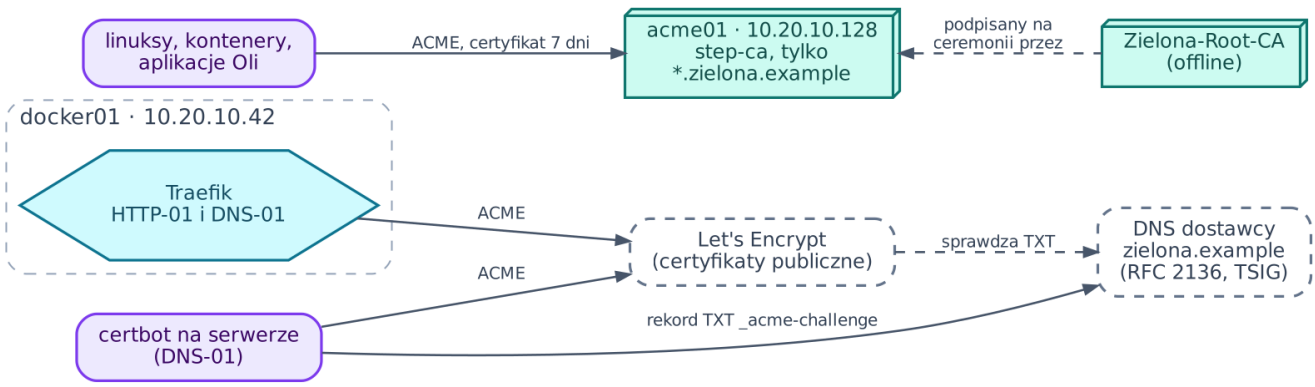
Jak to działa

□□ **Rozwiń: jak to działa pod spodem**

ACME w jednym akapicie

> **Pojęcie: ACME (Automatic Certificate Management Environment).** Protokół, którym program na serwerze sam zakłada konto w urzędzie, prosi o certyfikat, udowadnia, że kontroluje nazwę, odbiera certyfikat i odnawia go przed końcem ważności. Opisany w RFC 8555 z 2019 roku, mówią nim Let's Encrypt, wiele urzędów komercyjnych, step-ca, EJBCA i FreeIPA.

Dowód kontroli nazwy (walidacja) ma trzy popularne odmiany: HTTP-01 (plik pod adresem `http://nazwa/.well-known/acme-challenge/`), DNS-01 (rekord TXT `_acme-challenge.nazwa`) i TLS-ALPN-01 (specjalny certyfikat na porcie 443). Traefik w Zielonej używa HTTP-01, więc port 80 na `docker01` musi być osiągalny z internetu.



Rysunek 1. Dwie drogi ACME w Zielonej: certyfikaty publiczne z Let's Encrypt przez DNS-01 u dostawcy strefy zielona.example albo HTTP-01 przez Traefika na docker01, oraz certyfikaty wewnętrzne z acme01 ze step-ca podpisanego przez Zielona-Root-CA, dla serwerów linuksowych i kontenerów (kliknięcie otwiera pełny rozmiar)

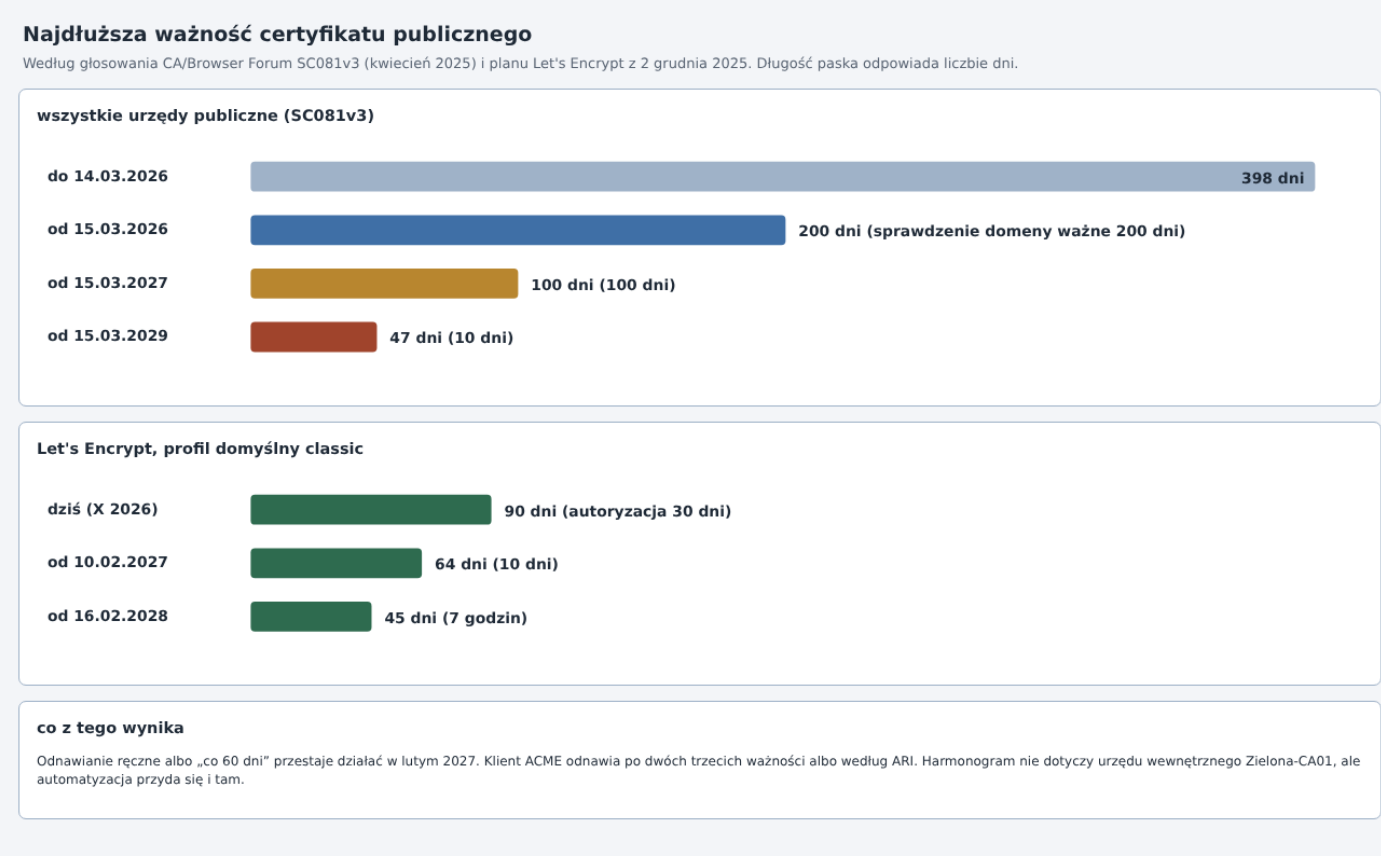
Walidacja	Kiedy wybieramy	Wady
HTTP-01	serwer jest osiągalny z internetu na porcie 80, pojedyncze nazwy	brak certyfikatów z gwiazdką, nie działa dla nazw wewnętrznych
DNS-01	certyfikaty z gwiazdką, nazwy wewnętrzne w domenie publicznej, serwery za zaporą	klucz do zmiany strefy DNS na serwerze; jego wyciek pozwala przejąć domenę
TLS-ALPN-01	serwer ma tylko port 443	mniej klientów, nie działa przez większość proxy

Walidacja	Kiedy wybieramy	Wady
DNS-PERSIST-01	jeden stały rekord `_validation-persist` zamiast zmiany przy każdym odnowieniu	nowa metoda (głosowanie SC-088v3 w październiku 2025); Let's Encrypt planował produkcję na II kwartał 2026, a obsługę w naszym kliencie sprawdzamy przed użyciem

> ⚠ Każdy certyfikat z publicznego urzędu trafia do publicznych dzienników Certificate Transparency. Certyfikat dla `git.zielona.example` z Let's Encrypt ogłasza światu, że taka nazwa istnieje. Dla nazw, których nie chcemy pokazywać, wybieramy certyfikat z gwiazdką albo urząd wewnętrzny.

Harmonogram skracania ważności

W kwietniu 2025 roku CA/Browser Forum przyjęło głosowanie SC081v3. Ustala ono najdłuższą ważność certyfikatów TLS z urzędów publicznie zaufanych i to, jak długo urząd może korzystać z wcześniejszego sprawdzenia kontroli domeny.



Rysunek 2. Harmonogram ważności certyfikatów publicznych: 398 dni do 15 marca 2026, potem 200 dni, od 15 marca 2027 100 dni, od 15 marca 2029 47 dni; obok Let's Encrypt: 90 dni dziś, 64 dni od 10 lutego 2027 i 45 dni od 16 lutego 2028 (kliknięcie otwiera pełny rozmiar)

Od dnia	Najdłuższa ważność certyfikatu	Ponowne użycie sprawdzenia domeny
do 14 marca 2026	398 dni	398 dni
15 marca 2026	200 dni	200 dni
15 marca 2027	100 dni	100 dni
15 marca 2029	47 dni	10 dni

Let's Encrypt ma własny, krótszy harmonogram, ogłoszony 2 grudnia 2025 roku:

Od dnia	Profil	Ważność	Ponowne użycie autoryzacji
dziś (październik 2026)	`classic` (domyślny)	90 dni	30 dni
13 maja 2026	`tlsserver` (do wyboru)	45 dni	według profilu
10 lutego 2027	`classic`	64 dni	10 dni
16 lutego 2028	`classic`	45 dni	7 godzin
bez zmian	`shortlived` (do wyboru)	6 dni	według profilu

Dwie rzeczy z tego wynikają dla Zielonej. Po pierwsze, skrypt albo kalendarz z odnawianiem „co 60 dni” przestanie działać w lutym 2027, więc klient ma odnawiać według ARI albo po dwóch trzecich ważności. Po drugie, od 11 lutego 2026 domyślne certyfikaty Let's Encrypt nie mają zastosowania do uwierzytelniania klienta, a profil `tlsclient` zakończono 8 lipca 2026: certyfikaty publiczne nie nadają się już do logowania serwer do serwera (na przykład wzajemnego TLS między serwerami poczty), do tego służy urząd wewnętrzny.

> **Pojęcie: ARI (ACME Renewal Information).** Rozszerzenie ACME, w którym urząd podpowiada klientowi, kiedy najlepiej odnowić certyfikat. Gdy urząd musi masowo unieważnić certyfikaty po błędzie, przez ARI każe klientom odnowić je wcześniej, a klient z ARI zrobi to bez naszego udziału.

> Harmonogram SC081v3 nie dotyczy urzędów wewnętrznych. `Zielona-CA01` może dalej wydawać certyfikaty serwerów na rok, bo komputery ufają mu z magazynu firmowego, a nie z listy przeglądarek. Krótsza ważność i ACME

> także wewnątrz mają jednak sens: certyfikat, który odnawia się sam, nie wygasa w piątek o 16:00.

Wewnętrzny ACME: step-ca na acme01

AD CS nie mówi protokołem ACME. Serwery z Windows dostają certyfikaty przez automatyczną rejestrację, ale linuksy, kontenery, urządzenia sieciowe i aplikacje Oli dostają je dziś ręcznie, z `certreq` i OpenSSL, według strony Generowanie certyfikatów: OpenSSL i urząd certyfikacji Windows. Własny urząd ACME zamienia to na ten sam mechanizm, którego używamy z Let's Encrypt.

Pytanie	Odpowiedź dla Zielonej
czym jest `acme01`	urzędem podrzędnym `Zielona-Root-CA` ze step-ca, podpisanym na ceremonii, z listą dozwolonych nazw `*.zielona.example` i `*.ad.zielona.example`
czy może wydać certyfikat do logowania w domenie	nie: nie jest w magazynie NTAuth, więc kontroler nie przyjmie jego certyfikatów do logowania
jaka ważność	7 dni dla serwerów z klientem ACME, odnowienie automatyczne
warstwa	0, dopóki certyfikat urzędu nie ma twardego ograniczenia nazw (name constraints); z ograniczeniem do rozważenia warstwa 1
lista unieważnień	przy ważności 7 dni unieważnienie ma małe znaczenie; czy włączamy CRL w step-ca, decydujemy przy wdrożeniu (opis w dokumentacji Smallstep)
co z FreeIPA	serwery zapisane w FreeIPA na `ipa01` mogą zamiast tego używać ACME z Dogtag (`ipa-acme-manage enable`) z urzędem FreeIPA; wtedy ten urząd musi być zaufany na stacjach

> ⚠ `acme01` dostaje certyfikat urzędu, ale nigdy klucza `Zielona-Root-CA` ani `Zielona-CA01`. Klucza urzędu nie eksportujemy poza urząd: step-ca ma własny klucz urzędu pośredniego, a podpis pod nim składa urząd główny na ceremonii.

Droga bez Microsoftu

Ta strona w ogóle nie wymaga Microsoftu: Let's Encrypt, certbot, Traefik i step-ca działają tak samo w firmie z Google Workspace i serwerami na Rocky Linux. Microsoft wchodzi tylko w jednym miejscu: gdy serwer z Windows i IIS potrzebuje certyfikatu publicznego, używamy klienta ACME dla Windows (na przykład win-acme albo Posh-ACME) zamiast certbota, a wewnętrznie dalej automatycznej rejestracji z AD CS.

Częste błędy

Objaw	Przyczyna	Co robimy
`certbot renew --dry-run` kończy się `NXDOMAIN looking up TXT for _acme-challenge`	rekord nie zdążył się rozejść albo klucz TSIG nie ma praw do strefy	dłuższe `--dns-rfc2136-propagation-seconds`, test `nsupdate` z tym samym kluczem
Certyfikat odnowiony, przeglądarka pokazuje stary	usługa nie przeładowała certyfikatu	`--deploy-hook` z przeładowaniem usługi
Let's Encrypt odmawia z `too many certificates`	limit wydań dla tej samej nazwy przy testach	testy zawsze z `--dry-run` albo `--test-cert` (staging)
Klient odrzuca certyfikat z `acme01`	brak `Zielona-Root-CA` w magazynie albo serwer nie podaje certyfikatu pośredniego	`fullchain.pem` zamiast `cert.pem` w konfiguracji usługi, `update-ca-trust` na kliencie
step-ca odmawia wydania dla `sklep.inna-firma.example`	nazwa poza listą dozwolonych w `policy`	to zamierzone; certyfikat dla innej domeny bierzemy z publicznego urzędu
Po lutym 2027 certyfikaty z Let's Encrypt wygasają przed odnowieniem	zadanie odnawiające „co 60 dni” przy ważności 64 dni	timer certbota albo klient z ARI zamiast własnego harmonogramu
Serwer poczty partnera przestał przyjmować nasz certyfikat klienta	certyfikat publiczny bez zastosowania uwierzytelniania klienta (od lutego 2026)	certyfikat klienta z urzędu wewnętrznego albo uzgodnienie z partnerem innego sposobu uwierzytelnienia

□□ Ćwiczenia

1. Marek chce certyfikat dla panelu WMS dostępnego tylko w sieci magazynu pod nazwą `wms.zielona.example`. HTTP-01 czy DNS-01 i dlaczego?

Odpowiedź

DNS-01, bo Let's Encrypt nie dotrze z internetu do serwera w sieci magazynu, a DNS-01 sprawdza tylko rekord w publicznej strefie. Trzeba jednak pamiętać, że nazwa trafi do

dzienników Certificate Transparency; jeśli to przeszkadza, certyfikat bierzemy z `acme01` albo z `Zielona-CA01`.

1. Klucz TSIG z pliku `rfc2136.ini` wyciekł z kopii serwera. Co może zrobić napastnik i co robimy?

Odpowiedź

Może zmieniać rekordy w strefie `zielona.example` w zakresie praw klucza, więc także wystawić sobie certyfikat z Let's Encrypt dla naszych nazw albo przekierować ruch. Natychmiast unieważniamy klucz u dostawcy DNS, wydajemy nowy z najwęższymi prawami (tylko `_acme-challenge`), sprawdzamy strefę i dzienniki Certificate Transparency pod kątem certyfikatów, których nie zamawialiśmy.

1. Ile razy w roku odnowi się certyfikat Let's Encrypt z profilu `classic` od 16 lutego 2028 roku, jeśli klient odnawia po dwóch trzecich ważności?

Odpowiedź

Ważność 45 dni, odnowienie po około 30 dniach, czyli około dwunastu razy w roku. Przy ręcznym odnawianiu to dwanaście okazji do pomyłki, przy ACME zero.

1. Ola pyta, czy `acme01` może wydawać certyfikaty do VPN z EAP-TLS, żeby „wszystko było w jednym miejscu”. Co odpowiadamy?

Odpowiedź

Nie: VPN i Wi-Fi z NPS logują przez domenę, a kontroler przyjmuje do logowania tylko certyfikaty z urzędów w NTAuth z silnym mapowaniem, czyli z `Zielona-CA01`. `acme01` ma ograniczenie do nazw serwerów i służy certyfikatom TLS serwerów; rozdzielenie ról jest tu zaletą, nie wadą.

Powiązane: Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA · Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01 · Certyfikaty SSL: wystawienie, konwersja, weryfikacja · MailCow: codzienna praca z domenami, skrzynkami i spamem · Inwentarz certyfikatów i częste problemy: wygasła CRL, łańcuch, SAN, alarm w Zabbixie · Instalacja serwera FreeIPA na ipa01

Źródła: (odczyt 20 do 26.10.2026) · support.dnsimple.com, „SSL Certificate Validity Changes (2026 - 2029)” (SC081v3, kwiecień 2025: 200, 100, 47 dni) · knowledge.digicert.com, „Domain

validation reuse changes in 2026” (398, 200, 100, 10 dni) · isrg.org, „From 90 to 45” (2.12.2025: profile `tlsserver`, `classic`, `shortlived`, daty 13.05.2026, 10.02.2027, 16.02.2028, ARI) · letsencrypt.org, „DNS-PERSIST-01” (18.02.2026, SC-088v3 z października 2025, plan produkcji na II kwartał 2026) · letsencrypt.org, „Ending TLS Client Authentication” (14.05.2025: 11.02.2026 i 8.07.2026) · isrg.org, „Ending OCSP Support in 2025” (adresy OCSP usunięte 7.05.2025, serwery wyłączone 6.08.2025) · RFC 8555 · eff-certbot.readthedocs.io, wtyczka `certbot-dns-rfc2136` i `certbot reconfigure` · doc.traefik.io, „ACME DNS challenge” i go-acme.github.io/lego, dostawca `rfc2136` (nazwy zmiennych do potwierdzenia w naszej wersji) · smallstep.com/docs, „Installation” (repozytorium RPM), „Run step-ca as an intermediate under an existing root” (`step certificate create --csr`, podpis szablonem SubCA w AD CS), „ACME basics” i „Certificate issuance policies” · github.com/smallstep/certificates/releases (0.30.2, 23.03.2026) · cvefeed.io, CVE-2026-30836 (SCEP w step-ca przed 0.30.0)