Budowa hierarchii: urząd główny offline ca-root01 i urząd wydający ca01

Poziom: zaawansowany

Dotyczy: AD CS na Windows Server 2025, ca-root01 (poza domeną, bez sieci), ca01 (10.20.10.121), IIS, DNS ad.zielona.example, CAPolicy.inf, certutil, certreq, moduł ADCSAdministration

Czas: ~4 h z ceremonią

Strona prowadzi przez budowę hierarchii zaprojektowanej na stronie o projekcie: najpierw urząd główny bez sieci, potem urząd wydający w domenie, publikacja list unieważnień po HTTP i ceremonia klucza z protokołem. Budowa nie zmienia niczego w działającym `CA-Zielona`, więc robimy ją w oknie zmian, ale bez wpływu na użytkowników. Wracamy tu przy odnowieniu urzędu i co pół roku przy ceremonii listy unieważnień.

ZAŁOŻENIA SCENARIUSZA

`ca-root01` to maszyna wirtualna generacji 2 na Hyper-V osobnej stacji administracyjnej (PAW), bez karty sieciowej, z plikami na zaszyfrowanym BitLockerem dysku USB; drugi dysk z kopią leży w sejfie w Swarzędzu. `ca01` to maszyna wirtualna na klastrze `hvclu01`. Budowę planujemy po zakazie zmian, na wtorek 19 stycznia 2027, poza Patch Tuesday i zamknięciem miesiąca.

Skróty użyte na tej stronie (16)

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

Skrót	Co znaczy
ANSI	American National Standards Institute: tu chodzi o kody sterujące kolorem i pozycją kursora w terminalu
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty
CDP	CRL Distribution Point: adres w certyfikacie, pod którym urząd publikuje listę unieważnionych certyfikatów
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
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
HTTP	Hypertext Transfer Protocol: protokół stron WWW
IIS	Internet Information Services: serwer WWW wbudowany w Windows Server
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
MIME	Multipurpose Internet Mail Extensions: oznaczenie typu pliku, które serwer WWW wysyła razem z plikiem, na przykład application/pkix-crl dla listy unieważnień
NTAuth	magazyn NTAuth (NT Authentication): lista urzędów w konfiguracji lasu AD, których certyfikaty mogą służyć do logowania do domeny
PAW	Privileged Access Workstation: osobna stacja administracyjna bez poczty i przeglądarki internetowej, z której zarządzamy kontrolerami i serwerami
USB	Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne

Fiszka

Polecenia na `ca-root01` wykonujemy lokalnym kontem administratora (maszyna nie jest w domenie), na `ca01` kontem `.t0` z grupy Enterprise Admins (instalacja urzędu Enterprise i publikacja w konfiguracji lasu tego wymagają). Pliki między maszynami przenosimy wyłącznie na nośniku z ceremonii.

□□ PLIK KONFIGURACYJNY

Plik zasad urzędu głównego: C:\Windows\CAPolicy.inf na ca-root01

```
[Version]
Signature="$Windows NT$"
```

```
[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=Weeks
CRLPeriodUnits=52
CRLDeltaPeriodUnits=0
AlternateSignatureAlgorithm=0

[CRLDistributionPoint]

[AuthorityInformationAccess]

[BasicConstraintsExtension]
PathLength=1
Critical=Yes
```

Plik zapisujemy przed instalacją roli, w kodowaniu ANSI, jako `CAPolicy.inf`, a nie `CAPolicy.inf.txt`. Puste sekcje `[CRLDistributionPoint]` i `[AuthorityInformationAccess]` sprawiają, że certyfikat urzędu głównego nie ma adresów CDP i AIA, bo nikt nie sprawdza unieważnienia samego korzenia. `AlternateSignatureAlgorithm=0` zostawia klasyczny format podpisu, który rozumieją też starsze urządzenia sieciowe.

ANSI = American National Standards Institute: tu chodzi o kody sterujące kolorem i pozycją kursora w terminalu · **CDP** = CRL Distribution Point: adres w certyfikacie, pod którym urząd publikuje listę unieważnionych certyfikatów · **AIA** = Authority Information Access: miejsce w certyfikacie, które mówi, skąd pobrać certyfikat urzędu, który go podpisał · **NT** = pierwotnie kryptonim N-Ten, od procesora, dla którego system miał powstać; popularnie dziś odczytywane jako New Technology, choć to rozwinięcie nie jest oficjalne: rdzeń dzisiejszego Windows Server

ZMIENIA SYSTEM

Instalacja urzędu głównego: Install-AdcsCertificationAuthority -CAType StandaloneRootCA

```
Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
Install-AdcsCertificationAuthority -CAType StandaloneRootCA -CACommonName
"NazwaUrzeduGlownego" -CADistinguishedNameSuffix "O=NazwaFirmy,C=PL" -CryptoProviderName
"RSA#Microsoft Software Key Storage Provider" -KeyLength 4096 -HashAlgorithmName SHA256
```

```
-ValidityPeriod Years -ValidityPeriodUnits 20 -Force
```

Komendy można wykonać jako blok. Klucz powstaje w programowym dostawcy kluczy na `ca-root01` i nigdy nie opuszcza tej maszyny inaczej niż w zaszyfrowanej kopii urzędu. Dla Zielonej `NazwaUrzeduGlownego` to `Zielona-Root-CA`, a sufiks `O=Zielona sp. z o.o.,C=PL`.

RSA = Rivest, Shamir, Adleman: algorytm szyfrowania kluczem publicznym, którym Vaultwarden podpisuje tokeny sesji, stąd pliki rsa_key* w danych aplikacji · **SHA256** = funkcja skrótu kryptograficznego dająca 256-bitowy odcisk danych

ZMIENIA SYSTEM

Ustawienia urzędu głównego: certutil -setreg

```
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod "Years"
certutil -setreg CA\CRLPeriodUnits 52
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\AuditFilter 127
auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
```

Komendy można wykonać jako blok. Urząd główny wystawia certyfikaty urzędów na najwyżej 10 lat i listę unieważnień ważną rok, bez listy różnicowej. `AuditFilter 127` włącza wszystkie kategorie audytu urzędu, a `auditpol` sprawia, że zdarzenia trafiają do dziennika Security. Na systemie w innym języku niż angielski nazwa podkategorii jest przetłumaczona, więc sprawdzamy ją w `auditpol /list /subcategory:*`.

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

ZMIENIA SYSTEM

Adresy CDP i AIA zapisywane w certyfikatach: Add-CACrlDistributionPoint

```
Get-CACrlDistributionPoint | Remove-CACrlDistributionPoint -Force
Add-CACrlDistributionPoint -Uri
"C:\Windows\System32\CertSrv\CertEnroll\<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl" -
PublishToServer -Force
```

```
Add-CACrlDistributionPoint -Uri
"http://NazwaSerweraPKI/pki/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl" -
AddToCertificateCdp -Force
Get-CAAuthorityInformationAccess | Remove-CAAuthorityInformationAccess -Force
Add-CAAuthorityInformationAccess -Uri
"http://NazwaSerweraPKI/pki/<ServerDNSName>_<CAName><CertificateName>.crt" -
AddToCertificateAia -Force
Restart-Service certsvc
```

Komendy można wykonać jako blok. Usuwamy adresy domyślne (LDAP i HTTP z nazwą serwera), urząd zapisuje listę lokalnie, a do wydawanych certyfikatów trafia tylko adres HTTP. Znaczniki w nawiasach ostrych podstawia urząd: `<CAName>` to nazwa urzędu, `<ServerDNSName>` nazwa serwera. W Zielonej `NazwaSerweraPKI` to `pki.ad.zielona.example`.

CDP = CRL Distribution Point: adres w certyfikacie, pod którym urząd publikuje listę unieważnionych certyfikatów · **AIA** = Authority Information Access: miejsce w certyfikacie, które mówi, skąd pobrać certyfikat urzędu, który go podpisał · **LDAP** = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) · **HTTP** = Hypertext Transfer Protocol: protokół stron WWW

ZMIENIA SYSTEM

Wystawienie listy unieważnień: certutil -crl

```
certutil -crl
```

Urząd podpisuje nową listę i zapisuje ją we wszystkich miejscach z flagą publikacji. Na `ca-root01` robimy to przy budowie i na każdej ceremonii, na `ca01` po każdym unieważnieniu certyfikatu, bo listy publikowanej automatycznie nie chcemy czekać tydzień.

Przykład:

```
CertUtil: -CRL command completed successfully.
```

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

PLIK KONFIGURACYJNY

Plik zasad urzędu wydającego: C:\Windows\CAPolicy.inf na ca01

```
[Version]
Signature="$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
CRLPeriod=Days
CRLPeriodUnits=7
CRLDeltaPeriodUnits=0
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=0

[BasicConstraintsExtension]
PathLength=0
Critical=Yes
```

`LoadDefaultTemplates=0` sprawia, że po instalacji urząd nie wydaje niczego, dopóki sami nie opublikujemy szablonów. To celowe: domyślne szablony (między innymi `WebServer` w wersji 1, podatny na ESC15) nie trafiają na urząd przez przypadek. `PathLength=0` zabrania wydawania z `ca01` kolejnych urzędów.

□□ **NT** = pierwotnie kryptonim N-Ten, od procesora, dla którego system miał powstać; popularnie dziś odczytywane jako New Technology, choć to rozwinięcie nie jest oficjalne: rdzeń dzisiejszego Windows Server

□□ ZMIENIA SYSTEM

Instalacja urzędu wydającego z żądaniem do pliku: Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA

```
Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA -CACommonName
"NazwaUrzeduWydajacego" -CADistinguishedNameSuffix "O=NazwaFirmy,C=PL" -
CryptoProviderName "RSA#Microsoft Software Key Storage Provider" -KeyLength 4096 -
HashAlgorithmName SHA256 -OutputCertRequestFile "C:\PKI\NazwaUrzeduWydajacego.req" -
Force
```

Komendy można wykonać jako blok. Urząd powstaje, ale nie startuje, bo czeka na swój certyfikat od urzędu głównego. Plik `.req` przenosimy na nośniku na ceremonię.

Przykład:

```
ErrorId ErrorString
------- -----------
    398 The Active Directory Certificate Services installation is incomplete. To
complete the installation, use the request file "C:\PKI\Zielona-CA01.req" to obtain a
certificate from an appropriate parent CA. ...
```

Komunikat o niepełnej instalacji jest w tym kroku oczekiwany.

RSA = Rivest, Shamir, Adleman: algorytm szyfrowania kluczem publicznym, którym Vaultwarden podpisuje tokeny sesji, stąd pliki rsa_key* w danych aplikacji · **SHA256** = funkcja skrótu kryptograficznego dająca 256-bitowy odcisk danych · **PKI** = Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów

ZMIENIA SYSTEM

Podpisanie żądania urzędu wydającego na urzędzie głównym: certreq -submit i certutil -resubmit

```
certreq -submit -config "ca-root01\NazwaUrzeduGlownego"
E:\Ceremonia\NazwaUrzeduWydajacego.req
certutil -resubmit NumerZadania
certreq -retrieve -config "ca-root01\NazwaUrzeduGlownego" NumerZadania
E:\Ceremonia\NazwaUrzeduWydajacego.crt
```

Urząd Standalone nie wydaje certyfikatów sam, tylko zostawia żądanie w kolejce. `certutil -resubmit` to świadome zatwierdzenie żądania przez administratora, a `certreq -retrieve` zapisuje gotowy certyfikat na nośnik (gdzie `E:` to nośnik ceremonii).

Przykład:

```
RequestId: 2
RequestId: "2"
Certificate request is pending: Taken Under Submission (0)
```

certreq = narzędzie Windows do tworzenia i wysyłania żądań certyfikatów (CSR) do CA · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

ZMIENIA SYSTEM

Publikacja urzędu głównego w Active Directory: certutil -dspublish RootCA

```
certutil -dspublish -f "C:\PKI\ca-root01_NazwaUrzeduGlownego.crt" RootCA
```

Zapisuje certyfikat urzędu głównego w konfiguracji lasu. Po odświeżeniu zasad grupy każdy komputer w domenie ma go w magazynie zaufanych urzędów głównych, bez osobnego GPO. Wymaga konta z grupy Enterprise Admins.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń · **PKI** = Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów

ZMIENIA SYSTEM

Instalacja certyfikatu urzędu wydającego: certutil -installcert

```
certutil -installcert "C:\PKI\ca01.ad.zielona.example_NazwaUrzeduWydajacego.crt"
Start-Service certsvc
```

Kończy instalację rozpoczętą żądaniem do pliku. Polecenie sprawdza łańcuch i listę unieważnień urzędu głównego, więc zanim go użyjemy, certyfikat i lista `Zielona-Root-CA` muszą leżeć w `C:\PKI` i być osiągalne pod adresem `http://pki.ad.zielona.example/pki/`.

PKI = Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

ZMIENIA SYSTEM

Katalog publikacji w IIS: New-WebVirtualDirectory

```
Install-WindowsFeature Web-Server -IncludeManagementTools
New-Item -ItemType Directory -Path "C:\PKI" -Force
New-WebVirtualDirectory -Site "Default Web Site" -Name "pki" -PhysicalPath "C:\PKI"
```

Komendy można wykonać jako blok. IIS udostępnia katalog `C:\PKI` pod adresem `/pki/`. Typy plików `.crl` i `.crt` IIS zna od instalacji, więc nie dopisujemy typów MIME.

IIS = Internet Information Services: serwer WWW wbudowany w Windows Server · **PKI** = Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów · **MIME** = Multipurpose Internet Mail

Extensions: oznaczenie typu pliku, które serwer WWW wysyła razem z plikiem, na przykład application/pkix-crl dla listy unieważnień

◫◫ ZMIENIA SYSTEM

Alias dla adresów publikacji: Add-DnsServerResourceRecordCName

```
Add-DnsServerResourceRecordCName -ComputerName "NazwaKontroleraDC" -ZoneName
"NazwaDomeny" -Name "pki" -HostNameAlias "NazwaSerwera.NazwaDomeny"
```

> (gdzie `NazwaDomeny` to `ad.zielona.example`, a `NazwaSerwera.NazwaDomeny` to `ca01.ad.zielona.example`; alias wpisany raz w certyfikatach przetrwa przeniesienie publikacji na inny serwer)

◫◫ TYLKO ODCZYT

Sprawdzenie listy z linuksa: openssl crl

```
curl -fsS -o /tmp/ca01.crl http://pki.ad.zielona.example/pki/Zielona-CA01.crl
openssl crl -inform DER -in /tmp/ca01.crl -noout -issuer -lastupdate -nextupdate
```

Pobieramy listę tak, jak zrobi to serwer linuksowy albo `fw01`, i odczytujemy wystawcę oraz daty. Data `nextUpdate` w przeszłości oznacza, że klienci zaczną odrzucać certyfikaty.

Przykład:

```
issuer=C=PL, O=Zielona sp. z o.o., CN=Zielona-CA01
lastUpdate=Jan 19 15:42:10 2027 GMT
nextUpdate=Jan 29 15:42:10 2027 GMT
```

◫◫ **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala · **openssl** = zestaw narzędzi do certyfikatów i szyfrowania · **DER** = binarny, nieczytelny dla człowieka format zapisu certyfikatu

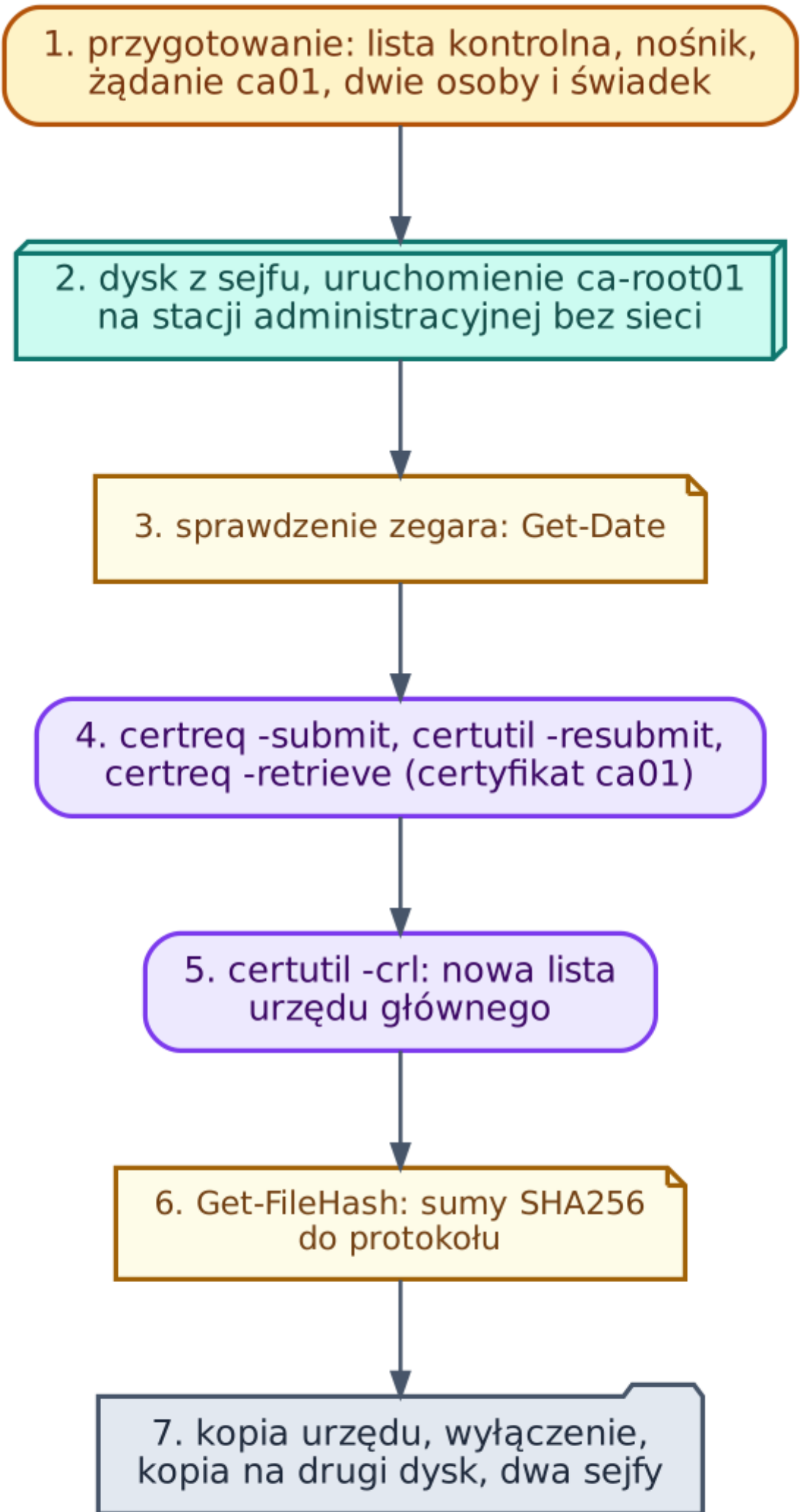
Zanim zaczniemy

◫◫ Z ŻYCIA WZIĘTE

> Wtorek, 16:30, tydzień przed budową. Tomek pyta, po co cała ceremonia, skoro „to trzy kliknięcia w kreatorze”. Pokazujemy mu certyfikat `CA-Zielona` sprzed lat: nikt nie pamięta, kto go zakładał, jakie hasło ma kopia klucza i czy kopia w ogóle istnieje. Ceremonia to te same trzy kliknięcia, tylko z protokołem, świadkiem i dwiema kopiami, dzięki czemu za dziesięć lat ktoś będzie wiedział, co zrobiliśmy.

Wymaganie	Jak sprawdzamy
projekt zatwierdzony (nazwy, ważności, adresy)	strona Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA, zgłoszenie w GLPI
obraz Windows Server 2025 z bieżącymi poprawkami na nośniku	suma kontrolna ISO zgodna z portalem licencyjnym
dwa dyski USB z BitLockerem, hasła i klucze odzyskiwania w Vaultwardenie i w kopercie	`manage-bde -status` na stacji administracyjnej
`ca01` zainstalowany, w domenie, z poprawkami, w jednostce serwerów warstwy 0	`Get-ADComputer ca01` pokazuje właściwą jednostkę
adres 10.20.10.121 wolny i wpisany w NetBox	`Test-Connection 10.20.10.121` bez odpowiedzi przed instalacją
reguły `fw01`: HTTP do `ca01` z VLAN 10, 20, 30 i VPN, RPC do `ca01` tylko z sieci serwerów i stacji	przegląd polityk z zespołem sieci
konto `.t0` z członkostwem czasowym w Enterprise Admins na dzień budowy	`Get-ADGroupMember "Enterprise Admins"`
zgłoszenie zmiany w GLPI z oknem we wtorek 17:00 do 20:00	strona Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć

> **Pojęcie: ceremonia klucza.** Zaplanowane, opisane krok po kroku i zaprotokołowane uruchomienie urzędu głównego. Biorą w niej udział co najmniej dwie osoby (w Zielonej obaj administratorzy) i świadek (pan Zbigniew albo osoba, którą wskaże). Protokół zawiera datę, uczestników, wykonane polecenia, sumy kontrolne plików i miejsca przechowywania nośników, a trafia do GLPI i na papierze do sejfu.


1. przygotowanie: lista kontrolna, nośnik, żądanie ca01, dwie osoby i świadek
2. dysk z sejfu, uruchomienie ca-root01 na stacji administracyjnej bez sieci
3. sprawdzenie zegara: Get-Date
4. certreq -submit, certutil -resubmit, certreq -retrieve (certyfikat ca01)
5. certutil -crl: nowa lista urzędu głównego
6. Get-FileHash: sumy SHA256 do protokołu
7. kopia urzędu, wyłączenie, kopia na drugi dysk, dwa sejfy

Rysunek 1. Ceremonia klucza krok po kroku: przygotowanie nośnika i listy kontrolnej, uruchomienie ca-root01 bez sieci, sprawdzenie zegara, podpisanie żądania ca01 i wystawienie listy, sumy kontrolne, wyłączenie i kopia na dwa dyski, publikacja plików na ca01 i protokół w GLPI (kliknięcie otwiera pełny rozmiar)

Przebieg

Część 1: urząd główny ca-root01

1. Na stacji administracyjnej zakładamy maszynę bez karty sieciowej. Pliki maszyny trzymamy na dysku USB z BitLockerem (`F:` w przykładzie).

```
New-VM -Name "ca-root01" -Generation 2 -MemoryStartupBytes 4GB -NewVHDPath "F:\ca-root01\ca-root01.vhdx" -NewVHDSizeBytes 60GB -Path "F:\ca-root01"
Get-VMNetworkAdapter -VMName "ca-root01" | Remove-VMNetworkAdapter
Add-VMDvdDrive -VMName "ca-root01" -Path "SciezkaDoObrazuISO"
```

1. Instalujemy Windows Server 2025 Standard z poprawkami z nośnika, ustawiamy nazwę `ca-root01`, strefę czasową i silne hasło lokalnego administratora (Vaultwarden i koperta). Maszyny nie dołączamy do domeny.
2. Sprawdzamy zegar: `Get-Date` musi zgadzać się z zegarem stacji. Urząd z cofniętym zegarem wystawi certyfikaty, które „jeszcze nie obowiązują”.
3. Zapisujemy `C:\Windows\CAPolicy.inf` z fiszki i instalujemy urząd główny.
4. Ustawiamy okresy ważności, audyt, adresy CDP i AIA (trzy fiszki), restartujemy usługę i wystawiamy listę `certutil -crl`.
5. Kopiujemy na nośnik ceremonii (`E:`) dwa pliki z `C:\Windows\System32\CertSrv\CertEnroll`: `ca-root01_Zielona-Root-CA.crt` i `Zielona-Root-CA.crl`, i liczymy ich sumy:

```
Get-FileHash -Algorithm SHA256 E:\Ceremonia\*.crt, E:\Ceremonia\*.crl | Format-Table Hash, Path
```

1. Robimy pierwszą kopię urzędu (klucz i baza) na nośnik ceremonii, z hasłem z Vaultwardena. Polecenie i zasady kopii opisuje strona Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza.
2. Nie wyłączamy jeszcze maszyny: za chwilę podpisze żądanie `ca01`.

Część 2: publikacja i urząd wydający ca01

1. Na `ca01` zakładamy katalog `C:\PKI` i katalog wirtualny IIS, a na kontrolerze alias `pki` (fiszki). Kopiujemy do `C:\PKI` oba pliki urzędu głównego z nośnika i porównujemy sumy z protokołem.
2. Publikujemy urząd główny w lesie (`certutil -dspublish ... RootCA`) i dodajemy go lokalnie, żeby `ca01` ufał mu od razu:

```
certutil -addstore -f Root "C:\PKI\ca-root01_Zielona-Root-CA.crt"
```

1. Zapisujemy `C:\Windows\CAPolicy.inf` urzędu wydającego i instalujemy urząd z żądaniem do pliku. Plik `C:\PKI\Zielona-CA01.req` kopiujemy na nośnik ceremonii.
2. Na `ca-root01` podpisujemy żądanie (`certreq -submit`, `certutil -resubmit`, `certreq -retrieve`). Sprawdzamy w `certutil -dump` na nowym certyfikacie, że ma długość ścieżki 0, adres CDP i AIA z `pki.ad.zielona.example` i ważność 10 lat.
3. Na `ca-root01` robimy drugą kopię urzędu (baza zawiera teraz wydany certyfikat `ca01`), wyłączamy maszynę i kopiujemy cały katalog `F:\ca-root01` na drugi zaszyfrowany dysk. Oba dyski idą do sejfów (Pamiątkowo i Swarzędz).
4. Na `ca01` kopiujemy certyfikat do `C:\PKI\ca01.ad.zielona.example_Zielona-CA01.crt`, instalujemy go (`certutil -installcert`) i uruchamiamy usługę.
5. Ustawiamy `ca01`:

```
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod "Years"
certutil -setreg CA\CRLPeriodUnits 7
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLOverlapPeriodUnits 3
certutil -setreg CA\CRLOverlapPeriod "Days"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\AuditFilter 127
auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
Get-CACrlDistributionPoint | Remove-CACrlDistributionPoint -Force
Add-CACrlDistributionPoint -Uri
"C:\Windows\System32\CertSrv\CertEnroll\<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl" -
PublishToServer -Force
Add-CACrlDistributionPoint -Uri "C:\PKI\<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl" -
PublishToServer -Force
Add-CACrlDistributionPoint -Uri
"http://pki.ad.zielona.example/pki/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl" -
AddToCertificateCdp -Force
Get-CAAuthorityInformationAccess | Remove-CAAuthorityInformationAccess -Force
Add-CAAuthorityInformationAccess -Uri
"http://pki.ad.zielona.example/pki/<ServerDNSName>_<CAName><CertificateName>.crt" -
AddToCertificateAia -Force
```

```
Restart-Service certsvc
certutil -crl
```

Komendy można wykonać jako blok. Urząd wystawia listę ważną 7 dni z trzydniową zakładką, czyli nową listę co tydzień, a ostatnia lista działa jeszcze trzy dni po planowanej publikacji, gdyby `ca01` akurat leżał.

1. Odbieramy członkostwo czasowe w Enterprise Admins, zamykamy protokół ceremonii w GLPI z sumami kontrolnymi, numerami seryjnymi obu certyfikatów urzędów i miejscami przechowywania dysków.

Część 3: ceremonia półroczna listy urzędu głównego

Lista `Zielona-Root-CA` jest ważna rok, a wystawiamy ją co pół roku: w marcu i we wrześniu, poza zakazem zmian i zamknięciem miesiąca. Po wystawieniu listy na ceremonii zostaje jeszcze pół roku zapasu na wypadek choroby albo zgubionego klucza do sejfu.

1. Wyjmujemy dysk z sejfu w Pamiątkowie, uruchamiamy `ca-root01` na stacji administracyjnej, sprawdzamy zegar.
2. `certutil -crl`, kopiujemy `Zielona-Root-CA.crl` na nośnik, liczymy sumę, robimy kopię urzędu, wyłączamy maszynę.
3. Na `ca01` podmieniamy plik w `C:\PKI` i sprawdzamy datę `nextUpdate` z linuksa (fiszka).
4. Ten sam dysk po ceremonii kopiujemy na dysk ze Swarzędza przy najbliższej wizycie, żeby oba dyski miały aktualną bazę urzędu.

Weryfikacja

```
certutil -verify -urlfetch "C:\PKI\ca01.ad.zielona.example_Zielona-CA01.crt"
Invoke-WebRequest -Uri "http://pki.ad.zielona.example/pki/Zielona-Root-CA.crl" -
UseBasicParsing | Select-Object StatusCode
certutil -viewstore -enterprise NTAuth
```

Pierwsze polecenie sprawdza łańcuch `ca01` do urzędu głównego razem z pobraniem listy i certyfikatu spod adresów z certyfikatu. Drugie sprawdza, że IIS podaje plik, a trzecie, że `Zielona-CA01` jest w NTAuth obok `CA-Zielona`.

Przykład (skrót):

```
Verified Issuance Policies: All
Verified Application Policies: All
Cert is a CA certificate
Leaf certificate revocation check passed
CertUtil: -verify command completed successfully.

StatusCode
----------
       200
```

Na stacji w biurze po `gpupdate /force` sprawdzamy, że urząd główny dotarł:

```
Get-ChildItem Cert:\LocalMachine\Root | Where-Object Subject -like "*Zielona-Root-CA*" |
Select-Object Subject, NotAfter, Thumbprint
```

Na koniec otwieramy `pkiview.msc`: dla `Zielona-Root-CA` i `Zielona-CA01` wszystkie wiersze mają status OK.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: pkiview.msc z dwoma poziomami hierarchii, Zielona-Root-CA i pod nim Zielona-CA01, wszystkie wiersze CA Certificate, AIA Location i CDP Location ze statusem OK i adresami http://pki.ad.zielona.example/pki/.

Wycofanie zmian

Nowa hierarchia nie obsługuje jeszcze żadnego użytkownika, więc wycofanie nic nie psuje. Na `ca01` usuwamy rolę poleceniem `Uninstall-AdcsCertificationAuthority -Force`, a w `pkiview.msc` (menu Action, Manage AD Containers) usuwamy `Zielona-Root-CA` z zakładek Certification Authorities i AIA oraz `Zielona-CA01` z NTAuthCertificates, AIA i Enrollment Services. Dysków z `ca-root01` nie niszczymy, dopóki nie zdecydujemy, czy budujemy od nowa z inną nazwą, czy powtarzamy ceremonię z tą samą maszyną.

Gdy coś nie zadziała

Objaw	Przyczyna	Co robimy

`certutil -installcert` kończy się błędem `CRYPT_E_REVOCATION_OFFLINE` (0x80092013)	`ca01` nie pobiera listy urzędu głównego spod adresu z certyfikatu	sprawdzamy alias DNS, IIS i plik `Zielona-Root-CA.crl` w `C:\PKI`; w skrajnym razie `certutil -setreg CA\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE` tylko na czas instalacji
Certyfikat `ca01` ma ważność krótszą niż 10 lat	urząd główny miał domyślne `ValidityPeriodUnits` przy podpisie	poprawiamy ustawienie na `ca-root01`, podpisujemy nowe żądanie na kolejnej ceremonii
Po instalacji szablony domyślne są na urzędzie	plik `CAPolicy.inf` zapisany jako `.txt` albo w Unicode	usuwamy szablony `Remove-CATemplate`, przy następnej odnowie poprawiamy plik
Plik `.crl` pobiera się z IIS, ale lista różnicowa nie (błąd 404.11)	włączona lista różnicowa, a jej nazwa ma znak `+`	u nas delty nie ma; gdyby była potrzebna, włączamy w IIS `allowDoubleEscaping` dla katalogu `pki`
Komputery nie mają `Zielona-Root-CA` po tygodniu	publikacja `RootCA` na koncie bez Enterprise Admins albo stacje bez łączności z kontrolerem	`certutil -viewstore "ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=ad,DC=zielona,DC=example?cACertificate?base?objectClass=certificationAuthority"`, potem `gpupdate /force`
Linuksy i kontenery odrzucają certyfikaty z `ca01`	urząd główny jest tylko w magazynach Windows	kopiujemy `Zielona-Root-CA` do `/etc/pki/ca-trust/source/anchors/` i `update-ca-trust`; lista miejsc w inwentarzu

□□ Ćwiczenia

1. Dlaczego certyfikat urzędu głównego nie ma adresów CDP i AIA, a certyfikat `ca01` ma?

Odpowiedź

Urzędowi głównemu klient ufa, bo ma go w magazynie zaufanych, więc nie sprawdza jego unieważnienia ani nie szuka wystawcy. Certyfikat `ca01` podpisał urząd główny, więc klient musi wiedzieć, skąd pobrać listę urzędu głównego, żeby sprawdzić, czy `ca01` nie został unieważniony.

1. Na ceremonii we wrześniu okazuje się, że zegar `ca-root01` wskazuje marzec. Co robimy przed `certutil -crl`?

Odpowiedź

Poprawiamy zegar maszyny (ustawienie godziny w systemie albo synchronizację czasu z hostem w usługach integracji) i sprawdzamy `Get-Date`. Lista wystawiona z datą z marca miałaby `nextUpdate` o pół roku za wcześnie i wygasłaby w przyszłym marcu zamiast we wrześniu.

1. Tomek chce zrobić z `ca01` także serwer publikacji dla `CA-Zielona`, „bo IIS już tam jest”. Co mu odpowiadamy?

Odpowiedź

Że stare certyfikaty mają zapisane adresy z nazwą `dc01` i LDAP, więc klient i tak nie zapyta `ca01`. Publikacja starego urzędu zostaje na `dc01` do wygaśnięcia ostatniego certyfikatu, co opisuje strona Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona.

Powiązane: Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA · Szablony, automatyczna rejestracja i silne mapowanie certyfikatów · Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza · Generowanie certyfikatów: OpenSSL i urząd certyfikacji Windows · Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM

Źródła: (odczyt 20 do 26.10.2026) · learn.microsoft.com, „Prepare the CAPolicy.inf file” i „CAPolicy.inf syntax” (miejsce pliku `%systemroot%`, kodowanie ANSI, sekcje i klucze, `[BasicConstraintsExtension]`) · learn.microsoft.com, `Install-AdcsCertificationAuthority` (parametry `-CAType`, `-CADistinguishedNameSuffix`, `-CryptoProviderName`, `-OutputCertRequestFile`) · learn.microsoft.com, moduł `ADCSAdministration` (`Add-CACrlDistributionPoint`, `Add-CAAuthorityInformationAccess`, znaczniki `<CAName>`, `<ServerDNSName>`) · learn.microsoft.com, „certutil” (`-setreg`, `-crl`, `-dspublish`, `-installcert`, `-resubmit`, `-verify -urlfetch`, `-viewstore -enterprise NTAuth`) i „certreq” (`-submit`, `-retrieve`) · learn.microsoft.com, „Advanced security audit policy: Audit Certification Services” · learn.microsoft.com, „Configure the CDP and AIA extensions” (podwójne kodowanie w IIS dla listy różnicowej)

Revision #2
Created 2026-10-26 14:05:58 UTC by Tomasz Konieczny
Updated 2026-10-26 14:28:19 UTC by Tomasz Konieczny