PKI i certyfikaty: od Diffiego i Hellmana do certyfikatów ważnych 47 dni

Poziom: podstawy

Dotyczy: kryptografia klucza publicznego, X.509, AD CS od Windows 2000 do Windows Server 2025, Let's Encrypt i ACME, step-ca, FreeIPA, stan na 26 października 2026

Czas: ~20 min

Ta strona otwiera książkę o certyfikatach: o tym, skąd przeglądarka, laptop Kasi i zapora `fw01` wiedzą, że rozmawiają z właściwym serwerem. Opowiada, jak z jednego artykułu z 1976 roku wyrósł system, na którym stoi dziś logowanie do VPN, Wi-Fi i każda strona z kłódką, i dlaczego w Zielonej urząd certyfikacji ma zejść z kontrolera domeny.

Pani Halina nie wie, co to certyfikat, a korzysta z niego kilkaset razy dziennie. Kłódka przy adresie Optimy w przeglądarce, Wi-Fi w biurze, które łączy się bez hasła, VPN Kasi w hotelu, podpisana aktualizacja Windows: za każdym razem jakiś program sprawdza, czy druga strona ma podpis od kogoś, komu ufamy. Gdy certyfikat wygaśnie, zgłoszenie brzmi „internet nie działa”, choć internet działa doskonale.

Skróty użyte na tej stronie (23)

Skrót	Co znaczy
ACME	Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku
AD 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
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty
CDP	CRL Distribution Point: adres w certyfikacie, pod którym urząd publikuje listę unieważnionych certyfikatów

Skrót	Co znaczy
CRL	Certificate Revocation List: lista certyfikatów unieważnionych przed upływem ich terminu ważności
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
GCHQ	Government Communications Headquarters: brytyjska służba wywiadu łączności, której kryptolodzy wcześniej niż Diffie, Hellman i RSA opisali klucz publiczny
IEEE	Institute of Electrical and Electronics Engineers: międzynarodowa organizacja inżynierów, która m.in. wydaje normy i przyznaje kamienie milowe w historii techniki
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector: sektor normalizacji Międzynarodowego Związku Telekomunikacyjnego, autor norm X.500 i X.509
LDAPS	LDAP szyfrowany TLS, zwykle port 636
MIT	MIT License: bardzo liberalna licencja wolnego oprogramowania, pozwala na dowolne użycie i modyfikację kodu
NPS	Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi
PKI	Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów
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
RSA	Rivest, Shamir, Adleman: algorytm szyfrowania kluczem publicznym, którym Vaultwarden podpisuje tokeny sesji, stąd pliki rsa_key* w danych aplikacji
SAN	w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
X.500	standard katalogów ITU-T z 1988 roku, pierwowzór modelu danych, na którym oparto później LDAP.

Skąd się wzięło

> **Pojęcie: para kluczy.** Dwa powiązane ze sobą ciągi liczb. Co zaszyfrujemy kluczem publicznym, odczyta tylko klucz prywatny, a co podpiszemy kluczem prywatnym, każdy sprawdzi kluczem publicznym. Klucz publiczny rozdajemy wszystkim, prywatnego nie pokazujemy nikomu.

1976: klucz, który można pokazać

Przez tysiące lat szyfrowanie wymagało wspólnego sekretu: obie strony musiały wcześniej spotkać się i umówić klucz. W listopadzie 1976 roku Whitfield Diffie i Martin Hellman opublikowali artykuł „New Directions in Cryptography”, w którym pokazali, jak dwie osoby mogą uzgodnić sekret przez kanał, który wszyscy podsłuchują. Rok później Ron Rivest, Adi Shamir i Leonard Adleman z MIT opisali RSA, pierwszy praktyczny algorytm, w którym jednym kluczem szyfrujemy, a drugim odszyfrowujemy. Ciekawostka: brytyjscy kryptolodzy z GCHQ doszli do podobnych pomysłów kilka lat wcześniej, ale ich prace odtajniono dopiero w 1997 roku.

1978: skąd wiemy, czyj to klucz

Klucz publiczny rozwiązał jeden problem i otworzył drugi: skąd wiemy, że klucz, który dostaliśmy, naprawdę należy do banku, a nie do kogoś, kto się pod bank podszywa. W maju 1978 roku Loren Kohnfelder w pracy dyplomowej na MIT zaproponował podpisany dokument łączący nazwę z kluczem i nazwał go certyfikatem. W tej samej pracy pojawiła się lista unieważnionych certyfikatów, czyli dzisiejsza CRL.

> **Pojęcie: certyfikat.** Elektroniczny dowód osobisty klucza publicznego: nazwa właściciela, jego klucz publiczny, daty ważności i podpis urzędu, który to poświadcza. Certyfikat sam w sobie nie jest tajny, tajny jest tylko klucz prywatny, który do niego pasuje.

X.509 i urzędy: łańcuch zaufania

W 1988 roku normy X.500, z których wyrósł też Active Directory, dostały część X.509: wspólny format certyfikatu. Wersja trzecia z połowy lat 90. dodała rozszerzenia, w tym pole SAN z listą nazw serwera i pole zastosowań klucza, które do dziś decydują o błędzie 13801 w VPN. W 1995 roku Netscape wprowadził SSL do przeglądarki, a pierwsze komercyjne urzędy zaczęły sprzedawać certyfikaty stronom internetowym.

> **Pojęcie: urząd certyfikacji (CA).** Ktoś, komu ufamy, że sprawdza tożsamość przed podpisaniem certyfikatu. Przeglądarka ufa kilkudziesięciu urzędom głównym wpisanym do

systemu, a komputery w domenie dodatkowo naszemu urzędowi firmowemu.

Pojęcie: PKI (infrastruktura klucza publicznego). Wszystko razem: urzędy, ich klucze, zasady wydawania, listy unieważnień, adresy publikacji, szablony i ludzie, którzy pilnują, żeby to działało. Sam serwer z rolą urzędu to dopiero jedna dziesiąta PKI.

Urząd w każdej firmie: Windows 2000 i AD CS

Microsoft wbudował urząd certyfikacji w Windows Server, a w Windows 2000 połączył go z Active Directory: urząd typu Enterprise czyta konta z katalogu i wydaje certyfikaty według szablonów. Windows Server 2003 dodał szablony w wersji drugiej i automatyczną rejestrację, dzięki której komputer sam prosi o certyfikat i sam go odnawia. Od tej chwili urząd można było postawić w kwadrans, kreatorem, na kontrolerze domeny, i wiele firm, także Zielona, zrobiło dokładnie to.

Gdy urząd zawodzi: DigiNotar i Certified Pre-Owned

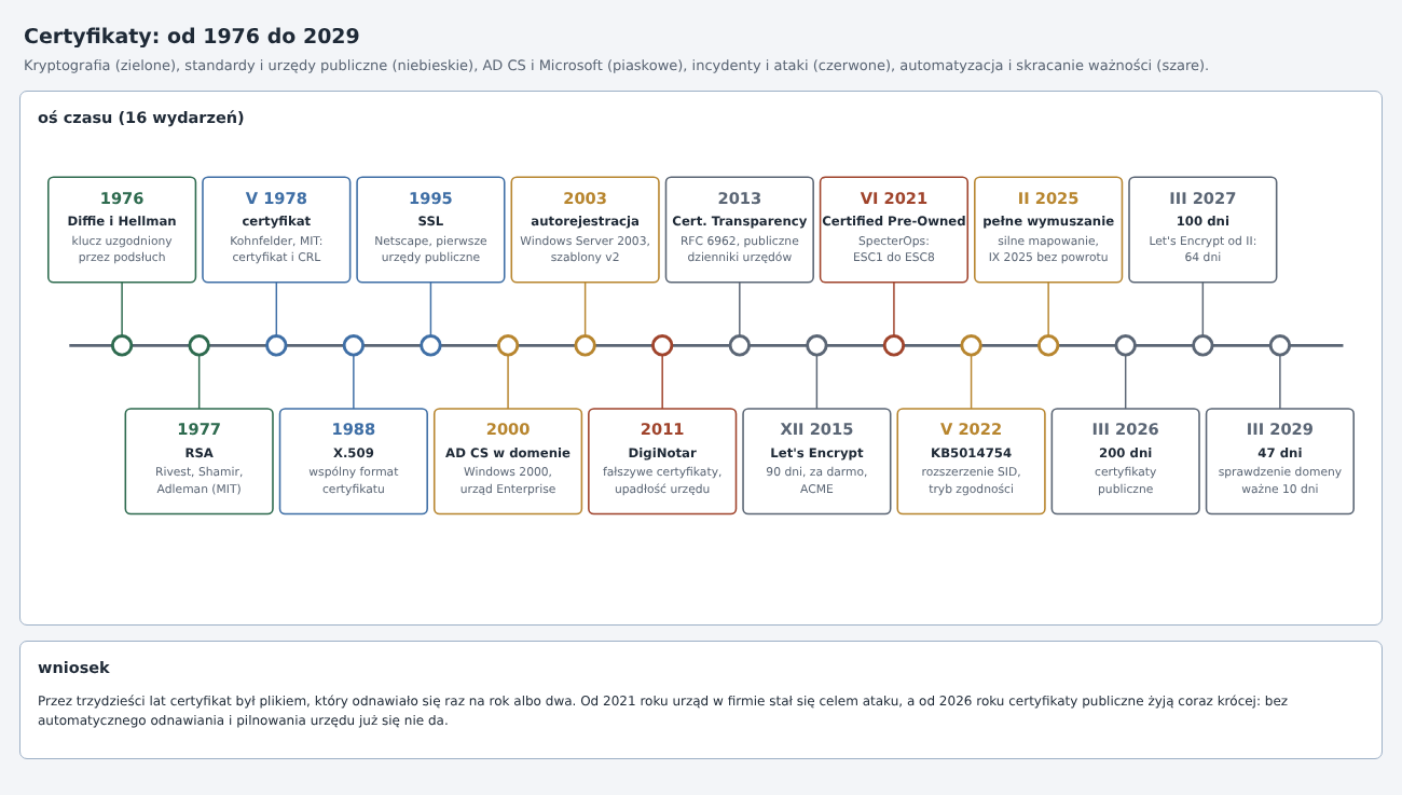
Latem 2011 roku włamywacze przejęli holenderski urząd DigiNotar i wystawili ponad pięćset fałszywych certyfikatów, między innymi dla domen Google. Przeglądarki usunęły DigiNotar z listy zaufanych, a firma zbankrutowała we wrześniu tego samego roku. Odpowiedzią była Certificate Transparency: publiczne dzienniki, w których każdy urząd publiczny zapisuje każdy wydany certyfikat (RFC 6962 z 2013 roku).

W czerwcu 2021 roku Will Schroeder i Lee Christensen ze SpecterOps opublikowali „Certified Pre-Owned” o tym, że źle ustawiony szablon w firmowym AD CS pozwala zwykłemu pracownikowi dostać certyfikat administratora domeny. Ponumerowali błędy od ESC1 do ESC8, a kolejni badacze doszli do ESC16. W maju 2022 roku Microsoft odpowiedział poprawkami do logowania certyfikatem (KB5014754), które od 2025 roku są wymuszane bez możliwości wyłączenia.

Let's Encrypt, ACME i coraz krótsze certyfikaty

W grudniu 2015 roku Let's Encrypt zaczął wydawać darmowe certyfikaty ważne 90 dni, automatycznie, protokołem ACME (opisanym w 2019 roku jako RFC 8555). Krótka ważność okazała się zaletą: certyfikat, który odnawia się sam, nie wygasa w piątek o 16:00. W kwietniu 2025 roku

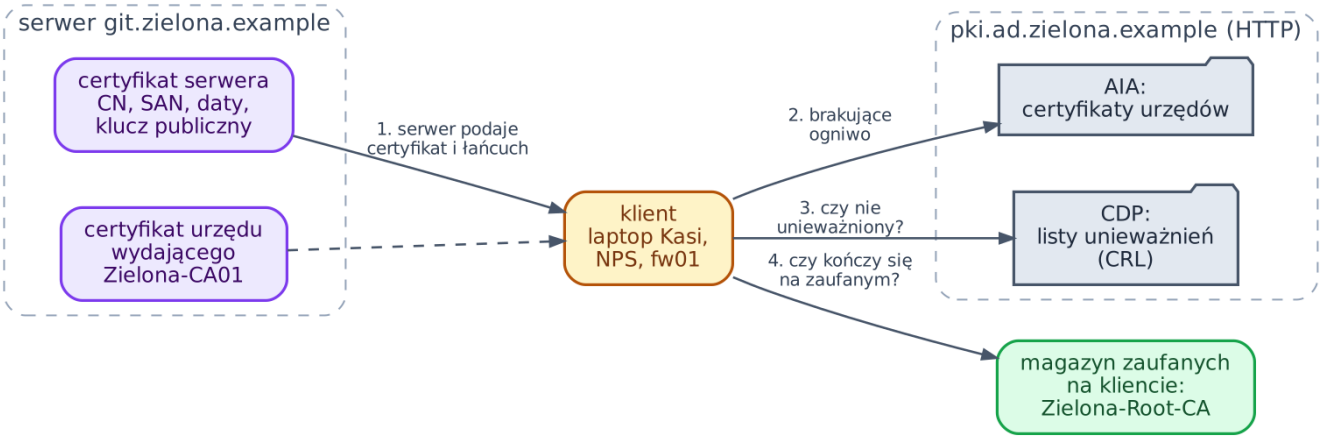
forum urzędów i przeglądarek (CA/Browser Forum) przyjęło harmonogram skracania ważności certyfikatów publicznych: 200 dni od 15 marca 2026, 100 dni od 15 marca 2027 i 47 dni od 15 marca 2029.



Rysunek 1. Oś czasu: od artykułu Diffiego i Hellmana z 1976 roku, przez certyfikat Kohnfeldera, X.509, AD CS, DigiNotar, Let's Encrypt i Certified Pre-Owned, po wymuszenie silnego mapowania w 2025 roku i certyfikaty publiczne ważne 47 dni w 2029 roku (kliknięcie otwiera pełny rozmiar)

Jak to działa w jednym obrazku

Każdy certyfikat w Zielonej kończy się na urzędzie głównym, któremu ufa komputer. Klient idzie od certyfikatu serwera w górę, sprawdza podpisy, pobiera po drodze brakujące certyfikaty urzędów (AIA) i listy unieważnień (CRL), a zatrzymuje się dopiero na certyfikacie, który ma w magazynie zaufanych.



Rysunek 2. Jak klient sprawdza certyfikat: serwer podaje certyfikat i certyfikat urzędu wydającego, klient pobiera brakujące ogniwa spod adresu AIA i listę unieważnień spod adresu CDP, a ufa dopiero urzędowi głównemu z własnego magazynu (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Wtorek, 7:50, styczeń. Wi-Fi w biurze przestaje łączyć laptopy, a VPN handlowców odrzuca certyfikaty, choć nikt niczego nie zmieniał. Tomek po godzinie znajduje przyczynę: lista unieważnień urzędu `CA-Zielona` wygasła w nocy, bo `dc01` był wyłączony przez weekend na wymianę dysku, a NPS na `dc02` bez aktualnej listy odrzuca każdy certyfikat. Pan Zbigniew pyta, czemu firma stoi przez plik, o którym nikt nie słyszał, a pan Wojtek przy następnym audycie pyta, kto ma kopię klucza urzędu i gdzie ona leży.

Urząd `CA-Zielona` powstał lata temu kreatorem na `dc01`, z jednym poziomem i ustawieniami domyślnymi. Od tamtej pory zależą od niego VPN z EAP-TLS, Wi-Fi, certyfikaty serwerów wewnętrznych, LDAPS kontrolerów, inspekcja SSL na `fw01` i profile Intune. Urząd na kontrolerze domeny oznacza, że kopia kontrolera zawiera klucz urzędu, wymiana kontrolera wymaga przenosin urzędu, a kto przejmie urząd, może wystawić sobie certyfikat dowolnego użytkownika. Ta książka opisuje, jak zabezpieczamy obecny urząd od razu i jak po zakazie zmian (od 15 listopada do 6 stycznia) budujemy hierarchię dwupoziomową z urzędem głównym offline.

Co wniosło i co zabrało

Wniosło	Zabrało albo utrudniło

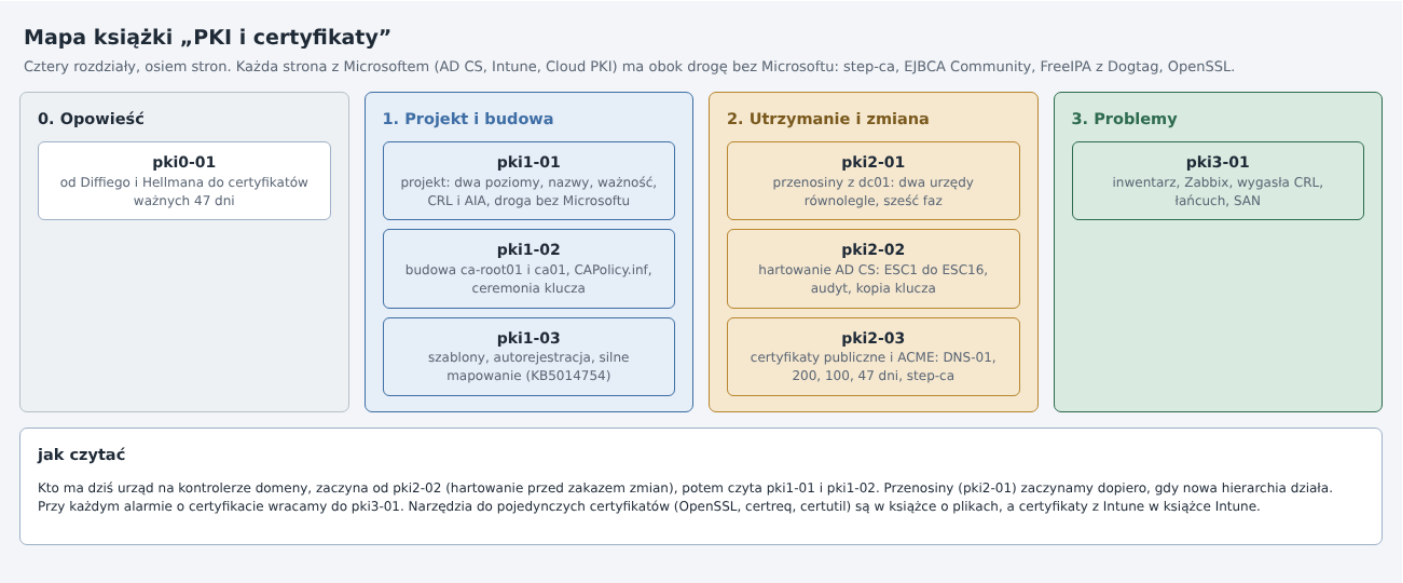
logowanie bez haseł: VPN, Wi-Fi i karty z certyfikatem	jeden źle ustawiony szablon daje drogę do przejęcia domeny
automatyczna rejestracja: certyfikaty odnawiają się same	wygasła lista unieważnień zatrzymuje Wi-Fi i VPN naraz
szyfrowanie każdej usługi wewnętrznej	nikt nie wie, ile certyfikatów mamy i kiedy wygasają
darmowe certyfikaty publiczne i ACME	coraz krótsza ważność: ręczne odnawianie przestaje być możliwe
zaufanie bez spotkania: wystarczy jeden certyfikat urzędu	klucz urzędu jest najcenniejszym plikiem w firmie

Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę
Certyfikat szyfruje dane.	Certyfikat potwierdza, czyj jest klucz. Szyfrują klucze sesji uzgodnione w trakcie połączenia.
Samopodpisany certyfikat jest tak samo bezpieczny, tylko darmowy.	Szyfruje tak samo, ale nikt go nie poświadcza i nie da się go unieważnić. Użytkownicy uczą się klikać „Dalej”.
Własny urząd to jeden serwer z kreatorem.	Urząd to klucz, zasady, publikacja list unieważnień, kopia, audyt i ludzie. Kreator robi tylko pierwszą z tych rzeczy.
Skracanie ważności do 47 dni dotyczy też naszego urzędu.	Dotyczy certyfikatów z urzędów publicznie zaufanych. Nasz urząd wewnętrzny ustala ważność sam, ale automatyzacja przyda się i tak.
Po unieważnieniu certyfikat przestaje działać od razu.	Przestaje działać, gdy klient pobierze nową listę unieważnień. Do tego czasu działa.

Mapa tej książki

Książka ma osiem stron w czterech rozdziałach. Strony z Microsoftem (AD CS, Intune, Cloud PKI) mają obok siebie drogę bez Microsoftu: step-ca, EJBCA Community, FreeIPA z Dogtag i OpenSSL do laboratorium.



Rysunek 3. Mapa książki: opowieść, projekt i budowa hierarchii, szablony z silnym mapowaniem, przenosiny z dc01, hartowanie, certyfikaty publiczne i ACME oraz inwentarz z częstymi problemami (kliknięcie otwiera pełny rozmiar)

0. Opowieść

Strona	Na jakie pytanie odpowiada
PKI i certyfikaty: od Diffiego i Hellmana do certyfikatów ważnych 47 dni	Skąd się wzięły certyfikaty i dlaczego urząd Zielonej schodzi z kontrolera

1. Projekt i budowa

Strona	Na jakie pytanie odpowiada
Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA	Ile poziomów, jakie nazwy i okresy ważności, gdzie publikujemy listy i jaka jest droga bez Microsoftu
Budowa hierarchii: urząd główny offline ca-root01 i urząd wydający ca01	Jak krok po kroku postawić oba urzędy, przeprowadzić ceremonię klucza i opublikować CRL po HTTP
Szablony, automatyczna rejestracja i silne mapowanie certyfikatów	Jakie szablony mamy, kto dostaje certyfikat sam i co zmieniło KB5014754

2. Utrzymanie i zmiana

Strona	Na jakie pytanie odpowiada

Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona	W jakiej kolejności przełączyć komputery, NPS, `fw01`, `conn01` i aplikacje, żeby nikt nie zauważył
Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza	Co zamknąć w obecnym urzędzie od razu i jak sprawdzać to co kwartał
Certyfikaty publiczne i ACME: Let's Encrypt z DNS-01, skracanie ważności i step-ca	Jak żyć z certyfikatami ważnymi 200, 100 i 47 dni i kiedy własny ACME

3. Problemy

Strona	Na jakie pytanie odpowiada
Inwentarz certyfikatów i częste problemy: wygasła CRL, łańcuch, SAN, alarm w Zabbixie	Skąd wiemy, co wygasa, i co robimy, gdy klient odrzuca certyfikat

Narzędzia do pojedynczych certyfikatów (OpenSSL, `certreq`, `certutil`) opisują strony Generowanie certyfikatów: OpenSSL i urząd certyfikacji Windows i Certyfikaty SSL: wystawienie, konwersja, weryfikacja, a dostarczanie certyfikatów przez Intune strona Certyfikaty, Wi-Fi i VPN z Intune: Certificate Connector czy Cloud PKI.

Nota metodyczna: czego nie wiemy

- Liczbę fałszywych certyfikatów DigiNotar podajemy w przybliżeniu („ponad pięćset”), bo raporty z 2011 i 2012 roku różnią się w szczegółach.
- Daty wersji X.509 podajemy z dokładnością do roku albo okresu, bez numerów zaleceń ITU-T.
- Harmonogram skracania ważności dotyczy certyfikatów TLS z urzędów publicznie zaufanych; Let's Encrypt ma własny, osobny harmonogram (strona o ACME).
- Stan odczytaliśmy między 20 a 26 października 2026 roku.

Źródła

Odczyt 20 do 26 października 2026.

Historia: Wikipedia, „Loren Kohnfelder” (praca dyplomowa MIT, maj 1978: certyfikat i lista unieważnień); dspace.mit.edu, „Towards a Practical Public-key Cryptosystem”; Diffie i Hellman, „New Directions in Cryptography”, IEEE Transactions on Information Theory, listopad 1976; Wikipedia, „DigiNotar” (włamanie 2011, upadłość wrzesień 2011); RFC 6962 (Certificate Transparency, 2013); RFC 8555 (ACME, 2019); ithelp.ithome.com.tw o „Certified Pre-Owned” (SpecterOps, czerwiec 2021, Schroeder i Christensen); docs.specterops.io, „Escalation techniques” (ESC1 do ESC16).

Stan 2026: support.microsoft.com, KB5014754 (maj 2022, pełne wymuszanie 11 lutego 2025, koniec obsługi klucza `StrongCertificateBindingEnforcement` 9 września 2025); support.dnsimple.com, „SSL Certificate Validity Changes (2026 - 2029)” (głosowanie SC081v3, kwiecień 2025: 200, 100 i 47 dni); isrg.org, „From 90 to 45” (2 grudnia 2025).

Ilustracje: wszystkie rysunki na tej stronie są własne, narysowane dla tej bazy.

Revision #2
Created 2026-10-26 14:05:54 UTC by Tomasz Konieczny
Updated 2026-10-26 14:28:15 UTC by Tomasz Konieczny