Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-net-certificates

SIECI KOMPUTEROWE

Certyfikaty SSL/TLS, czyli skąd wiesz, z kim rozmawiasz?

W poprzedniej historii **nauczyliśmy Pocztę Internetową używać zamkniętych kopert**. I bardzo dobrze! Tylko pewnego dnia jeden z klientów zadał niewygodne pytanie: „A skąd mam wiedzieć, że za drzwiami naprawdę siedzi ten, z kim chcę rozmawiać?”. Odpowiedzi szukamy w hotelu, w którym każdy może kupić garnitur. Nie każdy powinien jednak dostać klucze do gabinetu dyrektora.

Pięć gwiazdek, złote klamki i dyrektor znikąd

W centrum miasta otwarto luksusowy hotel. Marmur na podłogach, złote klamki, ogromny żyrandol. Na drzwiach napis: „HOTEL KRÓLEWSKI”. Do środka wchodzi gość.

— Dzień dobry. Mam umówione spotkanie z dyrektorem.
— Oczywiście. To ja.
— A skąd mam wiedzieć, że pan jest dyrektorem?
— Bo siedzę w gabinecie dyrektora.
— A dokumenty?
— Mam garnitur!
— Garnitur to nie dokument.
— TO PO CO WYDAŁEM NA NIEGO TRZY TYSIĄCE?!

🤣

Przy **HTTPS** podobne pytanie zadaje przeglądarka. Zanim zaufa połączeniu, chce sprawdzić, czy serwer naprawdę jest uprawniony do posługiwania się nazwą witryny, z którą się łączy. Potrzebuje czegoś więcej niż pięknego logo i zapewnienia „proszę mi wierzyć”.

Certyfikat TLS: dokument powiązany z nazwą domeny

Ochroniarz przy recepcji wyciąga rękę.

— Dokumenty, proszę pana.
— Jakie dokumenty? Przecież jestem dyrektorem!
— To proszę to potwierdzić.
— Na drzwiach jest moje nazwisko.
— A na drzwiach toalety jest napisane „Panowie”. To nie znaczy, że każdy w środku zarządza hotelem.

🤣

W sieci takim dokumentem jest **certyfikat cyfrowy TLS**. Zawiera m.in. nazwę lub nazwy domen, dla których został wystawiony, **klucz publiczny**, okres ważności oraz informacje o wystawcy. Certyfikat jest podpisany cyfrowo, aby można było sprawdzić jego autentyczność i wykryć zmianę zawartości.

Gdy odwiedzasz `hotel.example`, przeglądarka oczekuje certyfikatu odpowiedniego dla tej właśnie nazwy. Certyfikat dla `restauracja.example` nie wystarczy, nawet jeśli właściciel obu obiektów jest ten sam.

— Ale przecież restauracja należy do mnie!
— W dokumentach jest restauracja, a klient przyszedł do hotelu.
— TO NIE MOŻE PAN PRZYJĄĆ, ŻE TO PRAWIE TO SAMO?!
— Nie. Komputery wyjątkowo słabo reagują na „prawie”.

Urząd certyfikacji, czyli kto wystawił dokument?

Po pierwszej kontroli dyrektor przyniósł nowy certyfikat, wydrukowany na złotym papierze.

— Proszę. Dokument gotowy.
— Kto go wystawił?
— Ja.
— Słucham?
— Osobiście. Mam nawet pieczątkę!
— PANIE, TO JEST CERTYFIKAT WYSTAWIONY PRZEZ PANA DLA PANA!
— A kogo miałem poprosić? Konkurencyjny hotel?!

🤣🤣

Samodzielnie podpisany certyfikat, zwany **self-signed**, może być poprawny technicznie i przydatny w środowisku testowym albo w świadomie zarządzanej prywatnej infrastrukturze. Ale zwykła przeglądarka nie zaufa mu automatycznie tylko dlatego, że ktoś starannie go przygotował.

W publicznym WWW najczęściej korzystamy z certyfikatów wystawianych przez **CA (Certificate Authority)**, czyli urząd certyfikacji. CA przeprowadza określoną weryfikację, a następnie podpisuje certyfikat. Dla typowego certyfikatu **DV (Domain Validation)** chodzi przede wszystkim o potwierdzenie kontroli nad nazwą domenową, nie o badanie charakteru właściciela witryny.

— Chciałbym certyfikat dla `hotel.example`.
— Czy kontroluje pan tę domenę?
— Naturalnie.
— Proszę to wykazać.
— Mam wizytówki!
— To nie wystarczy.
— A pięć gwiazdek?
— To też nie.
— A pudełko czekoladek?
— PANIE DYREKTORZE, MY TU WERYFIKUJEMY DOMENĘ, NIE MENU DESEROWE!

Jak udowodnić, że domena jest twoja?

Urząd certyfikacji może poprosić o umieszczenie specjalnej informacji w **DNS** albo udostępnienie pliku lub odpowiedzi pod konkretnym adresem WWW. To tak, jakby urzędnik powiedział dyrektorowi:

— Jeśli naprawdę zarządza pan tym hotelem, proszę wywiesić w recepcji kartkę z numerem, który panu podam.
— Jaki numer?
— 7F2A.
— A mogę napisać „WITAMY SZANOWNĄ KOMISJĘ”?
— Nie. Ma być 7F2A.
— Panowie urzędnicy nie mają za grosz fantazji.

Popularny mechanizm **ACME**, z którego korzysta m.in. Let's Encrypt, pozwala zautomatyzować taką weryfikację, wystawianie i odnawianie certyfikatów. Dzięki temu administrator nie musi co jakiś czas ręcznie biegać z teczką do okienka.

Łańcuch zaufania, czyli urząd nad urzędem

Ochroniarz spojrzał na nowy dokument.

— Wystawił go urząd certyfikacji.
— Tak.
— A kto potwierdził ten urząd?
— Urząd nadrzędny.
— A kto potwierdził nadrzędny?
— Jeszcze wyższy.
— A TAMTEGO?!
— Panie kierowniku, proszę nie krzyczeć na łańcuch zaufania!

🤣🤣

Certyfikat witryny może być podpisany przez **pośredni urząd certyfikacji**, a jego certyfikat — przez kolejny urząd, aż do zaufanego **urzędu głównego (root CA)**. Przeglądarka weryfikuje podpisy, nazwy i inne warunki, a na końcu dochodzi do certyfikatu głównego, któremu jej środowisko już ufa.

To zaufanie nie spada z nieba. Przeglądarki lub systemy operacyjne mają **magazyny zaufanych certyfikatów głównych**, zarządzane według ustalonych reguł. Nie chodzi o nieskończony łańcuch urzędników — chodzi o dotarcie do znanego punktu zaufania.

— Czyli ostatni urząd nie musi za każdym razem pytać kolejnego?
— Nie, jest już na liście zaufanych.
— KTO STWORZYŁ LISTĘ?!
— Panie kierowniku, błagam. Klient od rana stoi przy recepcji.

Klucz publiczny dla każdego. Prywatny? Ani się waż!

Dyrektor postanowił usprawnić obsługę.

— Od dzisiaj rozdawajcie wszystkim klucze!
— Publiczne?
— WSZYSTKIE!
— Prywatnego klucza serwera nie wolno rozdawać.
— Dlaczego?!
— Bo ktoś mógłby podszywać się pod pana serwer.

— A skąd miałby wiedzieć, gdzie jest klucz?
— Umieścił pan go na stronie hotelu. W dziale „Do pobrania”.
— ...
— Z podpisem „Dla wygody klientów”.

🤣🤣🤣

Certyfikat zawiera **klucz publiczny** i może być pokazywany każdemu klientowi. Odpowiadający mu **klucz prywatny** musi pozostać pod kontrolą właściciela serwera. Podczas zestawiania TLS serwer potrafi wykazać posiadanie właściwego klucza prywatnego, dzięki czemu klient nie polega wyłącznie na ładnie wyglądającym dokumencie.

Uwaga: we współczesnym TLS 1.3 klucz z certyfikatu służy przede wszystkim do uwierzytelniania serwera. Klient i serwer uzgadniają osobne, tymczasowe sekrety potrzebne do **szyfrowania** transmisji, zwykle z użyciem wymiany kluczy (ECDHE). Nie należy wyobrażać sobie, że cały Internet szyfruje każdą stronę bezpośrednio kluczem publicznym z certyfikatu.

Handshake TLS, czyli zanim zamkniemy drzwi

Do recepcji podchodzi nowy gość.

— Dzień dobry. Chcę rozmawiać bezpiecznie.
— Proszę. Oto dokument hotelu.
— Sprawdzę nazwę, ważność, podpisy i wystawcę.
— Oczywiście.
— A teraz upewnię się, że rozmawiam z właściwym serwerem, i uzgodnimy klucze rozmowy.
— Bardzo proszę.
— Świetnie. Możemy zamknąć drzwi i rozmawiać.
— Czy życzy pan sobie kawy?
— Nie. Ale poproszę, żeby pan kierownik przestał podsłuchiwać pod drzwiami.

To obraz **TLS handshake**: strony uzgadniają parametry bezpieczeństwa, klient otrzymuje i sprawdza certyfikat serwera, a następnie powstają klucze sesyjne do ochrony dalszej komunikacji. Szczegóły różnią się pomiędzy wersjami TLS, ale sens jest prosty: **najpierw sprawdzamy, z kim rozmawiamy, i ustalamy bezpieczny sposób komunikacji; później przesyłamy dane**.

W zwykłym **HTTPS** certyfikat pokazuje przede wszystkim serwer. Istnieje też **mTLS**, gdzie serwer dodatkowo wymaga certyfikatu od klienta — ale to szczególny przypadek, a nie obowiązek przy każdej wizycie na stronie.

SSL czy TLS? Stara tabliczka na nowym budynku

Ochroniarz zauważył na ścianie napis „CERTYFIKAT SSL”.

— Panie dyrektorze, przecież używamy TLS!
— A dlaczego na tabliczce jest SSL?
— Bo tak się historycznie przyjęło.
— To mamy dwa systemy?!
— Nie. Stare SSL jest przestarzałe i nie powinno być używane, a współczesne bezpieczne połączenia

opierają się na TLS.
— TO CZEMU WSZYSCY NADAL MÓWIĄ „CERTYFIKAT SSL”?!
— Bo stare nazwy mają zadziwiająco długie życie.

🤣

SSL (Secure Sockets Layer) to starsza rodzina protokołów. Dziś używa się **TLS (Transport Layer Security)**; historyczne określenie „certyfikat SSL” nadal funkcjonuje potocznie. Sam certyfikat X.509 nie staje się innym rodzajem dokumentu tylko dlatego, że ktoś użył jednej albo drugiej nazwy. Bezpieczne wdrożenia powinny korzystać ze współczesnych wersji TLS, a nie ze starych SSL.

Termin ważności, czyli dyrektor z dokumentem sprzed wczoraj

O poranku ochroniarz zatrzymuje dyrektora.

— Dokumenty!
— Przecież pracuję tu od dziesięciu lat!
— Certyfikat stracił ważność wczoraj.
— ALE JA SIĘ NIE ZMIENIŁEM!
— Dokument wygasł.
— ALE TO NADAL MÓJ HOTEL!
— Dokument wygasł.
— CHOLERA, CZY PAN MA JAKĄŚ INNĄ ODPOWIEDŹ?!
— Tak. Proszę odnowić certyfikat.

🤣🤣

Każdy certyfikat ma określony **okres ważności**. Przeglądarka sprawdza, czy jest aktualny. Jeśli wygasł lub jest jeszcze nieważny, może wyświetlić ostrzeżenie i zablokować normalne wejście na stronę. Zła data w komputerze potrafi wywołać podobne zamieszanie.

Dlatego administratorzy automatyzują odnawianie i monitorują terminy. Wystawienie certyfikatu raz na zawsze nie jest rozsądnym planem utrzymania strony.

Dokument nieważny, nie ten hotel albo brak całej teczki

Ochroniarz ogląda kolejne dokumenty.

— Ten certyfikat jest dla innego hotelu.
— Ale tego samego właściciela!
— To nadal inna nazwa.
— A ten?
— Wystawił go urząd, którego nie znamy.
— A ten trzeci?
— Brakuje dokumentu pośredniego.
— PANIE DYREKTORZE, ILE PAN MA TYCH TECZEK?!
— Tyle, ile trzeba, żeby ochroniarz miał zajęcie!

Typowe przyczyny błędów to: **niezgodna nazwa domeny**, certyfikat **wygasły**, **niezaufany wystawca**, błędnie skonfigurowany **łańcuch certyfikatów** czy certyfikat, który został **unieważniony**. Przeglądarki mogą ostrzegać także o innych problemach z bezpieczeństwem połączenia.

Przy unieważnieniu sytuacja jest bardziej złożona niż zwykła data ważności: przeglądarki stosują różne mechanizmy i polityki sprawdzania statusu certyfikatów. Nie zawsze każde sprawdzenie odbywa się tak samo i nie zawsze gwarantuje natychmiastowe wykrycie problemu.

Jedna recepcja, wiele hoteli: SNI

Przy jednej bramie stoją tabliczki trzech hoteli. Gość podchodzi do ochroniarza.

— Dzień dobry, poproszę dokument hotelu.
— KTÓREGO?!
— Tego, do którego przyjechałem.
— ALE POD TYM ADRESEM SĄ TRZY HOTELE!
— A gdybym najpierw powiedział, do którego się kieruję?
— O! TO BY BARDZO POMOGŁO!

SNI (Server Name Indication) pozwala klientowi wskazać nazwę serwera podczas zestawiania TLS, dzięki czemu jeden **adres IP** może obsługiwać różne witryny z odpowiednimi certyfikatami. Klasyczne SNI może ujawniać nazwę serwera obserwatorom połączenia; rozwijane mechanizmy, takie jak ECH, mają tę ekspozycję ograniczać w obsługiwanych konfiguracjach.

Certyfikat nie daje pięciu gwiazdek ani gwarancji uczciwości

Dyrektor zebrał pracowników na uroczystej konferencji.

— PANOWIE! MAMY CERTYFIKAT!
— Gratulacje.
— Czyli mamy pięć gwiazdek?!
— Nie. Od tego jest inna ocena.
— Czyli klienci wiedzą, że zawsze mówimy prawdę?!
— Nie.
— CZYLI NIKT NIE MOŻE BYĆ OSZUSTEM, JEŚLI MA CERTYFIKAT?!
— Też nie.
— TO CO TEN DOKUMENT POTWIERDZA?!
— Między innymi to, że właściwy klucz jest związany z odpowiednią domeną i że można zweryfikować przedstawione poświadczenie.
— TO CZEMU NIE NAPISALIŚCIE NA NIM „UCZCIWY DYREKTOR”?!
— Bo na to nie wydaje się certyfikatów TLS.

🤣🤣🤣

To najważniejsze zastrzeżenie: **poprawny certyfikat HTTPS nie dowodzi, że właściciel strony jest uczciwy**. Oszust również może otrzymać poprawny certyfikat dla własnej domeny. Kłódka oznacza zabezpieczone, uwierzytelnione połączenie z daną nazwą — nie gwarancję jakości towaru, prawdziwości treści czy dobrych intencji rozmówcy.

Nie wszystkie certyfikaty sprawdzają to samo: obok popularnych DV istnieją warianty obejmujące dodatkową weryfikację organizacji, np. OV i EV. Nie zmienia to jednak certyfikatu w uniwersalny certyfikat uczciwości.

Finał: dyrektor pokazuje dokumenty

Po wielu dniach wdrażania zasad gość wreszcie wchodzi do hotelu.

— Dzień dobry, mam spotkanie z dyrektorem.
— Oto certyfikat właściwy dla naszej domeny.
— Nazwa się zgadza, certyfikat jest ważny, podpisy i łańcuch zaufania też. Świetnie.
— Czyli możemy rozpocząć bezpieczną rozmowę?
— Tak.
— WSPANIALE! — woła dyrektor. — WRESZCIE WSZYSCY MI UFAJĄ!
— Nie, panie dyrektorze. Ufamy poprawnie sprawdzonej tożsamości serwera.
— A MNIE?!
— Pana poznamy po obsłudze klienta.

🤣

Dyrekcja Hotelu Królewskiego informuje, że garnitur, złote klamki i pięć gwiazdek nie zastępują certyfikatu TLS. Z kolei certyfikat TLS nie zastępuje dobrych manier. Trwa spór, które z tych wymagań jest trudniejsze do spełnienia.