Wprowadzenie do PKI

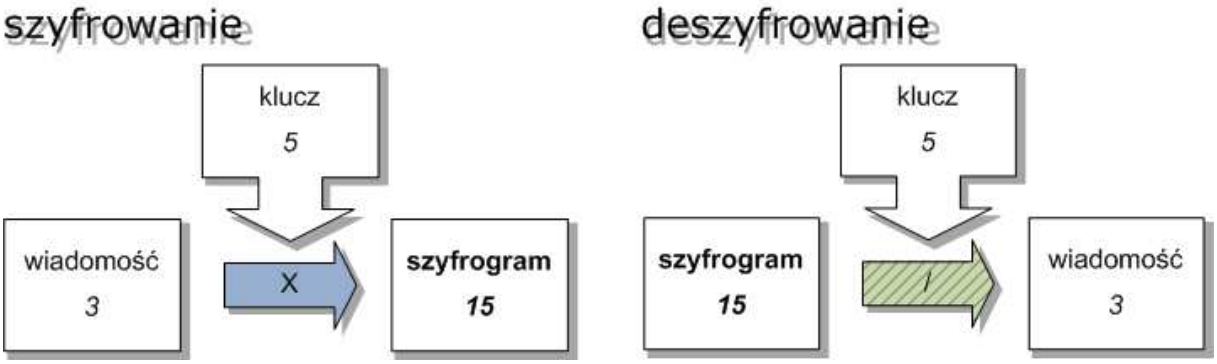
1. Wstęp

Infrastruktura klucza publicznego (ang. PKI - Public Key Infrastructure) to termin dzisiaj powszechnie spotykany. Pod tym pojęciem kryje się standard X.509 opracowany przez europejski instytut standaryzacyjny ITU-T w roku 1988. Norma opisuje między innymi standardowe formaty certyfikatów oraz sposoby weryfikacji ścieżki certyfikacji, które pozwalają utworzyć infrastrukturę wiarygodnego potwierdzania tożsamości.

Zastosowania PKI są bardzo szerokie – od podpisywania poczty elektronicznej, poprzez szyfrowanie różnych wiadomości, po bezpieczne metody uwierzytelniania. Wszystkie te zastosowania opierają się o kryptografię asymetryczną, chociaż są ściśle powiązane także z kryptografią symetryczną.

2. Kryptografia symetryczna

Kryptografia symetryczna polega na zastosowaniu takiego samego klucza w procesie szyfrowania oraz odszyfrowywania wiadomości (Rys. 1). Operacje szyfrowania i deszyfrowania są wzajemnymi odwrotnościami, natomiast klucz pozostaje taki sam.



Rys. 1. Szyfrowanie i deszyfrowanie w kryptografii symetrycznej;
liczby poniżej podpisów w dużym uproszczeniu obrazują wykonywane operacje.

Klucz powinien być tajny, ponieważ jego odtajnienie wiąże się z ujawnieniem informacji zawartej w szyfrogramie. Nakłada to ograniczenia na proces wymiany klucza, który powinien być realizowany bezpieczną metodą. Często wymiana kluczy symetrycznych odbywa się innym kanałem niż wymiana szyfrogramów. Równie skuteczną i powszechnie stosowaną metodą jest zastosowanie kryptografii asymetrycznej do wymiany kluczy symetrycznych.

3. Kryptografia asymetryczna

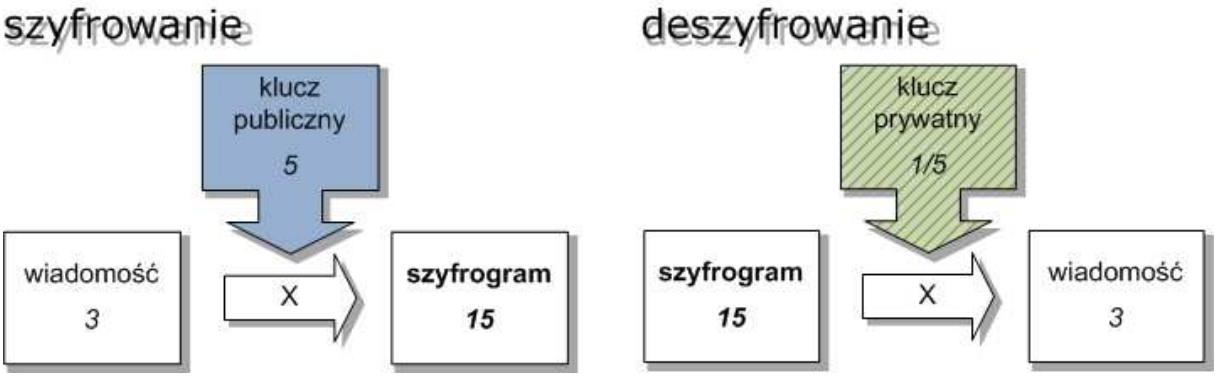
Alternatywą dla kryptografii symetrycznej jest kryptografia asymetryczna. Nazwa wzięła się stąd, że inny klucz używany jest do szyfrowania, a inny odszyfrowywania wiadomości. Klucze odpowiadają sobie wzajemnie i ewentualne uzyskanie klucza prywatnego z publicznego jest bardzo kosztowne numerycznie. Warto wspomnieć tutaj, że nie jest to niemożliwe, natomiast szacuje się że znanymi metodami przetwarzania informacji taka operacja zajęłaby nawet tysiące lat – jest to zależne między innymi od długości obu kluczy. Taki sposób szyfrowania informacji znany jest także pod nazwą kryptografii klucza publicznego, ponieważ jeden z dwóch kluczy podlega upublicznieniu (klucz publiczny).

Zależnie od przeznaczenia procesu szyfrowania informacji do tego celu może być wykorzystany jeden bądź drugi klucz.

W przypadku zapewniania poufności przesyłanej informacji w procesie szyfrowania używany jest klucz publiczny odbiorcy, podczas gdy odszyfrować wiadomość może odbiorca własnym kluczem prywatnym. Klucz publiczny powinien być w takiej sytuacji udostępniony grupie podmiotów, które są zainteresowane szyfrowaniem wiadomości do odbiorcy.

Klucz prywatny jest natomiast wykorzystywany przy składaniu podpisu elektronicznego. Nadawca podpisuje wiadomość swoim kluczem prywatnym, podpis zweryfikować może dowolny posiadacz klucza publicznego .

Kryptografia asymetryczna opiera się o wygenerowanie kompletu kluczy, które są odwrotnością siebie nawzajem. Obrazowo można przedstawić to następująco: klucz1 = 5, klucz2 = 1/5. Wykonanie tej samej operacji na danych z użyciem najpierw jednego, później drugiego klucza odpowiada szyfrowaniu i odszyfrowaniu wiadomości. Przedstawia to poniższy rysunek:

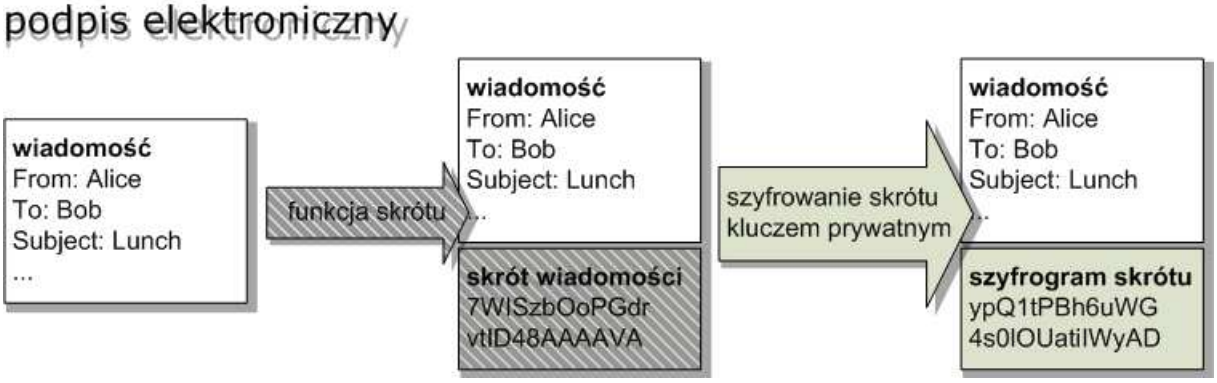


Rys. 2. Szyfrowanie i deszyfrowanie w kryptografii asymetrycznej

Warto wspomnieć, że kryptografia asymetryczna normalizowana przez standard X.509 jest złożona obliczeniowo i często stosowana tylko do bezpiecznej wymiany kluczy symetrycznych. Cechą kryptografii symetrycznej jest mniejsza złożoność obliczeniowa, a co za tym idzie, możliwość wykorzystania jej na przykład do szyfrowania na bieżąco strumienia danych lub danych o stosunkowo dużej objętości. Najczęściej klucze symetryczne wymieniane są co pewien czas, ustalany zależnie od istotności przesyłanych informacji.

4. Podpis elektroniczny

Kryptografia asymetryczna często stosowana jest do podpisywania dokumentów elektronicznych. Proces podpisywania wiadomości obrazuje poniższy diagram:



Rys. 3. Generowanie podpisu elektronicznego

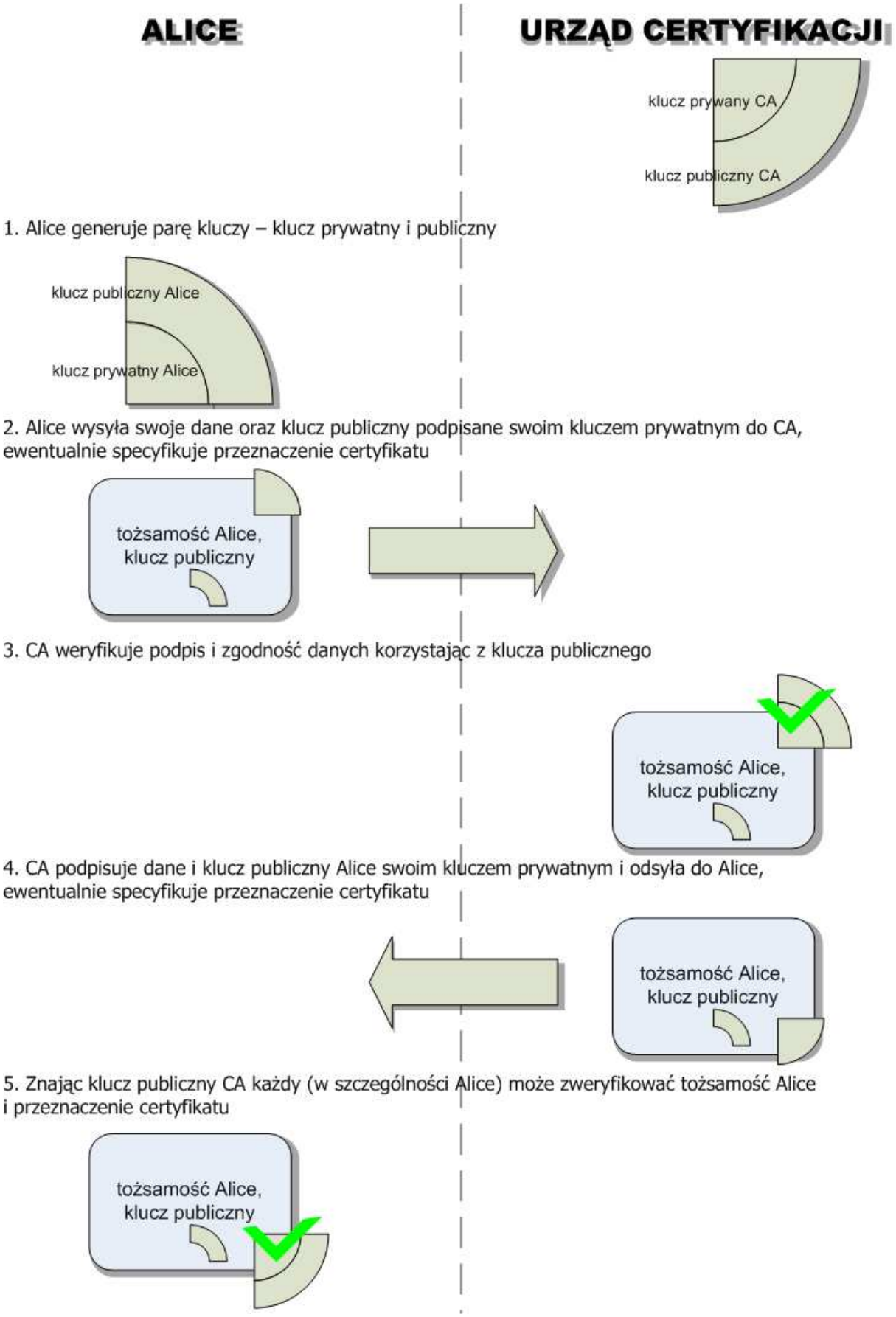
Najpierw generowany jest skrót podpisywanej wiadomości. Funkcja skrótu zapewnia, że w przypadku modyfikacji wiadomości, uzyskany skrót będzie znacząco różnił się od pierwotnego. Następnie skrót podlega zaszyfrowaniu własnym kluczem prywatnym nadawcy. Odbiorca – posiadacz klucza publicznego nadawcy – może odszyfrować skrót i porównać go z samodzielnie wygenerowanym skrótem otrzymanej wiadomości. Jeżeli wiadomość została zmodyfikowana podczas przesyłania, oba skróty będą się różniły.

Podpis elektroniczny wykorzystywany jest w kryptografii klucza publicznego. Urząd certyfikacyjny (ang. Certification Authority – CA) pełni w tym przypadku rolę zaufanego podmiotu, który podpisuje odpowiednio skonstruowany zbiór danych. Posiadanie klucza publicznego CA pozwala w ten sposób zweryfikować prawdziwość przesyłanych danych.

5. Certyfikaty

Certyfikat jest elektronicznym dokumentem (ciągiem danych) pozwalającym powiązać tożsamość podmiotu zapisaną w certyfikacie (np. nazwisko i imię, przeznaczenie certyfikatu) z kluczem publicznym podmiotu. Celowo używany jest zwrot „podmiot”, ponieważ często certyfikacji podlega nie osoba fizyczna, ale np. serwer WWW. Certyfikat zawsze zawiera klucz publiczny podmiotu oraz informacje o reprezentowanym podmiocie. Opcjonalnie może zawierać klucze publiczne urzędów certyfikacji poświadczających tę tożsamość, a nawet klucz prywatny do celów archiwizacji takiego kompletu przez właściciela.

W procesie generowania certyfikatu obie strony (certyfikowany podmiot – Alice i urząd certyfikacji – CA) są w stanie potwierdzić swoją tożsamość dzięki podpisowi elektronicznemu. Wymagane jest tylko bezpieczne dostarczenie klucza publicznego CA do Alice i klucza publicznego Alice do CA. Sposób tworzenia typowego certyfikatu można przedstawić za pomocą poniższego diagramu:



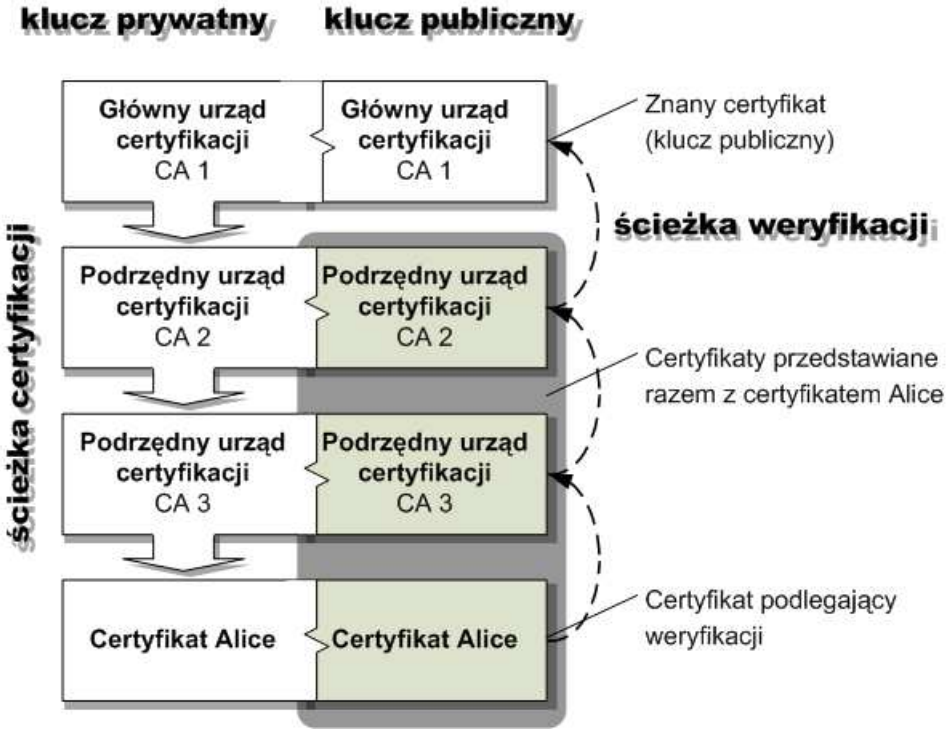
Rys. 4. Schemat procedury wystawiania certyfikatu

6. Ścieżka certyfikacji

Możliwość weryfikacji ścieżki certyfikacji jest kryptograficznym (matematycznym) mechanizmem potwierdzenia prawdziwości danych zawartych w certyfikacie. Opiera się o znajomość klucza publicznego urzędu certyfikacji, który potwierdzał prawdziwość wystawionego certyfikatu podmiotu. Urzędy certyfikacji mogą tworzyć hierarchię, dlatego weryfikacja konkretnego certyfikatu może zostać dokonana w następującej sytuacji:

- certyfikat jest poprawny, jeżeli posiadamy klucz publiczny urzędu certyfikacji, który potwierdza jego autentyczność

Często stosowanym w praktyce podejściem jest przedstawianie jednocześnie certyfikatu konkretnego podmiotu (np. serwera www) wraz z całą ścieżką certyfikacji (kluczami publicznymi kolejnych w hierarchii urzędów). Ilustruje to poniższy rysunek:



Rys. 5. Ścieżka certyfikacji dołączona do weryfikowanego certyfikatu

Znajomość certyfikatu CA 1 pozwala kolejno zweryfikować autentyczność certyfikatów CA 2, CA 3 i wreszcie certyfikatu Alice. Niespójność dowolnego etapu weryfikacji prowadzi do wyświetlenia komunikatu błędu informującego o niemożności sprawdzenia całego łańcucha certyfikacji. Certyfikat głównego urzędu certyfikacji, który może być jedynym w łańcuchu, powinien być dostarczany bezpiecznym medium. Typowo z systemem operacyjnym preinstalowany jest zestaw uznanych na świecie urzędów certyfikacji. Zestaw ten może być uaktualniany, ponadto systemy umożliwiają instalację dodatkowych zaufanych certyfikatów urzędów certyfikacji przez użytkownika.

Na zakończenie należy pamiętać, że poprawność zapewnienia bezpieczeństwa informacji w oparciu o PKI zależy od bezpieczeństwa przekazania certyfikatu stosowanego urzędu certyfikacji. Ten jeden element decyduje o dochowaniu poufności czy możliwości sprawdzenia integralności przesyłanych danych.