STUDIA INFORMATICA 2001
Volume 22 Number 1 (43)

Włodzimierz SOSNOWSKI
PWPT WASKO Sp. z o.o., Zakład Systemów Telekomunikacyjnych

DYSTRYBUCJA KLUCZY PUBLICZNYCH W SYSTEMACH PKI

Streszczenie. Artykuł poświęcony jest systemom kryptograficznym z kluczem jawnym. Artykuł omawia ogólnie podstawowe metody dystrybucji kluczy jawnych. W sposób bardziej szczegółowy przedstawia na przykładach metody dystrybucji kluczy jawnych oraz prywatnych w systemach PKI (ang. *Public Key Infrastructure*).

PUBLIC KEYS DISTRIBUTION IN PUBLIC KEY INFRASTRUCTURE SYSTEMS

Summary. The paper concerns Public Key Cryptographic Systems. It generally discusses basic methods of distribution public keys, especially in Public Key Infrastructure Systems.

1. Wstęp

Systemy teleinformatyczne stanowią obecnie jeden z głównych komponentów pośredniczących w wymianie informacji pomiędzy pracownikami przedsiębiorstwa, klientami oraz firmami współpracującymi. Przy czym przesyłana informacja może przechodzić przez wiele systemów teleinformatycznych, w zależności od aktualnych tablic routingu. Żadna ze stron wymieniających informacje nie ma żadnego wpływu na drogę wykorzystywaną do transmisji danych oraz na zabezpieczenia tranzytowych systemów teleinformatycznych, ograniczające nieupoważniony dostęp do przesyłanych danych. Należy w tym miejscu zauważyć, że informacja jest nierzadko traktowana jako jeden z najcenniejszych towarów, ponieważ ujawniona osobie nieupoważnionej może przesądzić o sukcesie lub porażce podejmowanych przez przedsiębiorstwo działań. Poszukiwana jest

zarówno informacja na temat produktów oferowanych przez firmę, zastosowanych technologii, jak również informacja na temat klientów przedsiębiorstwa.

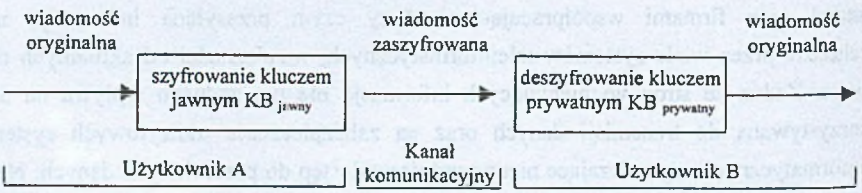
Zapewnienie poufności informacji wymaga stworzenia jednolitej polityki bezpieczeństwa dla całego przedsiębiorstwa, której skala zależy oczywiście od poziomu ważności ochranianych informacji. Jednym z podstawowych środków w realizacji polityki bezpieczeństwa są systemy kryptograficzne, wykorzystujące algorytmy z kluczem jawnym. W związku z tym wymagane jest stworzenie odpowiedniej infrastruktury dla celów generowania, przechowywania oraz dystrybucji kluczy jawnych oraz prywatnych.

2. Podstawowe zastosowania systemów z kluczem jawnym

W systemie z kluczem jawnym każdy użytkownik dysponuje parą związanych ze sobą kluczy: kluczem prywatnym ($KX_{prywatny}$) oraz kluczem jawnym (KX_{jawny}). Wiadomość zaszyfrowana za pomocą jednego ze związanych ze sobą kluczy można rozszyfrować jedynie za pomocą klucza komplementarnego. Przy czym każdy ze związanych ze sobą kluczy może pełnić rolę klucza szyfrującego. Klucz prywatny powinien być znany jedynie "właścicielowi". W związku z tym powinien być dostarczony i przechowywany w sposób bezpieczny, wykluczający jego poznanie przez osoby trzecie. Natomiast klucz jawny może być ujawniony wszystkim zainteresowanym użytkownikom.

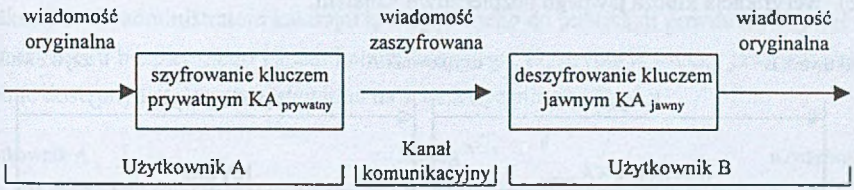
Algorytmy szyfrowania z kluczem jawnym można wykorzystać do dwóch podstawowych celów:

- Zapewnienie poufności wiadomości - użytkownik A szyfruje wiadomość kluczem jawnym użytkownika B (KB_{jawny}). Wiadomość tak zaszyfrowaną może odczytać wyłącznie użytkownik B za pomocą własnego klucza prywatnego ($KB_{prywatny}$). Należy zauważyć, iż taki rodzaj szyfrowania gwarantuje, że zaszyfrowaną wiadomość odczyta wyłącznie użytkownik B, natomiast nie gwarantuje wiarygodności użytkownika A, ponieważ każdy może użyć klucza jawnego użytkownika B (rys. 1).



Rys. 1. Zapewnienie poufności wiadomości
Fig. 1. Message confidentiality

- Uwierzytelnienie wiadomości - użytkownik A szyfruje wiadomość własnym kluczem prywatnym ($KA_{prywatny}$). Każdy użytkownik dysponujący kluczem jawnym użytkownika A (KA_{jawny}) może odszyfrować wiadomość. Ponieważ kluczem $KA_{prywatny}$ dysponuje wyłącznie użytkownik A, tak więc ten schemat szyfrowania gwarantuje jednoznaczne uwierzytelnienie użytkownika A. Oczywiście, powyższy schemat szyfrowania nie gwarantuje poufności, ponieważ każdy może użyć klucza jawnego użytkownika A (rys. 2).



Rys. 2. Uwierzytelnianie wiadomości
Fig. 2. Message authentication

Z punktu widzenia jednoczesnego zachowania poufności i uwierzytelnienia obu stron wymiany informacji użytkownik A powinien zaszyfrować tę samą informację za pomocą własnego klucza prywatnego $KA_{prywatny}$ oraz klucza publicznego użytkownika B (KB_{jawny}).

3. Dystrybucja kluczy jawnych

Wszystkie systemy kryptograficzne wykorzystujące algorytmy z kluczem jawnym wymagają opracowania jednolitej, dla wszystkich użytkowników systemu, strategii dystrybucji kluczy jawnych, przy czym sposób dystrybucji jest funkcją wymagań odnośnie żądanego poziomu zaufania dla klucza jawnego. Podstawowe metody dystrybucji kluczy jawnych [1]:

- publiczne ogłaszanie kluczy jawnych,
- ogólnie dostępny katalog,
- Urząd ds. Kluczy Jawnych,
- Urząd ds. Certyfikatów.

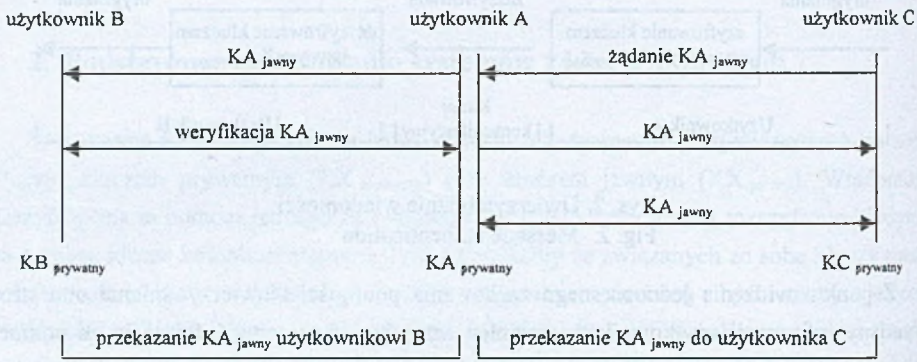
3.1. Publiczne ogłaszanie kluczy jawnych

Sposób ten jest najbardziej intuicyjny i opiera się na przekazywaniu klucza jawnego dostępnym kanałem komunikacyjnym indywidualnie osobom lub grupie osób

zainteresowanych. Przy czym każdy użytkownik musi indywidualnie zarządzać przechowywanymi kluczami, co oznacza, że musi zweryfikować przynależność klucza do konkretnego użytkownika oraz jego ważność. W praktyce oznacza to, że w celu zachowania odpowiednio wysokiego poziomu zaufania do klucza KX_{jawny} każdorazowe wykorzystanie tego klucza powinno być poprzedzone weryfikacją jego ważności.

Czynności związane z dystrybucją klucza jawnego (rys. 3):

1) przesłanie klucza jawnego użytkownikowi zainteresowanemu,
2) weryfikacja klucza jawnego bezpiecznym kanałem.



Rys. 3. Publiczne ogłaszanie kluczy jawnych
Fig. 3. Public announce of key

Podstawowe zalety:

- metoda nie wymaga inwestycji w warstwę sprzętową, programową oraz personel utrzymujący system dystrybucji kluczy jawnych.

Podstawowe wady:

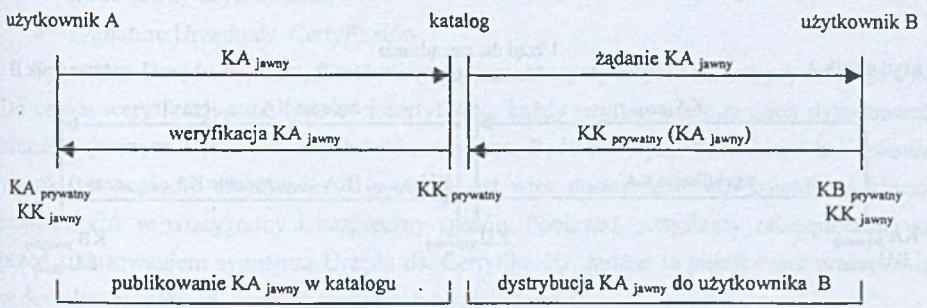
- wszelkie działania związane z zarządzaniem kluczami jawnymi oraz ich weryfikacją spoczywają na użytkownikach,
- każdorazowa zmiana klucza jawnego użytkownika wiąże się z koniecznością ponownego przekazania tego klucza wszystkim zainteresowanym stronom.

3.2. Ogólnie dostępny katalog

Metodę opisaną w poprzednim punkcie można nieco usprawnić poprzez publikowanie kluczy jawnych w ogólnie dostępnym katalogu. Dzięki temu każdy użytkownik dysponujący dostępem do tego katalogu może uzyskać dowolny zapisany w nim klucz jawny KX_{jawny}. W celu zapewnienia możliwości weryfikacji pochodzenia autentyczności uzyskanego klucza jawnego KX_{jawny} zapisane w katalogu klucze jawne powinny być szyfrowane lub

podpisywane za pomocą klucza prywatnego administratora katalogu $KK_{prywatny}$. Każdy użytkownik dysponujący kluczem jawnym administratora katalogu KK_{jawny} może zweryfikować autentyczność pochodzenia otrzymanego klucza jawnego KX_{jawny}. Przy czym klucz KK_{jawny} powinien zostać przekazany użytkownikom w sposób gwarantujący jego autentyczność poprzez bezpieczny kanał komunikacyjny.

W celu zapewnienia odpowiedniego poziomu wiarygodności kluczy jawnych wymagane jest, aby rejestracja każdego klucza jawnego w katalogu odbywała się dopiero po uprzedniej weryfikacji tożsamości podmiotu przez administratora katalogu. W związku z tym również przekazanie do administratora katalogu klucza jawnego do publikacji powinno odbywać przy wykorzystaniu bezpiecznego kanału komunikacyjnego. Dystrybucję kluczy jawnych poprzez ogólnie dostępny katalog przedstawiono na schematycznie na rys. 4.



Rys. 4. Dystrybucja kluczy poprzez ogólnie dostępny katalog
Fig. 4. Keys Distribution by open to the public catalog

Podstawowe zalety:

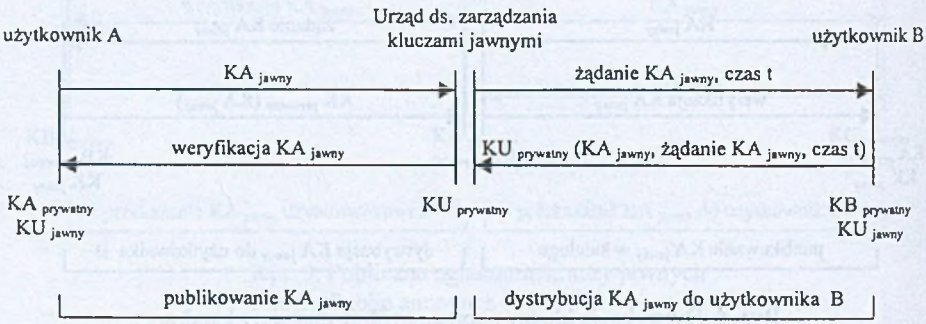
- użytkownik rejestruje swój klucz jawny jednokrotnie w katalogu po uprzedniej jego weryfikacji przez administratora katalogu,
- klucz jawny jest dostępny poprzez katalog dla dowolnej, żądającej tego osoby.

Podstawowe wady:

- na użytkowniku spoczywa konieczność weryfikacji okresu ważności wykorzystania kluczy,
- brak możliwości weryfikacji, czy otrzymany klucz jawny jest aktualnie obowiązującym kluczem; oznacza to, że przestępca może zamiast aktualnego klucza podesłać klucz, który jest już nieaktualny.

3.3. Urząd ds. Kluczy Jawnych

Kolejna modyfikacja poprzedniej metody polega na utworzeniu tzw. Urzędu ds. Kluczy Jawnych. Urząd ten umożliwia nie tylko szyfrowanie lub podpisywanie kluczy jawnych, ale również dokładniejszą kontrolę nad dystrybucją kluczy jawnych. Każdy komunikat wygenerowany przez użytkownika B, zawierający prośbę o udostępnienie klucza jawnego użytkownika A jest uzupełniany o czas jego wysłania TB. Natomiast Urząd odpowiada użytkownikowi B zaszyfrowanym lub podpisanym komunikatem zawierającym: oryginalny komunikat wysłany przez użytkownika B, oryginalny czas TB oraz klucz jawny użytkownika A. Taki zestaw działań uniemożliwia przestępcy wysłanie odpowiedzi zawierającej nieaktualny klucz jawny użytkownika A. Powyższa metoda dystrybucji została przedstawiona na rys. 5.



Rys. 5. Dystrybucja kluczy poprzez Urząd ds. Zarządzania Kluczami Jawnymi
Fig. 5. Keys Distribution by Public-key Authority

Podstawowe zalety:

- użytkownik rejestruje swój klucz jawny jednokrotnie w katalogu, po uprzedniej jego weryfikacji przez administratora katalogu,
- klucz jawny jest dostępny poprzez katalog dla dowolnego, żądającego tego użytkownika,
- system chroni przed możliwością podesłania przez przestępcę starego klucza.

Podstawowe wady:

- na użytkowniku spoczywa konieczność weryfikacji okresu ważności wykorzystywanych kluczy.

3.4. Urząd ds. Certyfikatów

Kolejne usprawnienie metod dystrybucji opisanych w poprzednich punktach opiera się na wystawianiu kluczom jawnym certyfikatów. Certyfikat wydaje tzw. Urząd ds. Certyfikatów CA (ang. *Certification Authority*) po uprzedniej weryfikacji tożsamości podmiotu będącego właścicielem tego klucza jawnego. Przy czym dystrybucji podlega nie sam klucz jawny, ale klucz jawny wraz z certyfikatem wystawionym przez Urząd ds. Certyfikatów.

Każdy certyfikat zawiera między innymi następujące informacje [1]:

- informacje na temat CA wydającego i sygnującego certyfikat,
- okres ważności certyfikatu (od-do),
- podstawowe dane osobowe użytkownika klucza,
- klucz jawny użytkownika,
- sygnaturę Urzędu ds. Certyfikatów.

Sygnatura Urzędu ds. Certyfikatów jest generowana przy użyciu klucza prywatnego CA. Do celów weryfikacji autentyczności certyfikatu, każdy użytkownik powinien dysponować kluczem jawnym CA, które wystawiło certyfikat. Podstawowym warunkiem zachowania wysokiego poziomu niezawodności systemu jest więc dostarczenie użytkownikom klucza jawnego CA w wiarygodny i bezpieczny sposób. Ponieważ certyfikaty zabezpieczone są przed sfałszowaniem sygnaturą Urzędu ds. Certyfikatów, można je publikować praktycznie w dowolny sposób, np. poprzez serwer usług katalogowych.

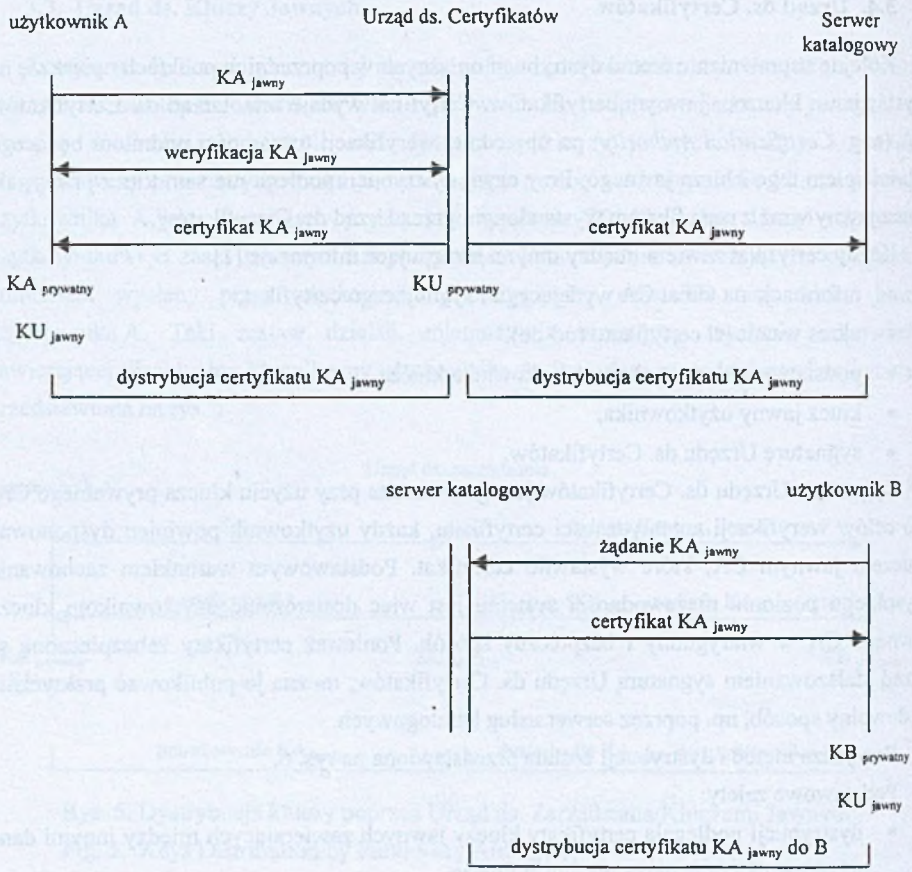
Powyższa metoda dystrybucji została przedstawiona na rys. 6.

Podstawowe zalety:

- dystrybucji podlegają certyfikaty kluczy jawnych zawierających między innymi dane użytkownika oraz okres ważności klucza.

Podstawowe wady:

- konieczność zainwestowania w stworzenie infrastruktury do dystrybuowania oraz zarządzania kluczami jawnymi.



Rys. 6. Dystrybucja kluczy jawnych poprzez Urząd ds. Certyfikatów
Fig. 6. Keys Distributions by Certification Authority

4. Dystrybucja kluczy prywatnych

Klucz prywatny w systemach z kluczem jawnym powinien jednoznacznie identyfikować posługujący się nim podmiot, tak więc wymagane jest zapewnienie odpowiedniego poziomu wiarygodności klucza prywatnego w zależności od ważności informacji ochranianej przez ten klucz. Wiąże się to nie tylko z zapewnieniem odpowiednich procedur weryfikacji podmiotu ubiegającego się o klucz, ale również z zagwarantowaniem bezpiecznych i wiarygodnych kanałów dystrybucji oraz bezpiecznych metod przechowywania tych kluczy przez ich użytkowników. Należy w tym miejscu również zaznaczyć, że szczególnie w przypadku

przedsiębiorstw istotnym problemem jest możliwość odtworzenia klucza prywatnego w razie jego zgubienia. Wiąże się to więc z koniecznością archiwizowania kluczy jawnych oraz prywatnych wszystkich użytkowników systemu.

W związku z tym w przypadku średnich i dużych przedsiębiorstw klucze publiczne powinny być generowane i zarządzane przez uprawnione organa, a dopiero następnie dystrybuowane do użytkowników końcowych.

Klucz prywatny może być zapisany na dowolnym nośniku, przy czym powinien być przechowywany w postaci zaszyfrowanej. W praktyce wykorzystuje się następujące podstawowe rodzaje nośników:

1. Nośniki magnetyczne (dyskietka) - w zasadzie umożliwiają jedynie przechowywanie kluczy prywatnych. Każdy użytkownik otrzymuje dyskietkę z zapisanym kluczem prywatnym oraz kluczem jawnym. Oprogramowanie działające na stacji roboczej powinno gwarantować, że dostęp do klucza prywatnego w postaci jawnej będzie możliwy dopiero po poprawnym podaniu przez użytkownika hasła.
2. Karty magnetyczne - jak wyżej, przy czym karta magnetyczne wymaga stosowania specjalizowanych czytników instalowanych przy każdej stacji roboczej.
3. Karty pamięci - jak wyżej.
4. Karty mikroprocesorowe - karty te zawierają wbudowany mikroprocesor, na którym działa system operacyjny. System operacyjny umożliwia między innymi wykonywanie operacji szyfrowania/deszyfrowania. Zaimplementowany na karcie system plików umożliwia nie tylko przechowywanie kluczy prywatnych, ale również dodatkowych danych, np. danych do logowania się do domeny NT (nazwa użytkownika oraz hasło). Dostęp do danych zapisanych na karcie wymaga podania hasła. Karty mikroprocesorowe wymagają stosowania specjalizowanych czytników.
5. Wirtualny schowek certyfikatów - klucze prywatne wszystkich użytkowników oraz wszelkie dodatkowe dane przynależne użytkownikom są przechowywane w centralnej bazie danych. Informacje te są pobierane do lokalnego schowka certyfikatów umieszczanego w pamięci komputera, na którym pracuje użytkownik dopiero po podaniu poprawnego hasła.

5. Dystrybucja kluczy w systemie PKI

W systemach klucza publicznego PKI standardową metodą gwarantowania autentyczności kluczy jest użycie Urzędu ds. Certyfikatów CA (ang. *Certificate Authority*). CA jest systemem, który wydaje cyfrowe certyfikaty, gwarantujące jednoznaczną identyfikację wszystkich stron wymieniających informację. Cyfrowy Certyfikat zawiera dane

personalne użytkownika, klucz publiczny oraz podpis CA. Oznacza to, że CA poświadcza autentyczność danych posiadacza certyfikatu.

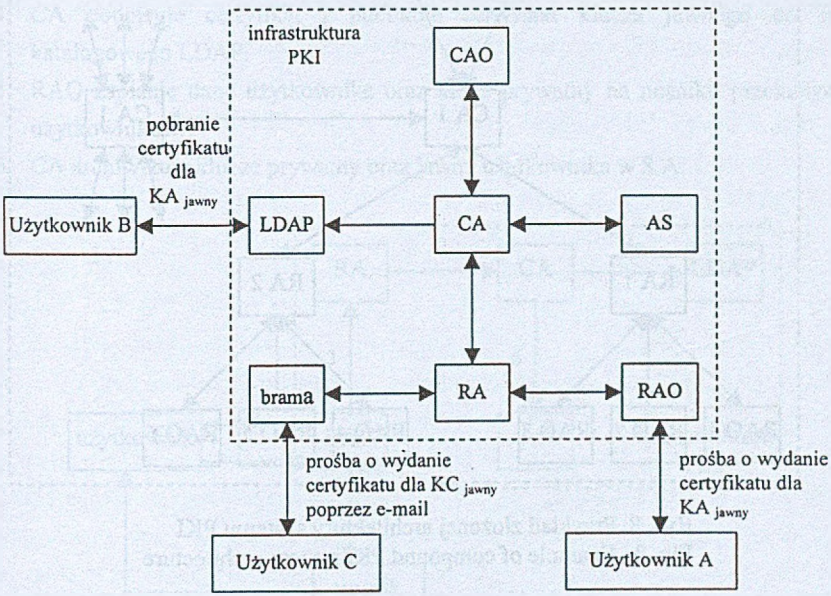
5.1. Architektura systemu PKI

Podstawowe komponenty systemu PKI oraz ich funkcje:

- Urząd ds. Certyfikatów CA:
  - podpisywanie certyfikatów wszystkich użytkowników oraz certyfikatów innych CA
  - podpisywanie listy certyfikatów unieważnionych CRL (ang. *Certificate Revocation List*)
  - dystrybuowanie podpisanych certyfikatów oraz podpisanych list CRL do serwerów katalogowych LDAP (ang. *Lightweight Directory Access Protocol*) lub X.500
  - archiwizowanie kluczy jawnych oraz prywatnych,
  - generowanie kluczy publicznych dla siebie oraz dla CAO (ang. *Certificate Authority Operator*)
- Oficer Urzędu ds. Certyfikatów CAO (ang. *Certificate Authority Operator*):
  - kreowanie oraz zarządzanie polityką bezpieczeństwa przedsiębiorstwa
  - unieważnianie certyfikatów
  - generowanie kluczy publicznych dla nowych modułów infrastruktury PKI
- Urząd ds. Rejestracji RA (ang. *Registration Authority*):
  - pośredniczenie w komunikacji między CA i RAO (ang. *Registration Authority Operator*)
- Oficer Urzędu ds. Rejestracji RAO:
  - aprobowanie lub nie prób o wydanie certyfikatów
  - generowanie kluczy prywatnych oraz jawnych użytkowników
  - przesyłanie zaaprobowanych oraz odrzuconych prób o wydanie certyfikatów do RA
- Bramy do innych systemów (ang. *Gateway*)
  - odbieranie próśb o wydanie certyfikatów od zdalnych użytkowników i przesyłanie ich do RA. Przesyłanie wydanych certyfikatów do użytkowników. Przykłady bram:
    - brama WEB — umożliwia wykorzystanie przeglądarki WEB do wysyłania próśb o wydanie certyfikatów oraz ich odbieranie
    - brama e-mail — umożliwia wykorzystanie poczty elektronicznej do wysyłania próśb o wydanie certyfikatów oraz ich odbieranie

- Serwer archiwizacyjny AS (ang. *Archive Server*):
  - archiwizacja jawnych oraz prywatnych kluczy użytkowników w postaci zaszyfrowanej
- Serwer katalogowy LDAP
  - udostępnienia wszystkim użytkownikom systemu listy ważnych oraz unieważnionych certyfikatów przekazanych i podpisanych przez serwer CA.

Typową architekturę systemu przedstawiono na rys. 7.



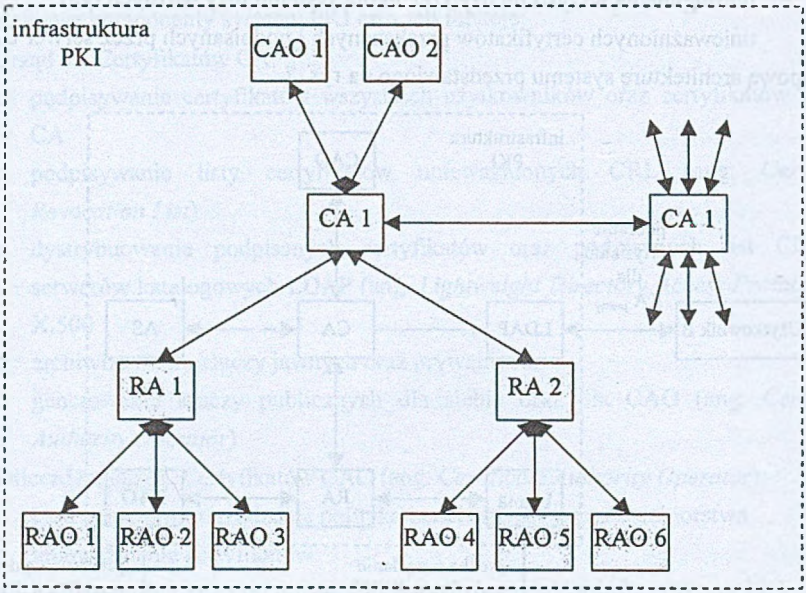
Rys. 7. Architektura systemu PKI
Fig. 7. Architecture of Public Key Infrastructure

Komunikacja między wszystkimi elementami systemu jest szyfrowana, a wszystkie komunikaty są podpisywane.

5.2. Hierarchizacja

W przypadku dużej liczby użytkowników korzystne jest stworzenie hierarchicznej infrastruktury systemu PKI na podstawie domen operacyjnych dla poszczególnych Urzędów ds. Rejestracji. Strukturę taką można stworzyć oczywiście w oparciu o strukturę oddziałów przedsiębiorstwa i przydzielić poszczególnym oficerom RAO określoną z góry grupę użytkowników.

W przypadku bardzo dużych korporacji infrastrukturę PKI można podzielić na domeny operacyjne poszczególnych Urzędów ds. Certyfikatów. Przy czy w tym przypadku system PKI musi zapewnić uwierzytelnienie certyfikatów pochodzących od innych CA. Powyższy model struktury hierarchicznej przedstawiono na rys. 8.



Rys. 8. Przykład złożonej architektury systemu PKI
Fig. 8. Example of compound PKI system architecture

5.3. Przykłady dystrybucji kluczy w systemach PKI

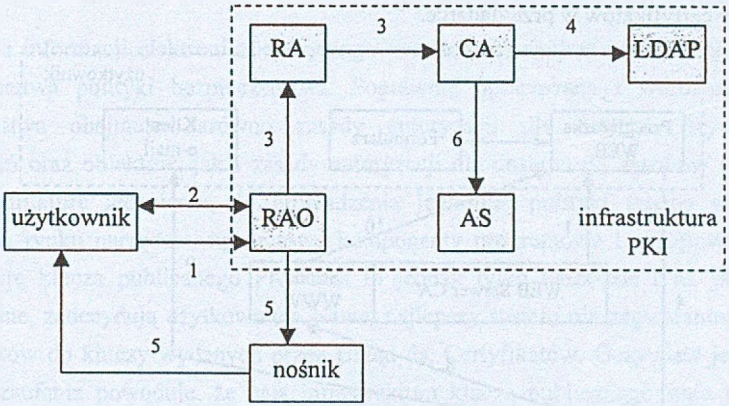
Omówiony w poprzednich punktach system PKI dzięki modularnej budowie może łatwo być dostosowany do konkretnego zastosowania. Dalej zaprezentowano przykłady typowych konfiguracji systemu PKI.

5.3.1. Bezpośrednia metoda dystrybucji certyfikatów

Bezpośrednią metodę dystrybucji kluczy wykorzystuje się przede wszystkim w instytucjach publicznych i przedsiębiorstwach. Metoda ta opiera się na bezpośredniej weryfikacji użytkownika starającego się o certyfikat przez Oficera Urzędu ds. Rejestracji. Po poprawnej weryfikacji użytkownik otrzymuje nośnik z zapisanym kluczem prywatnym oraz certyfikatem klucza jawnego.

Zestaw wymaganych czynności podejmowanych przez użytkownika oraz system czynności w celu uzyskania certyfikatu (rys. 9):

1. Użytkownik zgłasza żądanie wystawienia certyfikatu do RA.
2. RAO weryfikuje żądanie użytkownika, np. w wyniku spotkania zainteresowanego użytkownika i RAO.
3. RAO generuje parę kluczy publicznych dla użytkownika i przekazuje przez RA do CA.
4. CA podpisuje certyfikat i publikuje certyfikat klucza jawnego do serwera katalogowego LDAP.
5. RAO zapisuje dane użytkownika oraz klucz prywatny na nośniku przekazywanym użytkownikowi.
6. CA archiwizuje klucze prywatny oraz jawny użytkownika w S.A.



Rys. 9. Bezpośrednia metoda dystrybucji kluczy publicznych
Fig. 9. Keys distribution by direct method

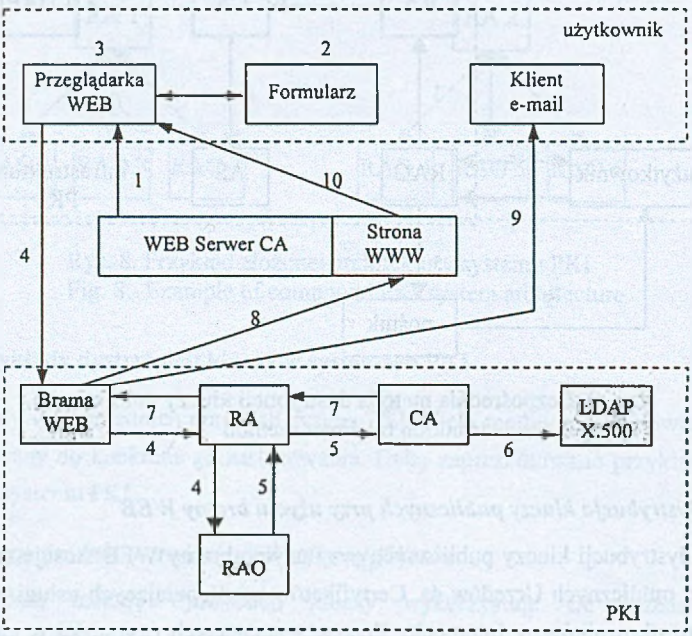
5.3.2. Dystrybucja kluczy publicznych przy użyciu bramy WEB

Metodę dystrybucji kluczy publicznych przy użyciu bramy WEB stosuje się najczęściej w przypadku publicznych Urzędów ds. Certyfikatów udostępniających usługi potwierdzania tożsamości użytkowników w Internecie. Zestaw wymaganych czynności w celu uzyskania certyfikatów (rys. 10):

1. Użytkownik otwiera w przeglądarce WWW stronę CA wystawiającego certyfikaty.
2. Użytkownik wprowadza dane personalne oraz własny adres e-mail.
3. Aplikacja działająca w środowisku przeglądarki WWW generuje parę związanych ze sobą kluczy. Przy czym oba klucze są generowane lokalnie, tzn. klucz prywatny nie

jest przesyłany w Internecie. Aplikacja wysyła prośbę o wydanie certyfikatu dla otrzymanego klucza jawnego do CA wraz z tym kluczem jawnym.

4. Prośba jest przesyłana do modułu bramy WEB, który przesyła ją poprzez RA do RAO.
5. Prośba jest weryfikowana przez RAO i po pozytywnym zaopiniowaniu jest przesyłana poprzez RA do CA.
6. CA podpisuje certyfikat i publikuje do serwera katalogowego.
7. Podpisany certyfikat poprzez RA jest przesyłany do modułu bramy WEB.
8. Moduł bramy WEB generuje unikalną stronę HTML dla użytkownika zawierającą żądany certyfikat.
9. Moduł bramy WEB wysyła e-mail do użytkownika z adresem strony WWW zawierającej certyfikat jego klucza jawnego.
10. Użytkownik otwiera tę stronę w przeglądarce i dodaje zapisany na niej certyfikat do listy certyfikatów w przeglądarce.



Rys. 10. Dystrybucja kluczy przy użyciu bramy WEB
Fig. 10. Keys distribution by WEB Gateway

5.3.3. Unieważnianie certyfikatów

W przypadku skończenia okresu ważności certyfikatu klucza KX_{jawny} lub skompromitowania klucza $KX_{prywatny}$ certyfikat jest unieważniany przez RAO lub CAO, po czym podpisana przez CA aktualna lista certyfikatów unieważnionych jest publikowana, np. w serwerze katalogowym. Należy w tym miejscu zauważyć, że każdy użytkownik powinien sprawdzać aktualną listę certyfikatów unieważnionych. Innym rozwiązaniem jest wykorzystanie oferowanych na rynku kompleksowych systemów PKI w powiązaniu z systemami zarządzania przywilejami. Systemy takie w sposób automatyczny, niewidoczny dla użytkownika, kontrolują listę certyfikatów unieważnionych korelując ją z certyfikatami przechowywanymi lokalnie na komputerze użytkownika.

6. Podsumowanie

Ochrona informacji elektronicznej wymaga opracowania spójnej i jednolitej dla całego przedsiębiorstwa polityki bezpieczeństwa. Poprawnie opracowana i wdrożona polityka bezpieczeństwa obejmuje zarówno zasady autoryzacji dla dostępu fizycznego do pomieszczeń oraz obiektów, jak i zasady autoryzacji dla dostępu do zasobów sieciowych. Jako infrastrukturę techniczną do prowadzenia jednolitej polityki można wykorzystać dostępne na rynku narzędzia, np. gotowe komponenty programowe i sprzętowe tworzące infrastrukturę klucza publicznego PKI. Jest to jednak tylko narzędzie i to, jak zostanie wykorzystane, zadecydują użytkownicy. Nawet najlepszy system nie zagwarantuje zaufania użytkowników do kluczy wydanych przez Urząd ds. Certyfikatów. Oczywiste jest, że brak takowego zaufania powoduje, że cała infrastruktura klucza publicznego staje się jedynie zbiorem nieprzydatnego sprzętu i oprogramowania.

LITERATURA

1. ITU-T X.509: Information technology – the directory: authentications framework.
2. Stalings W.: Ochrona danych w sieci i intersieci. W teorii i praktyce. WNT, Warszawa 1997.

Recenzent: Dr inż. Jarosław Francik

Wpłynęło do Redakcji 28 marca 2001 r.

Abstract

The paper concerns Public Key Cryptographic Systems. Author splits the article into four parts.

First part describes two basic application of Public Key Cryptographic Systems:

- Confidentiality - to keep information private (Fig. 1),
- Authentication – to prove the identify of an individual or application (Fig. 2).

Second Part discusses method distribution of public keys. There are describe four methods:

- Public announce of key (Fig. 3),
- Keys Distribution by open public catalog (Fig. 4),
- Keys Distribution by Public-key Authority (Fig. 5),
- Keys distribution by Certificate Authority (Fig. 6).

Next chapter concerns method storage of private keys.

Last chapter describes architecture of Public Key Infrastructure system (Fig. 7) and presents some examples of key distribution in PKI system (Fig. 9, Fig. 10).