Krzysztof Szczypiorski, Konrad Wrona
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: {kszczypi, kwrona}@tele.pw.edu.pl

Ochrona informacji w sieciach ATM

STRESZCZENIE

Artykuł przedstawia problemy i wymagania dotyczące ochrony informacji w sieciach ATM - w tym rozważania nad realizacją sprzętową i programową algorytmów kryptograficznych. Przedstawia propozycje bezpiecznego systemu dystrybucji kluczy składającego się z dwupoziomowego protokołu uzgadniania kluczy połączonego z uwierzytelnieniem oraz struktury urzędów ds. certyfikatów. Przedstawiony system jest uniwersalny - można go bezpośrednio przenieść do innych sieci telekomunikacyjnych.

Data Security in ATM Networks

ABSTRACT

The paper discusses problems and requirements concerning data security in ATM networks - including hardware and software implementations of cryptographic algorithms. A proposal of secure key distribution system, made up of two-tiered key agreement hierarchy and certification authorities structure, is presented. The reviewed system should be considered as an universal model - it could be directly adopted to any communications network.

Krzysztof Szczypiorski, Konrad Wrona
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: {kszczypi,kwrona}@tele.pw.edu.pl

Ochrona informacji w sieciach ATM

Artykuł przedstawia problemy i wymagania dotyczące ochrony informacji w sieciach ATM - w tym rozważania nad realizacją sprzętową i programową algorytmów kryptograficznych. Przedstawia propozycje bezpiecznego systemu dystrybucji kluczy składającego się z dwupoziomowego protokołu uzgadniania kluczy połączonego z uwierzytelnieniem oraz struktury urzędów ds. certyfikatów. Przedstawiony system jest uniwersalny - można go bezpośrednio przenieść do innych sieci telekomunikacyjnych.

1. Wprowadzenie

Obecnie większość sieci telekomunikacyjnych jest ściśle powiązana z realizowaną w nich usługą lub grupą pokrewnych usług. Naturalnym dążeniem jest próba stworzenia szerokopasmowej sieci z integracją usług - B-ISDN (Broadband Integrated Services Digital Network), sieci umożliwiającej przesyłanie zarówno danych komputerowych, jak i obrazu telewizyjnego czy też ludzkiego głosu. ATM (Asynchronous Transfer Mode) został wybrany przez CCITT (obecnie ITU-T) jako docelowa metoda przekazu informacji dla B-ISDN.

Niniejszy artykuł przedstawia problemy i wymagania dotyczące ochrony informacji w sieciach ATM oraz propozycje bezpiecznego systemu dystrybucji kluczy składającego się z dwupoziomowego protokołu uzgadniania kluczy połączonego z uwierzytelnieniem i projektu struktury urzędów ds. certyfikatów.

2. Oznaczenia

Poniżej (tabela 1) przedstawiono listę używanych w tym artykule oznaczeń:

Tab. 1 Lista oznaczeń

H	mocna funkcja skrótu (np. SHA, MD5)	*A, B, C, X, Y*	strony biorące udział
H_K	mocna funkcja skrótu powiązana z kluczem np. dla MD5 H_K *(DATA)*=MD5*(K,DATA,K)*	PK_X	publiczny klucz *X*
SK_X	prywatny klucz *X*	*Cert(X)*	publiczny certyfikat *X*
K_{ab}^m	długoterminowy klucz dzielony przez *A* i *B*	{*text*}	opcjonalny ciąg *text*
K_{ab}^s	sesyjny klucz dzielony przez *A* i *B*	R_X	losowa liczba wygenerowana przez *X*
K_{xx}^m	udział strony *X* w nadrzędnym kluczu K_{ab}^m	T_X	znacznik czasu utworzony przez *X*
K_{xx}^s	udział strony *X* w sesyjnym kluczu K_{ab}^s	N_X	Numer kolejny utworzony przez *X*
K(text)	zaszyfrowanie ciągu *text* kluczem *K*	$\oplus$	działanie XOR
$S_X[text]$	podpis cyfrowy wyznaczony przy użyciu SK_X		

3.Problemy bezpieczeństwa w sieciach ATM

3.1 Sytuacja obecna

Prace nad bezpieczeństwem w sieci ATM są prowadzone w ośrodkach skoncentrowanych wokół ATM Forum - organizacji skupiającej przede wszystkim przodujących wytwórców sprzętu telekomunikacyjnego dla sieci szerokopasmowych i dla usług multimedialnych. W obrębie ATM Forum działa grupa AF-SECURITY - Security Specialists.

Stopień zaawansowania prac dotyczących bezpieczeństwa sieci ATM można porównać z poziomem prac dotyczącym Internetu pod koniec lat 80. Internet jest najpoważniejszym polem doświadczalnym w dziedzinie sieciowych technik ochrony informacji i niektóre zaakceptowane tam mechanizmy są wprost przenoszone do ATM.

3.2 Usługi kryptograficzne w sieciach LAN, MAN i WAN

Następujące usługi są realizowane lub mogą być realizowane w sieciach LAN, MAN i WAN:

- kontrola dostępu,
- integralność danych,
- uwierzytelnienie,
- poufność,
- niezaprzeczalność.

Usługi te można świadczyć (za wyjątkiem niezaprzeczalności) poniżej warstwy aplikacji w warstwach: łącza danych, transportowej, sieciowej. Mogą one zostać zrealizowane jako usługi end-to-end (między stacjami końcowymi) lub hop-to-hop. Dla ATM hop-to-hop można pojmować jako: ATM-endpoint-to-ATM-endpoint (dwa punkty końcowe w sieci ATM), switch-to-switch (przełącznik-przełącznik) oraz ATM-endpoint-to-switch.

3.3 Usługi kryptograficzne w sieci ATM

Następujące usługi mogą być realizowane w sieci ATM:

- integralność danych,
- uwierzytelnienie,
- poufność.

Pierwsza usługa - integralność danych - nie może być zapewniona bez udziału warstwy AAL, odpowiadającej za składanie i segmentację danych. Nierozsądne wydaje się dołączanie kryptograficznej sumy kontrolnej do każdej komórki ATM (np. przy zastosowaniu MD5 dającej 16 bajtowy skrót - pozostałyby tylko 32 bajty na informację). Stąd integralność powinna być realizowana w stacjach końcowych.

Dwie ostatnie usługi mogą być realizowane pomiędzy stacjami końcowymi (end-to-end), krawędziami sieci wyznaczonymi przez przełączniki (edge-to-edge - ATM przełącznik- ATM przełącznik) lub endpoint-to-switch. Bezpieczeństwo pomiędzy krawędziami sieci może być wymagane przez organizację potrzebującą jedynie bezpiecznego połączenia poprzez sieć publiczną pomiędzy odległymi ośrodkami.

3.4 Oddzielenie usług w poszczególnych warstwach czy też nie

W niektórych pracach [Peyra95a] proponuje się rozdzielić usługi bezpieczeństwa realizowane w warstwie ATM od usług bezpieczeństwa w wyższych warstwach.

Podczas ustanawiania połączenia wirtualnego, stacje końcowe ATM powinny uwierzytelnić się nawzajem i wymienić między sobą klucze do zabezpieczenia przesyłanych informacji poprzez dane połączenie wirtualne i należących do jednego lub wielu połączeń wyższych warstw.

Obecnie: połączenie SETUP - inicjujące procedurę połączenia - zawiera opcjonalne pole określające identyfikator zgłaszającego się (calling party ID). Sugeruje się aby [Stevens95] podczas łączenia się stron następowało wzajemne uwierzytelnienie poprzez podpis cyfrowy. Podobnie polecenie RESTART - służące do zwrócenia wszelkich zasobów związanych z danym połączeniem wirtualnym - nie zawiera identyfikatora nadawcy, a ono również powinno być powiązane z uwierzytelnieniem nadawcy.

Rozdzielenie usług realizowanych w poszczególnych warstwach neguje inną tendencje zakładającą poszerzenie sygnalizacji ATM o informacje związane z realizowanymi w wyższych warstwach usługami bezpieczeństwa. Innym wyrazem dążenia do łączenia usług bezpieczeństwa jest sugestia aby każde połączenie pomiędzy wyższymi warstwami było odwzorowane dokładnie jednym połączeniem wirtualnym. W tym wypadku każde połączenie jest uwierzytelniane przy ustanawianiu połączenia (setup) i podczas komunikacji w danym VC. Pomysł ten jednak nie jest zbyt udany - następuje sztywne odwzorowanie między warstwami - nie zawsze możliwe do realizacji praktycznej.

3.5 Problem straconych komórek

Przy prawdopodobieństwie straty komórki przez sieć równym 10^{-9} (przy szybkości 622 Mbit/s) średnio raz na 15 minut będą tracone dane.

Sugeruje się zatem zastosowanie algorytmów kryptograficznych odpornych na przekłamania - szczególne znaczenie ma problem rozszerzania się błędów (error extension) podczas użycia różnych trybów blokowych szyfrów symetrycznych takich, jak DES (Data Encryption Standard) i IDEA (International Data Encryption Algorithm).

Tryb ECB (Electronic Codebook) nie jest polecany do użycia dla długich ciągów informacji jednak pojedynczy błąd podczas transmisji zaszyfrowanego bloku nie wpływa na zawartość kolejnych. Tryb ECB wydaje się atrakcyjny dla ochrony (na poziomie komercyjnym) skompresowanego obrazu wideo lub zeskramblowanego głosu ludzkiego.

Tryb OFB (Output Feedback) zapewnia brak propagacji błędów. Jednak jego użycie wiąże się ze zmniejszeniem efektywnej szybkości szyfrowania, gdyż szyfrowana w jednym kroku algorytmu ilość informacji jest mniejsza od bloku 64.bitowego.

Tryb CBC (Cipher Block Chaining) jest trybem samo-uzdrawiającym się (self-recovering). Po wystąpieniu błędu w zaszyfrowanym bloku n, blok n+2 nie jest obarczony już błędem. Tryb ten, podobnie jak OFB i CFB, wymaga oprócz znajomości klucza również znajomości wektora początkowego IV.

3.6 Problemy szybkościowe

Istotnym problemem przy praktycznej realizacji usług kryptograficznych są względy szybkościowe. Istniejące implementacje sprzętowe są wystarczające dla sieci 100 Mbit/s (FDDI), implementacje programowe dla 10 Mbit/s (Ethernet) i wolniejszych (X.25).

Obecna technologia sprzętowa umożliwia osiągnięcie szybkości rzędu 1,2 Gbit/s dla szyfru DES w trybie CBC, 240 Mbit/s dla MD5 i około 100 kbit/s dla szyfru RSA (klucz 512 bitów). Przy szybkościach pracy ATM na poziomie warstwy transmisyjnej 155,520 Mbit/s i 622,080 Mbit/s oraz 130 Mbit/s na poziomie aplikacji (HDTV) wydają się one wystarczające do celów komercyjnych, ale niewystarczające dla wojskowych.

Prowadzone są [Touch95] badania nad nowymi algorytmami funkcji skrótu - problem integralności danych dla nowej rodziny protokołów IP - IPng - IPv4 i IPv6 - lub nad modyfikacjami istniejących (np. projekt MD5++). Nie ma **sprzętowego** konkurenta dla algorytmu DES - prace nad szyframi pseudostrumieniowymi RC4 i RC5 przynajmniej na razie nie wydają się stanowić zagrożenia. Ewentualną pomocą może być oczekiwany w ciągu najbliższych kilkunastu lat przełom technologiczny w elektronice - np. gigabitowe układy cyfrowe oparte o technikę nadprzewodnictwa.

Oczywiście duża szybkość dla DES - 1,2 Gbit/s - odnosi się do pojedynczego przebiegu - dla zalecanej implementacji w sieci opartej o IPng - 3DES [Karn95] (Triple DES - potrójny DES) szybkość ta spada do 400 Mbit/s.

Niestety problem efektywnej realizacji sprzętowej szyfrów asymetrycznych (np. RSA) jest skomplikowany. Wydaje się, iż użycie tu metod programowych, ze względów ekonomicznych jest stosowniejsze.

3.7 Kryptograficzna sygnalizacja

Kryptograficzna sygnalizacja (security signalling) w warstwie ATM powinna zawierać informacje uwierzytelniające stacje końcowe i ewentualnie rozprowadzające klucze dzielone niezbędne do szyfrowania lub zabezpieczenia integralności danych.

W przypadku niektórych protokołów można przesłać dodatkowe (zabezpieczone) informacje (adres IP), które są niezbędne do pracy systemów typu firewall lub innych mechanizmów filtrowania.

4. Szkielet systemu dystrybucji kluczy z uwierzytelnieniem w sieciach ATM

4.1 Ogólna architektura

Proponowana architektura składa się z dwóch protokołów (poziomów) dystrybucji kluczy.

- **Master Key Protocol** (MKP - protokół klucza nadrzędnego) pozwala węzłom (punktom końcowym lub przełącznikom) otrzymywać[1] (lub odświeżać) współdzielone klucze nadrzędne (shared master keys). Protokół jest oparty na systemach klucza publicznego (asymetrycznych).
- **Session Key Protocol** (SKP - protokół klucza sesyjnego) - z kolei, pozwala węzłom wymieniać klucze sesyjne przy pomocy kluczy nadrzędnych (dla algorytmów symetrycznych). Protokół jest oparty na algorytmach z dzielonym kluczem.

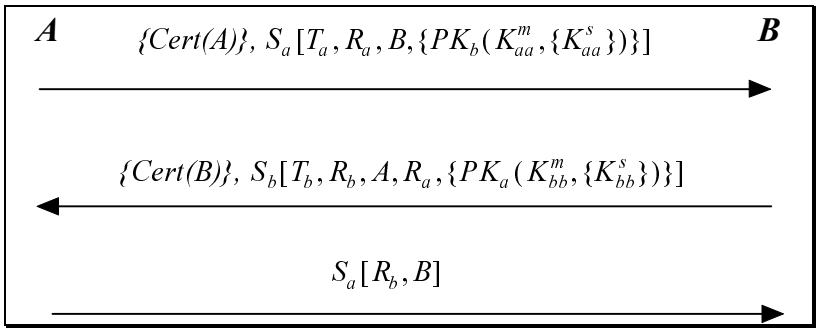
Klucz nadrzędny jest kluczem „długoterminowym" (long-lived) - sesyjny - „krótkotrwałym" (short-lived).

Przyjęta dwupoziomowa architektura jest podyktowana względami szybkościowymi.

Wybór systemu klucza publicznego dla dystrybucji kluczy nadrzędnych (MKP) jest podyktowany wymaganiem rozszerzalności (scalable) tzn. dowolny węzeł musi mieć możliwość połączenia z innym niekoniecznie sąsiadującym węzłem. Dla dwóch węzłów, które dzielą między sobą tajny klucz nadrzędny, efektywny staje się protokół SKP umożliwiający ustalenie kluczy „krótkotrwałych" sesyjnych bez użycia skomplikowanych obliczeniowo algorytmów asymetrycznych.

4.2 Ustanowienie kluczy nadrzędnych

MKP (rysunek 1) zakłada, że infrastruktura klucza publicznego jest zbudowana. Szczegóły budowy infrastruktury omówione zostaną w następnym rozdziale.



Rys. 1 Protokół MKP

Dla celów dalszej dyskusji, zakładamy że:

1. Każdy węzeł *X* biorący udział w operacjach dystrybucji klucza posiada parę kluczy: prywatny SK_X i publiczny PK_X wraz z certyfikatem *Cert(X)*[2], potwierdzającym ważność klucza publicznego i potwierdzonym przez znany urząd ds. certyfikatów (*CA).*

[1] wtedy gdy dwa węzły nie dzielą klucza nadrzędnego

[2] w domyśle *Cert(X)* =Cert(PK_X)

2. Dowolne dwa węzły (np. *A* i *B*) mogą otrzymać certyfikaty drugiej strony (odpowiednio *Cert(B)* i *Cert(A)*) poprzez wymianę własnych certyfikatów przed lub w czasie realizacji protokołu wymiany kluczy lub poprzez pobranie certyfikatu drugiej strony z lokalnego serwera katalogu.

Proponowany MKP jest identyczny do procedury „silnego uwierzytelnienia" (standard ISO X.509). X.509 oferuje trzy różne procedury silnego uwierzytelnienia: jednoprzebiegową, dwuprzebiegową i trzyprzebiegową (odpowiednio one-way, two-way i three-way). Każda z nich oferuje inny stopień bezpieczeństwa. Używając MKP, węzły ustanawiają pojedynczy dzielony klucz nadrzędny K_{ab}^m lub dwa jednokierunkowe klucze nadrzędne K_{ab}^m i K_{ba}^m. Przy okazji MKP można ustanowić klucze sesyjne. Zostanie to opisane w następnym podrozdziale.

4.2.1 Szczegółowy opis MKP

Oto szczegółowy opis MKP:

1. W początkowej wiadomości, strona *A* wysyła stronie *B* token $S_a[T_a, R_a, B, \{PK_b(K_{aa}^m, \{K_{aa}^s\})\}]$ i opcjonalnie swój certyfikat *Cert(A)*. Znacznik czasu T_a potwierdza fakt, iż wiadomość jest aktualna. R_a jest liczbą losową - wysyłaną jako zabezpieczenie przed atakiem powtórzenia[3]. Podpis cyfrowy S_A uwierzytelnia wiadomość. Razem z tokenem A przekazuje B dwie tajne wartości K_{aa}^m i K_{aa}^s - są one wkładami A odpowiednio w klucz nadrzędny i początkowy klucz sesyjny.
2. Druga wiadomość jest symetryczna do pierwszej: B uwierzytelnia się przed A i bezpiecznie wysyła swoje wkłady K_{bb}^m i K_{bb}^s - odpowiednio w klucz nadrzędny i początkowy klucz sesyjny. T_b nie jest konieczne (może być równe 0) - potwierdzenie aktualności jest zagwarantowane przez włączenie liczby odebranej od A - R_a.

   Jeśli A wysłał w pierwszym przebiegu do B co najmniej jeden wkład (zaszyfrowany PK_B), A musiał posiadać (lub otrzymać) *Cert(B)* przed wysłaniem pierwszej wiadomości. Tylko w poniższych przypadkach B powinien dołączyć *Cert(B)* w drugim przebiegu:
   - A nie wysłał wkładu w pierwszej wiadomości. To mogłoby się wydarzyć w przypadku gdy A nie może lub nie chce pobrać *Cert(B)* z serwera katalogu lub nie akceptuje wkładu w dzielone klucze.
   - A wysyłał wkład, lecz B odkrył po odszyfrowaniu $PK_b(K_{aa}^m, \{K_{aa}^s\})$, że A użył niewłaściwego (np. starego) PK_B. W tym przypadku B może wysłać swój certyfikat A w drugim przebiegu. A może powtórzyć procedurę używając właściwego PK_B.
3. Trzecia wiadomość zawiera potwierdzenia A i jest ostatnią częścią trzyprzebiegowej procedury.
   - Przy przeprowadzaniu trzyprzebiegowej procedury nie jest konieczne użycie znaczników T_a i T_b.
   - Warto zwrócić uwagę, że procedura trzyprzebiegowa jest jedyną drogą wymiany kluczy A i B przy braku synchronizacji ich zegarów.

4.2.2 Tworzenie kluczy nadrzędnych

Pojedynczy klucz nadrzędny lub dwa dwukierunkowe klucze nadrzędne mogą zostać wyznaczone na podstawie K_{aa}^m i K_{bb}^m w następujący sposób:

- $K_{ab}^m = f(K_{aa}^m, K_{bb}^m)$ lub
- $K_{ab}^m = f_1(K_{aa}^m, K_{bb}^m)$ *i* $K_{ba}^m = f_2(K_{aa}^m, K_{bb}^m)$,

gdzie $f(), f_1() \; i \; f_2()$ są mocnymi funkcjami jednokierunkowymi np. SHA.

---

[3] samo T_a nie jest wystarczającym zabezpieczeniem

4.2.3 Modularność i negocjacja wersji protokołu MKP

Jedno-, dwu- i trzyprzebiegowe wersje MKP są wzajemnie powiązane: jednokierunkowa wchodzi w skład dwuprzebiegowej, ta natomiast wchodzi w skład trzyprzebiegowej. Cecha modularności umożliwia dwóm stronom decydować (negocjować) na bieżąco (bez uprzednich ustaleń), która z trzech wersji ma zostać użyta. Zatem negocjacja wersji protokołu MKP jest negocjacją dotyczącą liczby przebiegów.

Modularność protokołu i bieżąca negocjacja (run-time negotiation) są ważne ze względów ekonomicznych - kiedy strony A i B są fizycznie odległe - ograniczenie wymiany informacji może znacznie obniżyć koszt ustanawiania połączenia.

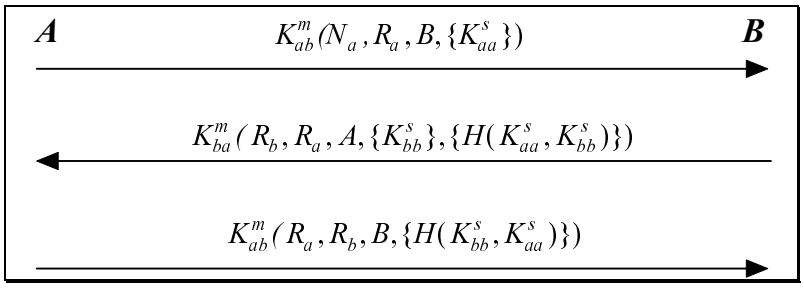
4.3 Ustanowienie kluczy sesyjnych

Do ustalenia kluczy sesyjnych, proponuje się rodzinę trzech protokołów o wspólnym rodowodzie (ISO 11770-2) i podobnym stopniu bezpieczeństwa.

4.3.1 Podstawowy protokół klucza sesyjnego

Pierwszy protokół - podstawowy protokół klucza sesyjnego (Basic Session Key Protocol - B-SKP) przedstawiono na rysunku 2. W B-SKP dwa węzły dzielą między sobą jeden klucz nadrzędny K_{ab}^m (lub dwa jednokierunkowe K_{ab}^m i K_{ba}^m). Protokół składa się z następujących kroków:

1. W pierwszej wiadomości, A przesyła B wiadomość (zaszyfrowaną K_{ab}^m) zawierającą znacznik czasu (lub numer kolejny) N_a, liczbę losową R_a, identyfikator B i opcjonalnie wkład A do klucza sesyjnego K_{aa}^s.
2. B odpowiada podobnie zaszyfrowaną wiadomością zawierającą: liczbę losową R_b, liczbę R_a otrzymaną od A, wkład B do klucza sesyjnego K_{bb}^s oraz opcjonalnie sprawdzenie integralności klucza $H(K_{aa}^s, K_{bb}^s)$. Ostatnia operacja udowadnia A integralność obydwu wkładów.
3. Ostatnia wiadomość, A uwierzytelnia się przed B zwracając zaszyfrowane wartości dwóch liczb losowych (R_a oraz R_b) i (opcjonalnie) potwierdza posiadanie obydwu wkładów.

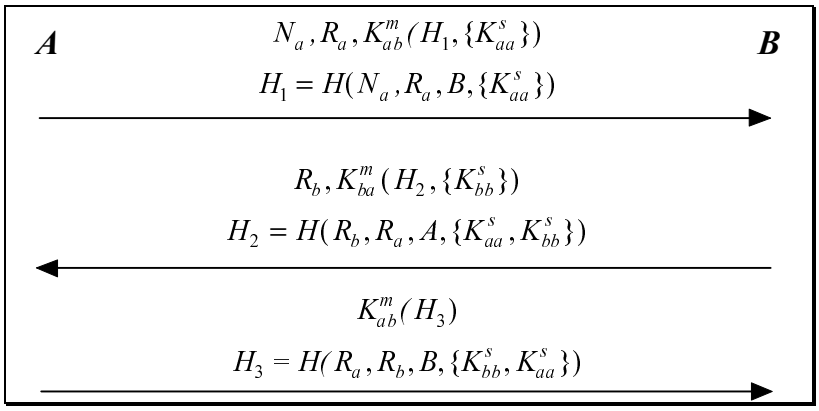


Rys. 2 Protokół B-SKP

4.3.2 Protokół klucza sesyjnego z ograniczonym szyfrowaniem

Łatwo dostrzec, że B-SKP szyfruje więcej danych niż jest to konieczne. Drugi protokół - protokół klucza sesyjnego z ograniczonym szyfrowaniem (Encryption-Efficient Session Key Protocol - EE-SKP) przedstawiony na rysunku 3 - jest zoptymalizowaną względem poniższych zagadnień wersją B-SKP:

- Tajne są jedynie wkłady stron w klucz sesyjny K_{aa}^s i K_{bb}^s.
- Uwierzytelnienie w B-SKP jest dokonywane poprzez szyfrowanie znacznika czasu, liczb losowych oraz identyfikatorów. Może to być przeprowadzone poprzez kryptograficzne sprawdzenie integralności (funkcja skrótu).

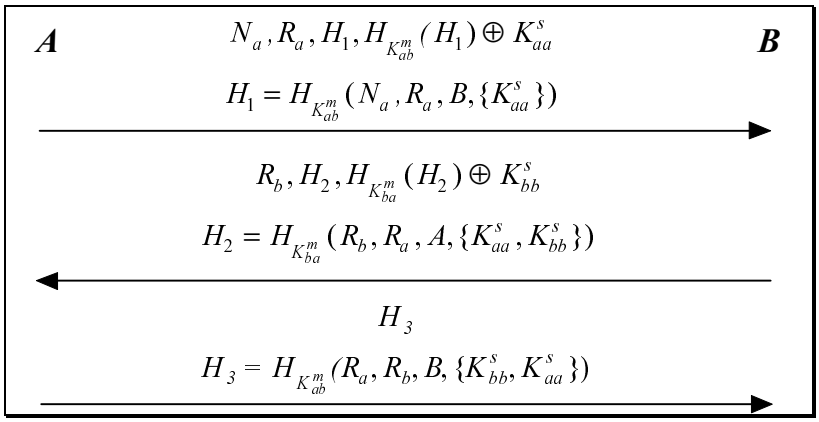


Rys. 3 Protokół EE-SKP

4.3.3 Protokół klucza sesyjnego bez szyfrowania

EE-SKP jest bardziej efektywny niż B-SKP - wciąż jednak szyfrowane są skróty wkładów stron w klucz sesyjny. Trzeci protokół - protokół klucza sesyjnego bez szyfrowania (Encryption-Free Session Key Protocol - EF-SKP) przedstawiony na rysunku 4 - jak wskazuje nazwa nie używa żadnych algorytmów szyfrowania - przez co jest szybszy i może być bez żadnych restrykcji eksportowany[4].

W EF-SKP stosuje się H_K. Przy dystrybucji klucza używa się działania XOR.



Rys. 4 Protokół EF-SKP

4.3.4 Tworzenie kluczy sesyjnych

Klucze sesyjne są tworzone w podobny sposób jak klucze nadrzędne:

- dwukierunkowy klucz: $K^s_{ab} = g(K^s_{aa}, K^s_{bb})$ lub
- dwa jednokierunkowe klucze: $K^s_{ab} = g_1(K^s_{aa}, K^s_{bb})$ *i* $K^s_{ba} = g_2(K^s_{aa}, K^s_{bb})$,

gdzie $g()$, $g_1()$ *i* $g_2()$ są mocnymi funkcjami jednokierunkowymi np. SHA.

4.3.5 Połączenie punkt-punkt i połączenia wielopunktowe

Dla połączeń punkt-punkt węzły A i B decydują o wkładach w klucz sesyjny.

Dla połączeń wielopunktowych - węzeł nadrzędny może zechcieć ustanowić ten sam klucz sesyjny dla wszystkich (podrzędnych) węzłów uczestniczących w połączeniu. W tym przypadku żaden z węzłów podrzędnych nie decyduje o wkładzie.

[4] np. problem patentu RSA, IDEA

5. Szkielet systemu certyfikatów w ATM

5.1 Certyfikaty i urzędy ds. certyfikatów

A musi kontaktować się bezpiecznie z B i / lub tylko zweryfikować podpis B. Potrzebny do tego jest klucz publiczny B PK_B (pobrany z lokalnej bazy danych [ze schowka (cache)], z centralnej bazy danych lub bezpośrednio od B). Aby uniknąć skutków ataku man-in-the-middle przez stronę X - zamiany PK_B na PKx - klucze publiczne są przechowywane i rozpowszechniane w postaci certyfikatów. Certyfikat zawiera unikalny identyfikator strony, klucz publiczny i inne dodatkowe informacje - poświadczone podpisem upoważnionego urzędu ds. certyfikatów (CA). Posiadając klucz publiczny CA można zweryfikować certyfikat i pobrać zawarty w nim klucz publiczny właściciela.

5.2 Format certyfikatu

Proponuje się przyjąć format certyfikatów zgodny z X.509. Certyfikat powinien być zbudowany w następujący sposób:

- numer wersji certyfikatu
- unikalny numer seryjny nadawany przez wystawcę (CA)
- nazwa algorytmu użytego do generacji podpisu i niezbędne parametry
- unikalny identyfikator wystawcy (urzędu ds. certyfikatów)
- okres ważności certyfikatu w odniesieniu do czasu uniwersalnego (np. GMT)
- identyfikator strony, której wystawiono certyfikat
- klucz publiczny strony, nazwę użytego algorytmu i niezbędne parametry
- podpis wystawcy

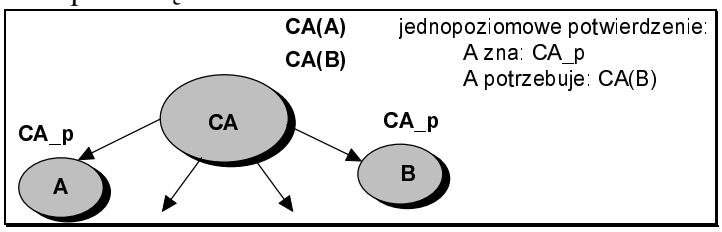
5.3 Ścieżka certyfikacji

Aby węzeł A pobrał klucz publiczny B musi:

1. Pobrać certyfikat klucza publicznego B.
2. Sprawdzić ważność certyfikatu.

Rysunek 5 przedstawia dwa węzły należące do tej samej domeny (potwierdzenia pochodzą od tego samego CA). Strzałka CA $\rightarrow$ A oznacza, że CA potwierdza A. Certyfikaty podpisane przez CA - w tym wypadku CA(A) i CA(B) - są narysowane obok CA (co nie znaczy, że są fizycznie przechowywane w bazie danych umieszczonych w CA). Dodatkowo każda ze stron A lub B może przechowywać swoje własne certyfikaty. Zakładamy, że te certyfikaty są dostępne w serwerze katalogu.

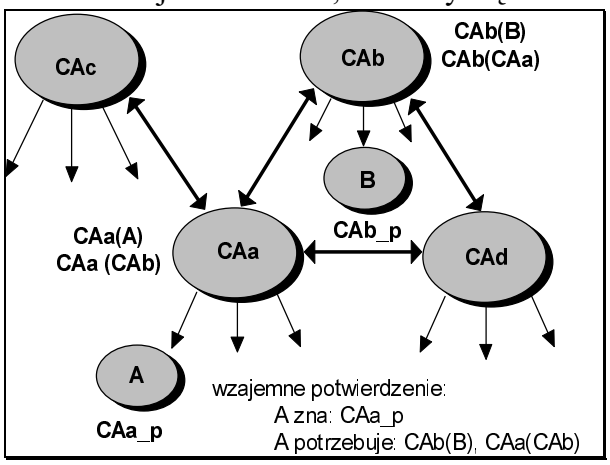
Kiedy A chce porozumieć się z B, pobiera certyfikat B CA(B) z serwera katalogu i znając PK_{CA} sprawdza certyfikat. W innym przypadku A pobiera od B certyfikat B podczas ustalonego protokołu wymiany. Unika się w ten sposób łączenia z serwerem.



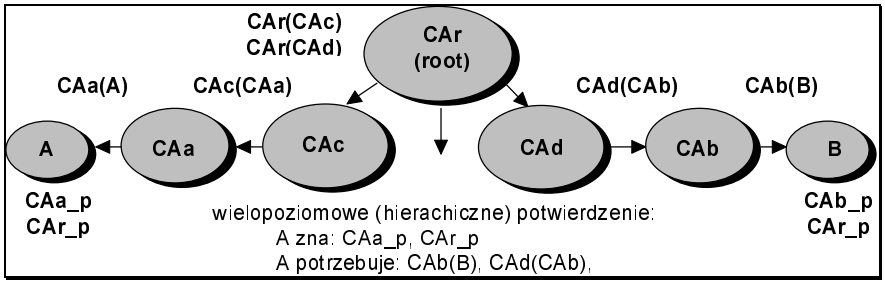
Rys. 5 Struktura jednopoziomowego potwierdzenia (one-level certification)

Natomiast gdy A i B należą do różnych domen (CAa i CAb), A musi także pobrać certyfikat CAb(B). Klucz publiczny CAb potwierdza ważność certyfikatu B. W przypadku wzajemnego potwierdzenia - rysunek 6 - (direct cross-certification) A musi pozyskać jeszcze CAa(CAb). Dla trzypoziomowej hierarchii z CAr (r - root) (rysunek 7) potrzebne są certyfikaty CAb(B), CAd(CAb)

i CAr(CAd) - dla skonstruowania pełnej ścieżki certyfikacji (certification path). Warto zwrócić uwagę, że jedyną drogą potwierdzenia jest założenie, że każdy węzeł zna klucz publiczny roota.



Rys.6 Struktura wzajemnego potwierdzenia (direct cross-certification)



Rys.7 Struktura wielopoziomowego potwierdzenia (hierarchical certification)

5.4 Jaką strukturę potwierdzenia przyjąć w ATM?

Połączone sieci ATM będą wymagać znacznej ilości CA. Rozpatrywany będzie przypadek wymiany certyfikatów pomiędzy różnymi podsieciami. Stąd dla ułatwienia, założono, że każda organizacja posiada dokładnie jeden CA widziany z zewnątrz. Wspomniany CA może być nadrzędnym (root) w danej organizacji. Proponuje się dwa sposoby utworzenia ścieżki certyfikacji pomiędzy dwiema organizacjami:

- struktura wzajemnego potwierdzenia (opisana w poprzednim podrozdziale),
- przystosowanie modelu hierarchicznego - stworzenie jednego nadrzędnego CA w całej ogólnoświatowej sieci - podobnej do Internet Policy Registration Authority (IPRA). Nadrzędny CA potwierdza każde CA będące bezpośrednio pod nim, z kolei CA potwierdzają inne CA będące pod nimi. Proponuje się użycie hierarchii trzy- lub czteropoziomowej. Warto zaznaczyć, że potwierdzenie jest jednoprzebiegowe - zakłada się, że każdy węzeł zna klucz publiczny CA nadrzędnego.

Pierwszy scenariusz może być zrealizowany w przypadku, gdy organizacje preferują bezpośrednie negocjacje. Drugi - gdy jedna z organizacji (np. ITU) założy nadrzędne CA. Każda organizacja będzie mogła zarejestrować się w nadrzędnym CA, każdy węzeł będzie mógł porozumieć się z innym.

Wydaje się, iż wersja pierwsza zostanie wybrana tymczasowo, do momentu aż zostanie zdefiniowane CA nadrzędne. Jednak nie oznacza to, że struktura wzajemnych potwierdzeń zniknie - może być używana przez organizacje, dla których jest ona bardziej odpowiednia.

5.5 Unieważnienie certyfikatu

Unieważnienie certyfikatu może nastąpić w przypadku, gdy np. nie ma pewności, że klucz prywatny jest tajny (został skradziony, wyjawiony) lub automatycznie po przeminięciu jego daty

ważności. Po pobraniu przez A certyfikatu B, A może przechowywać PK_b wraz z jego okresem ważności. Wybór okresu ważności certyfikatu jest kompromisem pomiędzy bezpieczeństwem (krótka ważność) i efektywnością (długa ważność - dłuższy czas przechowywania).

Proponuje się także zastosowanie dynamicznego unieważniania certyfikatów. W tym przypadku każdy CA powinien gromadzić dane o unieważnionych certyfikatach w specjalnej liście - CRL (Certificate Revocation List - listą unieważnionych certyfikatów).

Proponuje się zastosować format stosowany przez IETF dla aplikacji zgodnych z PEM (Privacy Enhancement Mail) - [Linn93]. Lista powinna być zbudowana w następujący sposób:

- identyfikator algorytmu użytego do generacji podpisu i niezbędne parametry
- unikalny identyfikator wystawcy (urzędu ds. certyfikatów)
- data ostatniej i następnej przewidywanej modyfikacji listy w odniesieniu do czasu uniwersalnego
- odwołane certyfikaty: numer seryjny oraz data odwołania
- podpis wystawcy dotyczący całej listy

Kolejnym zagadnieniem, który należy rozważyć jest problem rozprowadzania CRL w rozproszonym środowisku ATM. Nawet jeśli serwer katalogu jest w stanie gromadzić informacje o wszystkich CRL pozostaje problem przekazania tej informacji do każdego węzła. Proces ten może być inicjowany przez węzły lub przez serwer katalogu. Serwery katalogu mogą okresowo wysyłać pełną informację o odwołanych certyfikatach. To rozwiązanie pociąga za sobą duży ruch w sieci i wymaga przechowywania stosunkowo wielu informacji przez węzły. Węzły mogą żądać CRL z bazy danych lub z serwera katalogu kiedy decydują o ważności certyfikatu.

6. Podsumowanie

Technika ATM stanowi wyzwanie dla wielu dziedzin telekomunikacji. Ochrona informacji przestaje być jedną z wielu aplikacji sieciowych a staje się integralnym elementem protokołu sieciowego (tak jak to ma miejsce w Global System for Mobile communications - GSM). Nie wiadomo czy w ATM zostaną zrealizowane (przynajmniej) usługi uwierzytelnienia i integralności danych. Jedno jest jednak pewne: szybkie sieci danych stawiają zupełnie inne wymagania przed ochroną informacji - dopingują środowisko kryptograficzne do konstruowania nowych efektywniejszych pod względem szybkości i bezpieczeństwa algorytmów.

Warto zwrócić uwagę, że przedstawiona w tej pracy propozycja bezpiecznego systemu dystrybucji kluczy jest uniwersalna - można ją bezpośrednio przenieść do innych sieci.

7. Literatura

[Karn95] - P.Karn, P.Metzger, W.Simpson - The ESP Triple DES Transform - RFC 1851, September 1995

[Linn93] - J.Linn, S.Kent, D.Balenson, B.Kaliski - Privacy Enhancement for Internet Electronic Mail - RFC 1421-24, October 1993

[Peyrav95a] - M. Peyravian, E. Van Herreweghen - ATM Security Scope and Requirements - ATM Forum/95-0579, IBM

[Peyrav95b] - M. Peyravian, G.Tsudik, E. Van Herreweghen - A Framework for Authenticated Key Distribution in ATM Networks - ATM Forum/95-0580, IBM

[Peyrav95c] - M. Peyravian, G.Tsudik, E. Van Herreweghen - A Certification Infrastructure for ATM - ATM Forum/95-xxxx, IBM

[Rivest92] - R.Rivest - The MD5 Message-Digest Algorithm - RFC 1321, April 1992

[Schnei94] - B.Schneier - Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1994

[Steven95] - D.Stevenson, N.Hillery, G.Byrd - Secure Communications in ATM Network - Communications of the ACM - February 1995/Vol.38, No.2

[Touch95] - J.Touch - Report on MD5 Performance - RFC 1810, June 1995