BIULETYN INFORMACYJNY INSTYTUTU ŁĄCZNOŚCI

1998
7

BIULETYN INFORMACYJNY INSTYTUTU ŁĄCZNOŚCI

ROK 38 INSTYTUT ŁĄCZNOŚCI NR 7(360)

WARSZAWA 1998

ISSN 0209-1046

Redaktor: mgr Krystyna Juszkiewicz

Skład komputerowy: Barbara Skwara

Instytut Łączności, Ośrodek Informacji Naukowej
ul. Szachowa 1, 04-894 Warszawa

Elżbieta Andrukiewicz

CZY W KONCEPCJI ZAUFANEJ TRZECIEJ STRONY (TTP) MIEŚCI SIĘ KRYPTOGRAFIA KONTROLOWANA?

SPIS TREŚCI

Elżbieta Andrukiewicz

351.817:654.01

CZY W KONCEPCJI ZAUFANEJ TRZECIEJ STRONY (TTP) MIEŚCI SIĘ KRYPTOGRAFIA KONTROLOWANA?

1. WPROWADZENIE

Jedną z podstawowych usług kryptograficznych jest usługa poufności, czyli szyfrowanie. W usłudze szyfrowania są wykorzystywane dwa podstawowe mechanizmy:

- **zaszyfrowania**, który na podstawie danych wejściowych tworzy tekst zaszyfrowany;
- **odszyfrowania**, który na podstawie tekstu zaszyfrowanego odtwarza tekst jawny.

Usługa szyfrowania może być scharakteryzowana za pomocą techniki kryptograficznej, która jest stosowana, tzn. symetrycznej lub asymetrycznej. W przypadku technik symetrycznych operacje zaszyfrowania i odszyfrowania są realizowane na podstawie tego samego klucza (wspólny klucz tajny). W przypadku technik asymetrycznych operacje zaszyfrowania i odszyfrowania są realizowane na podstawie dwóch różnych, ale związanych ze sobą kluczy, tzn. klucza publicznego i prywatnego.

Kryptografia znajduje zastosowanie w sytuacjach, w których trzeba chronić cenną informację przed ujawnieniem osobom trzecim. Istnieje rosnące zapotrzebowanie na takie algorytmy szyfrowania, które byłyby odporne na najbardziej zaawansowane narzędzia kryptoanalizy.

Szerokie zastosowanie silnych mechanizmów kryptograficznych napotyka jednak opór ze strony rządów i instytucji rządowych, np. organów ścigania i wymiaru sprawiedliwości. Z jednej strony bowiem takimi szyframi są zainteresowane organizacje komercyjne, np. banki,

Tablica 1

Ograniczenia w wykorzystaniu produktów kryptograficznych
w różnych krajach świata

Kraj	Import	Eksport	Wykorzystanie w telekomunikacji przewodowej	Wykorzystanie w telekomunikacji bezprzewodowej
Austria	dozwolony	restrykcje ONZ*)	dozwolone	niedozwolone
Belgia	dozwolony	wymagana licencja	zawiadomienie na 4 tygodnie przed rozpoczęciem użytkowania	zawiadomienie na 4 tygodnie przed rozpoczęciem użytkowania
Francja	wymagana licencja, jeśli długość klucza przekracza 40 bitów, a produkt jest spoza Unii	wymagana licencja	wymagana licencja, jeśli długość klucza przekracza 48 bitów, chyba że klucze są składowane w odpowiedniej instytucji	wymagana licencja, jeśli długość klucza przekracza 48 bitów, chyba że klucze są składowane w odpowiedniej instytucji
Holandia	dozwolony	restrykcje ONZ	istnieje obowiązek ujawnienia klucza na żądanie uprawnionej instytucji	istnieje obowiązek ujawnienia klucza na żądanie uprawnionej instytucji
Izrael	wymagana licencja	wymagana licencja	wymagana licencja	niedozwolone
Polska	wymagana licencja	restrykcje ONZ	dozwolone	dozwolone
USA	dozwolone	wymagana licencja**)	dozwolone	dozwolone

*) Restrykcje ONZ są przewidziane w porozumieniu z Wassenaar [4], które w 1995 r. podpisało wiele państw, w tym Polska. Układ ten przewiduje ograniczenia eksportu produktów podwójnego zastosowania; do tej kategorii należą także techniki kryptograficzne.

**) Do 1997 r. w USA obowiązywał zakaz eksportu produktów kryptograficznych o długości klucza przekraczającej 40 bitów, a w przypadku algorytmu DES - 56 bitów. Obecnie zezwolenie na eksport jest wydawane bez ograniczenia, jeśli eksporter zobowiąże się do wprowadzenia w ciągu dwóch lat funkcji odtwarzania klucza (*key recovery*). W przeciwnym przypadku obowiązują dotychczasowe restrykcje (z wyjątkiem produktów przeznaczonych dla banków).

towarzystwa ubezpieczeniowe, operatorzy telekomunikacyjni, dla których celem działania jest zaufanie własnych klientów. Z drugiej jednak strony takie same mechanizmy, jeśli znajdą się w rękach grup i organizacji przestępczych, mogą stać się narzędziem zapewniającym tym grupom praktyczną bezkarność. Dlatego nie jest obecnie możliwe zastosowanie mechanizmów kryptograficznych, których nie można złamać za pomocą współcześnie dostępnych komputerowych narzędzi kryptoanalizy*) oraz szerokie upowszechnienie usługi poufności w sieciach komputerowych. W wielu krajach obowiązują większe lub mniejsze ograniczenia w obrocie technikami kryptograficznymi. W tablicy 1 przedstawiono stan prawny w kilku przykładowych krajach [3].

Niemniej jednak, prace nad znalezieniem sposobu wyjścia z tego impasu trwają cały czas. Jedną z propozycji wprowadzenia usługi poufności na zasadach, które byłyby do zaakceptowania przez rządy poszczególnych krajów, a także przez ogół obywateli, jest proponowana przez rząd USA koncepcja kryptografii kontrolowanej.

2. KONCEPCJA KRYPTOGRAFII KONTROLOWANEJ - ZARYS OGÓLNY

W tym punkcie zostaną pokrótce omówione podstawowe pojęcia z zakresu kryptografii kontrolowanej w najnowszym ujęciu. Ponieważ

---

*) Matematyczny dowód niemożliwości złamania istnieje tylko dla klasycznego szyfru Vernama [13]. W przypadku pozostałych algorytmów kryptograficznych jest stosowane pojęcie obliczeniowej niewykonalności zadania kryptoanalizy. Oznacza ono, że czas, jaki jest potrzebny do realizacji zadania kryptoanalizy, jest dłuższy niż okres użyteczności informacji, która jest przedmiotem ataku. W pewnych zastosowaniach kryptograficznych może to być kilka sekund, w innych - kilkadziesiąt lat.

jest to zupełnie nowa dziedzina kryptografii, terminy i ich definicje nie są jeszcze ustabilizowane.

Systemy kryptograficzne z odtwarzaniem kluczy (*key recovery*) umożliwiają upoważnionym osobom lub instytucjom dostęp do tekstu jawnego poza normalnym procesem zaszyfrowania i odszyfrowania. Dostęp taki jest realizowany za pomocą klucza, zwanego docelowym *(target key)*. Kluczem docelowym mogą być zarówno dane klucza stosowanego w procesie odszyfrowania, jak i klucz, który jest wykorzystywany (pośrednio lub bezpośrednio) do odszyfrowania zaszyfrowanych danych klucza. Informacja, która jest niezbędna do odtworzenia klucza docelowego, jest określana jako "informacja odtworzenia klucza" *(KRI - Key Recovery Information)*.

Stosowane są różne techniki uzyskania klucza docelowego.

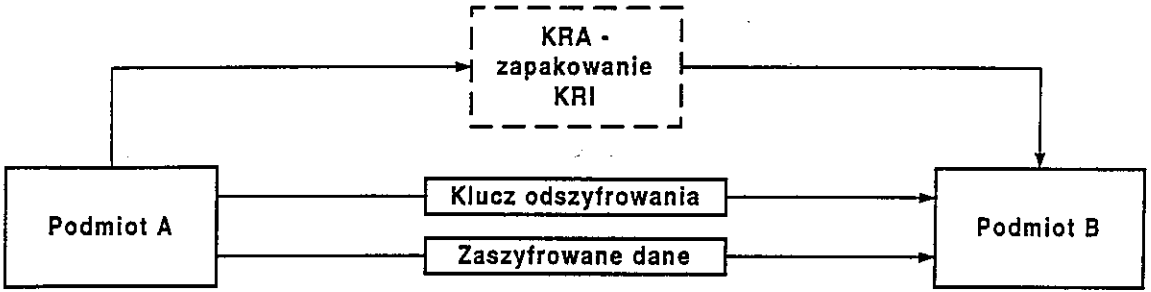
W systemach z pakowaniem informacji odtwarzania kluczy *(KRI Encapsulation)* klucz docelowy (lub jego część albo informacja z nim związana) jest szyfrowany za pomocą klucza agenta odtworzenia klucza *(KRA - Key Recovery Agent)*. Klucz szyfrujący jest tu zwykle kluczem publicznym KRA.

W systemach z kopią rezerwową klucza *(key backup)* klucz docelowy jest szyfrowany za pomocą klucza, dla którego odpowiadający mu klucz odszyfrowujący jest przechowywany, w całości lub części, przez jeden lub więcej agentów KRA.

Agent odtwarzania klucza (zarówno w przypadku stosowania techniki kopii rezerwowej klucza, jak i pakowania informacji odtworzenia klucza) może być integralną częścią własnej struktury zabezpieczenia użytkownika lub instytucją niezależną (trzecią stroną).

W przypadku systemu odtwarzania klucza przez stronę trzecią techniką kopii rezerwowej system taki jest często określany jako system z powierzeniem klucza *(key escrow system)*.

Systemy kryptograficzne z odtwarzaniem klucza są stosowane zarówno w przypadku informacji transmitowanej, jak i przechowywanej.



Rys. 1. Wymiana danych zaszyfrowanych za pomocą systemu kryptograficznego z odtwarzaniem klucza metodą zapakowania

Rys. 2. Wymiana danych zaszyfrowanych za pomocą systemu kryptograficznego z odtwarzaniem kluczy metodą kopii rezerwowej

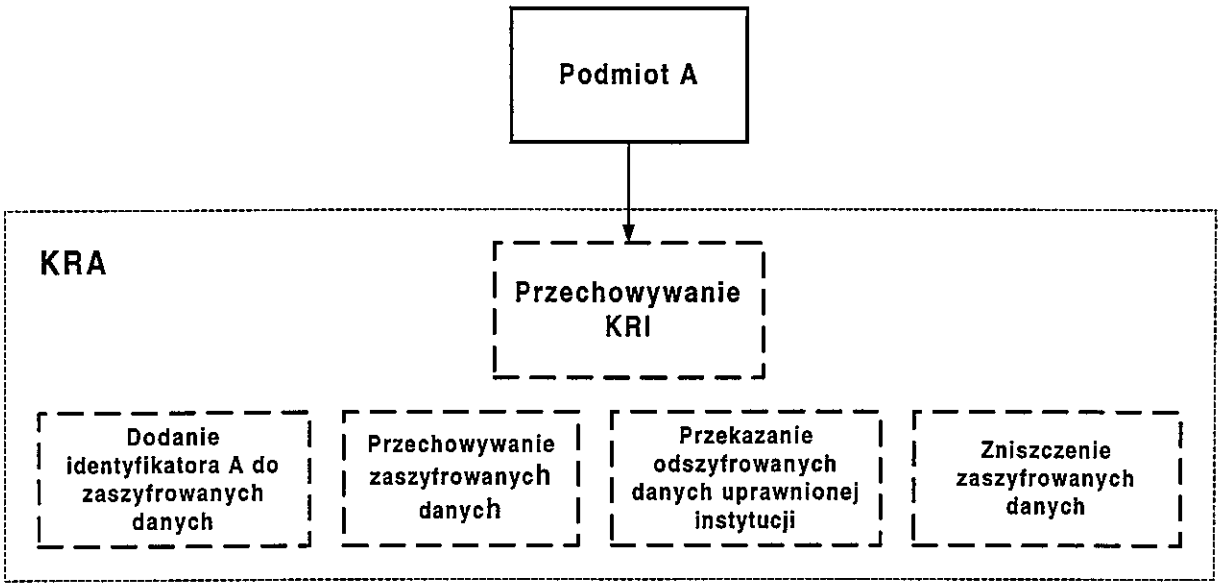
Na rys. 1 przedstawiono współdziałanie dwóch systemów końcowych, które biorą udział w wymianie zaszyfrowanych danych, a odtworzenie kluczy jest realizowane za pomocą metody pakowania informacji odtworzenia klucza.

Użytkownik końcowy (podmiot) A tworzy zapakowaną informację KRI dla siebie i opcjonalnie dla użytkownika B. Informacja ta jest gromadzona, a następnie szyfrowana oraz przechowywana w celu późniejszego odtworzenia (na żądanie upoważnionej osoby lub instytucji). Użytkownik B wraz z zaszyfrowanymi danymi oraz kluczem odszyfrowującym otrzymuje także KRI.

Na rys. 2 pokazano współdziałanie dwóch systemów końcowych, które biorą udział w wymianie zaszyfrowanych danych, a odtworzenie kluczy jest realizowane za pomocą metody kopii rezerwowej klucza. W tej metodzie klucze, części kluczy lub informacje związane z kluczami są przechowywane przez KRA. Podmiot dostarczający KRI przekazuje te informacje do KRA (jeśli nie jest to użytkownik końcowy, to także do niego).

Na rys. 3 przedstawiono system kryptograficzny z odtwarzaniem kluczy stosowany w przypadku składowania zaszyfrowanych danych. Agent odtwarzania klucza musi otrzymać od właściciela danych KRI, umożliwiającą ich odszyfrowanie. Po otrzymaniu tej informacji agent przechowuje dane w postaci zaszyfrowanej (do tych danych dodaje identyfikator właściciela). Na żądanie uprawnionej instytucji może, z wykorzystaniem KRI, dokonać odszyfrowania danych. Gdy upłynie czas przechowywania agent dokonuje nieodwracalnego zniszczenia zaszyfrowanych danych.

W analizie przeprowadzonej w niniejszym artykule skoncentrowano się przede wszystkim na systemach, w których agent odtwarzania klucza nie jest elementem wewnętrznej struktury systemu kryptograficznego, ale instytucją zewnętrzną. Konfiguracja z agentem zewnętrznym ma daleko poważniejsze implikacje dla bezpieczeństwa komunikacji między użytkownikami niż agent wewnętrzny



Rys. 3. Przechowywanie danych zaszyfrowanych za pomocą systemu kryptograficznego z odtwarzaniem klucza

(jakkolwiek w obu przypadkach, jak zostanie to wykazane w dalszej części artykułu, mamy do czynienia z istotnym osłabieniem bezpieczeństwa systemu).

3. TRUDNOŚCI Z WPROWADZANIEM ODTWARZANIA KLUCZY DO SYSTEMÓW KRYPTOGRAFICZNYCH

3.1. Zaufana trzecia strona i podstawowe usługi kryptograficzne

Jedną z koncepcji upowszechniania usług opartych na mechanizmach kryptograficznych jest wprowadzenie zaufanej strony trzeciej (*TTP - Trusted Third Party*).

Definicję zaufanej trzeciej strony można sformułować następująco [6]:

Zaufana strona trzecia (TTP) to usługa lub organizacja, która posiada zaufanie innych podmiotów**) w zakresie wszelkich podejmowanych przez nią działań związanych z bezpieczną komunikacją w sieci komputerowej.

Fundamentalny podział usług kryptograficznych obejmuje usługi uwierzytelniania i integralności oraz usługę poufności. W pierwszym przypadku stosowane mechanizmy kryptograficzne chronią informację (przetwarzaną, przechowywaną lub przesyłaną) przed nieuprawnioną modyfikacją lub zniekształceniem oraz gwarantują autentyczność danych i podmiotów uczestniczących w wymianie tych danych. Zapewnia to para przekształceń kryptograficznych: podpisu cyfrowego oraz jego weryfikacji. Szczegółowy opis usług TTP opartych na prze-

*) Podmiot (*entity*), zgodnie z definicją zawartą w [5], jest to aktywna jednostka uczestnicząca w wymianie informacji. Podmiotem jest przeważnie określany proces (program, procedura), realizująca daną funkcję. Podmiotem może być także stacja robocza albo sam jej użytkownik. W ujęciu niniejszego opracowania "podmiot" jest stroną w wymianie informacji w sieci komputerowej i w tym sensie jest pojęciem szerszym niż "użytkownik".

kształceniach kryptograficznych tego rodzaju został zaprezentowany w [2].

Czy taka sama instytucja może zapewnić także w drugim przypadku usługi poufności oparte na przekształceniu kryptograficznym z odtwarzaniem kluczy?

3.2. Analiza bezpieczeństwa systemów kryptograficznych z odtwarzaniem kluczy

Jak wynika z opisu przedstawionego w pkt. 2, system kryptograficzny z odtwarzaniem kluczy charakteryzują dwie cechy:

- istnieje mechanizm, zewnętrzny w stosunku do procesu szyfrowania i odszyfrowania, dzięki któremu trzecia strona może uzyskać ukryty dostęp do tekstu jawnego;
- istnieje klucz tajny, o wysokim stopniu poufności gwarantujący ten dostęp, który musi być chroniony przez długi czas.

Wprowadzenie odtwarzania kluczy do systemów kryptograficznych TTP powoduje powstanie wielu dodatkowych trudności prawnych, organizacyjnych i technicznych. Są one przedmiotem raportu czołowych autorytetów amerykańskich w dziedzinie kryptografii [1], którego wnioski zostały wykorzystane w niniejszym artykule.

3.2.1. Zróżnicowanie potrzeb użytkowników TTP

Usługa poufności głęboko różnicuje potencjalnych użytkowników TTP. O ile w przypadku usług integralności i uwierzytelnienia oczekiwania ze strony agencji rządowych i przedsiębiorstw były podobne, o tyle oczekiwania wobec usługi poufności są diametralnie różne. Różnice te zostały zgromadzone i omówione w tablicy 2. Istnienie rozbieżności potrzeb i oczekiwań użytkowników może stać się istotnym czynnikiem hamującym rozwój TTP.

Tablica 2

Podstawowe różnice dotyczące wymagań dla systemu kryptograficznego z odtwarzaniem kluczy, przeznaczonych dla agencji rządowych i instytucji komercyjnych

Cecha podstawowa	System dla agencji rządowej	System dla przedsiębiorstwa komercyjnego
Izolacja agenta odtwarzania kluczy i właściciela kluczy	tak - odtwarzanie kluczy następuje bez wiedzy i zgody właściciela kluczy	nie - odtwarzanie klucza następuje za wiedzą i (przeważnie) przy współudziale właściciela klucza
Dostępność systemu	wymagania natychmiastowej realizacji uprawnionego żądania udostępnienia (np. czas reakcji - maksimum 2 godziny od przedłożenia żądania [9])	nie ma konieczności gwarantowania natychmiastowej reakcji na żądanie udostępnienia
Charakterystyka danych	odtwarzanie kluczy, służących do szyfrowania zarówno danych przechowywanych, jak i transmitowanych	dostęp tylko do danych przechowywanych
Międzynarodowy system odtwarzania kluczy	tak - muszą nastąpić uzgodnienia międzypaństwowe	nie - centrum odtwarzania kluczy może być lokalne

3.2.2. Szczegółowe problemy związane z wprowadzaniem systemów z odtwarzaniem kluczy

Działanie TTP jako agenta odtwarzania kluczy stanowi dodatkowy, nie uwzględniony wcześniej aspekt organizacji TTP. Implikacje te można rozważać w czterech kategoriach, takich jak:

- ryzyko naruszenia zabezpieczenia systemu informatycznego TTP,
- złożoność oraz skalowność systemu TTP,
- koszty TTP,
- implikacje dla międzynarodowej struktury TTP.

- **Ryzyko naruszenia zabezpieczenia systemu informatycznego**

1. Rezygnacja z podstawowego zabezpieczenia systemów kryptograficznych, w których nie było innej drogi poznania tekstu otwartego niż metoda kryptoanalizy szyfrogramu (złamania klucza).

   W systemach z odtwarzaniem kluczy istnieje alternatywna droga poznania zaszyfrowanego wcześniej tekstu. Ponadto systemy z odtwarzaniem kluczy są zaprojektowane tak, aby drogę tę ukryć przed właścicielem kontrolowanego klucza. Konsekwencją tego faktu jest dalsze osłabienie mechanizmów zabezpieczeń (takim mechanizmem jest przecież świadomość użytkownika).
2. Powstanie dodatkowych punktów o zasadniczym znaczeniu dla bezpieczeństwa systemu, które mogą stać się celem ataku.

   W systemie z odtwarzaniem kluczy, poza dwoma komunikującymi się podmiotami, są jeszcze: TTP, pełniąca rolę agenta odtwarzania kluczy i podmiot, żądający odtworzenia klucza.

Agent odtwarzania kluczy musi mieć scentralizowaną bazę danych, służącą do odzyskiwania kluczy. Ujawnienie pojedynczego klucza lub niewielkiego zbioru prywatnych kluczy agenta może mieć konsekwencje dla dużej liczby użytkowników systemu, a poniesione szkody mogą być trudne do oszacowania. Systemy z dzielonym kluczem muszą utrzymywać odpowiednią liczbę agentów, ale - z punktu widzenia zabezpieczenia - nowym elementem podatnym na zagrożenia jest punkt składania klucza.

Uprawniony podmiot żądający odtworzenia klucza jest również narażony na atak. Zagrożenia rozmyślne, takie jak podszycie się, maskarada, mogą się urzeczywistnić, np. wskutek przejęcia jego klucza prywatnego, służącego do celów identyfikacji i uwierzytelniania.

- **Złożoność systemu informatycznego TTP**

System kryptograficzny z odtwarzaniem kluczy musi zapewnić gromadzenie dużej liczby identyfikatorów tych kluczy. Implementacja schematu jest działaniem o wiele bardziej skomplikowanym niż zwykłego systemu kryptograficznego. Brakuje narzędzi projektowania i testowania systemów. Świadczy o tym przykład systemu Clipper [12]. Konieczność upowszechnienia systemów z odtwarzaniem kluczy rodzi niebezpieczeństwo wprowadzania na rynek produktów, które nie tylko nie gwarantują użytkownikom odpowiedniego poziomu zabezpieczenia, ale także narażają go na szkody z tytułu wad mechanizmów odtwarzania kluczy.

Istotnym problemem jest **skalowalność**. Nie ma podstaw do oceny skalowalności systemów z odtwarzaniem kluczy. W przypadku wdrażania tych systemów w środowiskach rozproszonych, przy ocenie skalowalności systemu należy uwzględniać:

- liczbę agentów odtwarzania kluczy (np. lokalizowanych w różnych krajach, organizacjach, przedsiębiorstwach itp.);
- liczb uprawnionych agencji (międzynarodowe, narodowe, lokalne);
- liczbę użytkowników (np. w aplikacjach internetowych - już obecnie kilka procent transakcji internetowych jest szyfrowanych; współczynnik ten będzie zwiększał się wraz z upowszechnianiem internetowych standardów szyfrowania);

- liczbę kluczy i certyfikatów publicznych kluczy; system z kontrolą kluczy musi rejestrować każdą parę kluczy - zaleca się stosowanie różnych kluczy w różnych aplikacjach; ponadto niektóre aplikacje generują parę kluczy dla każdej transakcji;
- liczbę kluczy sesyjnych, które mają podlegać kontroli; należy przyjąć, że system z odtwarzaniem kluczy będzie musiał zapewniać przetwarzanie milionów kluczy (dla każdego przechowywanego i zaszyfrowanego pliku, dla każdej wiadomości przesłanej pocztą elektroniczną, każdej transakcji internetowej itp.).

Powyższe wskaźniki będą wzrastać dynamicznie wraz z upowszechnianiem usług i sieci komputerowych na całym świecie.

- **Koszty TTP**

Konieczność uwzględnienia mechanizmów odtwarzania kluczy na etapie projektowania, implementacji i eksploatacji systemów kryptograficznych w istotny sposób wpływa na koszt tych systemów. Dodatkowo, mogą być generowane następujące koszty działania agenta odtwarzania klucza związane z:

- zabezpieczeniem szczególnie wrażliwych baz danych, zawierających klucze o długim czasie przechowywania;
- przetwarzaniem żądań odtworzenia kluczy - identyfikacją, uwierzytelnieniem, a także zapewnieniem odpowiednich parametrów realizacji zadań: czasu reakcji na żądanie, niezawodności infrastruktury i oprogramowania itp.;
- zabezpieczeniem przesyłania odtworzonej informacji.

W systemach z odtwarzaniem kluczy pojawiają się nowe źródła zagrożeń. Z racji wymienionych wcześniej słabości, w wielu obszarach ich działania poziom ryzyka można określić jako ekstremalnie wysoki. Wprowadzanie odpowiednich mechanizmów zabezpieczeń wiąże się z koniecznością ponoszenia stosownych nakładów finansowych.

- **Implikacje dla międzynarodowej struktury TTP**

Problem ten zostanie omówiony szczegółowo w pkt. 5.

4. PROTOKÓŁ DYSTRYBUCJI KLUCZY W STRUKTURZE TTP Z OPCJĄ ODTWARZANIA KLUCZY

Poniżej zaprezentowano jedyny znany i działający w praktyce protokół dystrybucji kluczy z wykorzystaniem techniki kryptograficznej z odtwarzaniem kluczy*) [8]. Szczegółowy opis protokołu umożliwi zrozumienie implikacji, jakie niesie sama jego postać dla komunikacji w międzynarodowej strukturze złożonej z wielu TTP. Nazwą protokołu jest skrót utworzony z pierwszych liter nazwisk jego autorów - JMW.

- **Założenia wstępne protokołu wymiany klucza w architekturze TTP z funkcją odtwarzania klucza**

1. Przyjmuje się następujące oznaczenia stron protokołu:
   A, B – podmioty,
   TA, TB – odpowiednio, TTP podmiotu A, TTP podmiotu B.
2. TA i TB mają uzgodnioną dużą liczbę pierwszą p (gdzie p-1 jest podzielne przez inną dużą liczbę pierwszą q) oraz uzgodniony element pierwotny δ modulo liczba p**).
   Te wartości zostały przekazane do podmiotów A i B.

---

*) Techniczną implementację przedstawiono po raz pierwszy na IV Międzynarodowej Konferencji IS&N, która odbyła się w Cernobbio (Włochy), 27-29 maja 1997 roku [10].

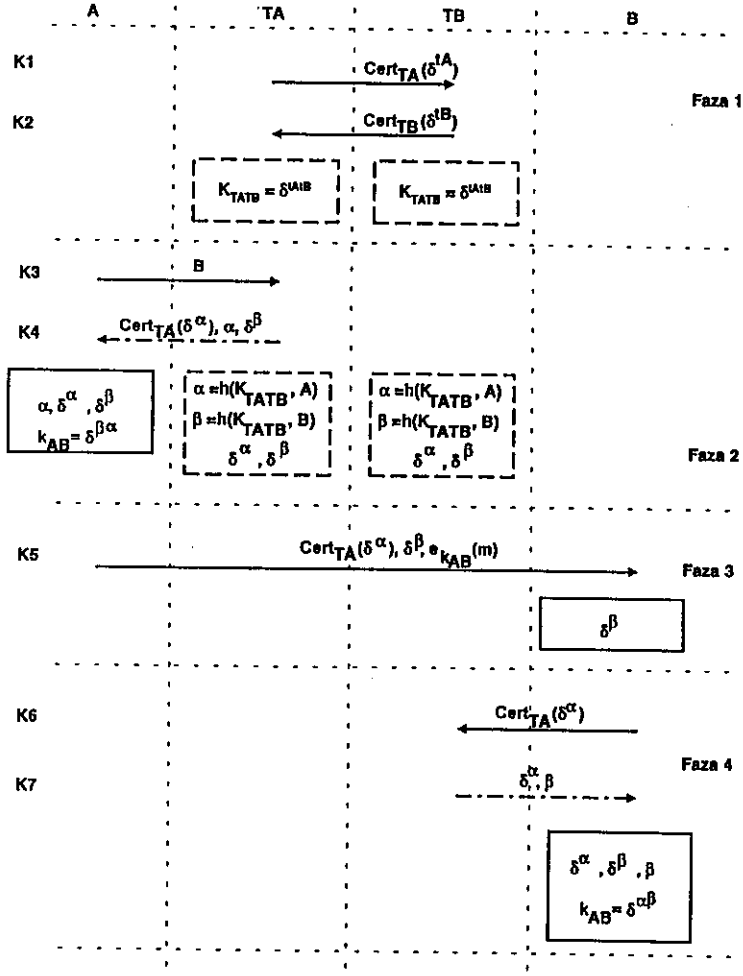
**) Element pierwotny δ generuje wszystkie liczby modulo p w taki sposób, że dla każdej liczby x modulo p istnieje liczba całkowita i taka, że $x = \delta^i$.

3. TA i TB uzgodniły funkcję generacji klucza h, dla której wartościami wejściowymi są: identyfikator podmiotu i wartość tajna, a wartością wyjściową - wartość klucza.
4. Każda TTP ma parę kluczy podpisu cyfrowego, w której prywatny klucz jest znany tylko TTP, a uwierzytelniona kopia klucza publicznego (weryfikującego) jest dostępna klientom TTP oraz innym TTP.
5. Każdy podmiot ma ze swoją macierzystą TTP wyodrębniony, bezpieczny kanał wymiany informacji, dzięki któremu można przeprowadzić uwierzytelnienie źródła danych oraz zapewnić integralność i poufność informacji.

W protokole następujące skróty i symbole oznaczają odpowiednio:

p	-	duża liczba pierwsza,
δ	-	uzgodniony między TA a TB prymityw modulo liczba pierwsza p,
tA, δ^{tA}	-	para kluczy (prywatny i publiczny) wykorzystywana przez TA w protokole uzgodnienia klucza z TB,
tB, δ^{tB}	-	para kluczy (prywatny i publiczny) wykorzystywana przez TB w protokole uzgodnienia klucza z TA,
h(K,id)	-	funkcja generacji prywatnego klucza dla podmiotu identyfikowanego jako *id*,
K_{TATB}	-	dzielony klucz tajny TA i TB,
$Cert_{TA}(\delta^{tA})$	-	certyfikat publicznego klucza δ^{tA} wydany przez TA,
α, δ^{α}.	-	para kluczy (prywatny i publiczny klucz nadawania) podmiotu A,
β, δ^{β}	-	para kluczy (prywatny i publiczny klucz odbioru) podmiotu B,
ek	-	funkcja symetrycznego szyfrowania za pomocą klucza k,
k_{AB}	-	dzielony klucz tajny podmiotów A i B.

Przebieg protokołu JMW przedstawiono na rys. 4.



Rys. 4. Protokół JMW wymiany kluczy

——→ - publiczny kanał wymiany informacji, - - - → - zabezpieczony kanał wymiany informacji między podmiotem a jego macierzystą TTP, ┌┄┐ - informacja uzyskana przez podmioty w kolejnych krokach protokołu

Faza 1 - ustanowienie tajnego klucza dzielonego między TA a TB

1. Każda TTP generuje parę kluczy (prywatny i publiczny) do celów uzgodnienia klucza, odpowiednio: (tA, δ^{tA}), (tB, δ^{tB}).
2. W komunikatach 1 i 2 (K1 i K2) TA i TB wymieniają certyfikaty publicznych kluczy $Cert_{TA}(\delta^{tA})$, $Cert_{TB}(\delta^{tB})$, używając odpowiedniego prywatnego klucza podpisującego.
3. Każda TTP weryfikuje otrzymany publiczny klucz drugiej strony, wykorzystując uwierzytelniony publiczny klucz, weryfikujący podpis cyfrowy drugiej strony.
4. Każda TTP oblicza dzielony klucz tajny K_{TATB}, używając własnego prywatnego klucza (dystrybucja kluczy wg schematu Diffie-Hellmana $K_{TATB} = \delta^{tAtB}$, $K_{TBTA} = \delta^{tBtA}$, $K_{TATB} = K_{TBTA}$).

Na końcu tej części protokołu TA i TB mają wspólnie ustanowiony klucz, za pomocą którego będą generować prywatny klucz odbioru podmiotu B.

Faza 2 - generacja certyfikatu w domenie podmiotu A do komunikacji z podmiotem B

5. Podmiot A wysyła do TA żądanie nawiązania komunikacji z podmiotem B (komunikat 3 - K3).
6. TA generuje liczbę losową α jako prywatny klucz nadawania podmiotu A i oblicza wartość klucza publicznego jako δ^{α}.
7. TA generuje certyfikat publicznego klucza nadawania podmiotu A, $Cert_{TA}(\delta^{\alpha})$.
8. TA oblicza prywatny klucz odbioru podmiotu B jako $\beta = h(K_{TATB},B)$ oraz odpowiadający mu klucz publiczny δ^{β}.
9. W komunikacie 4 (K4) TA odsyła podmiotowi A certyfikat jego publicznego klucza nadawania, jego prywatny klucz nadawania oraz publiczny klucz odbioru podmiotu B.

10. Podmiot A oblicza dzielony klucz $k_{AB} = \delta^{\beta\alpha}$, korzystając z wartości publicznego klucza odbioru podmiotu B (δ^{β}) oraz własnego prywatnego klucza nadawania α.

Na końcu tej fazy protokołu podmiot A ma wszystkie informacje, jakie potrzebuje, aby wysłać wiadomość do podmiotu B.

Faza 3 - przesłanie wiadomości od A do B

11. Podmiot A przesyła do B (komunikat 5 - K5) certyfikat swego publicznego klucza nadawania wydany przez TA, publiczny klucz odbioru podmiotu B oraz wiadomość zaszyfrowaną za pomocą dzielonego klucza k_{AB}.

Podmiot B musi teraz uzyskać odpowiednią informację od swej macierzystej TTP, która umożliwi mu odszyfrowanie wiadomości.

Faza 4 - weryfikacja certyfikatu podmiotu A w domenie podmiotu B i odszyfrowanie wiadomości

12. Po otrzymaniu wiadomości w kroku 5, podmiot B wysyła do TB żądanie (komunikat 6 - K6), zawierające certyfikat publicznego klucza nadawania podmiotu A wydany przez TA i publiczny klucz odbioru, który otrzymał w kroku 5 od podmiotu A.
13. TB oblicza prywatny klucz odbioru podmiot B, $\beta = h(K_{TATB}, B)$ i weryfikuje wartość δ^{β}.
14. TB weryfikuje certyfikat publicznego klucza nadawania podmiotu A, używając publicznego klucza weryfikującego TA.
15. TB odsyła do B publiczny klucz nadawania podmiotu A i prywatny klucz odbioru podmiotu B (komunikat 7 - K7).
16. B oblicza dzielony klucz $k_{AB} = \delta^{\alpha\beta}$, wykorzystując swój prywatny klucz odbioru i publiczny klucz nadawania podmiotu A.

Protokół jest zakończony. Podmiot B może odszyfrować zaszyfrowaną przez podmiot A, za pomocą klucza k_{AB}, wiadomość.

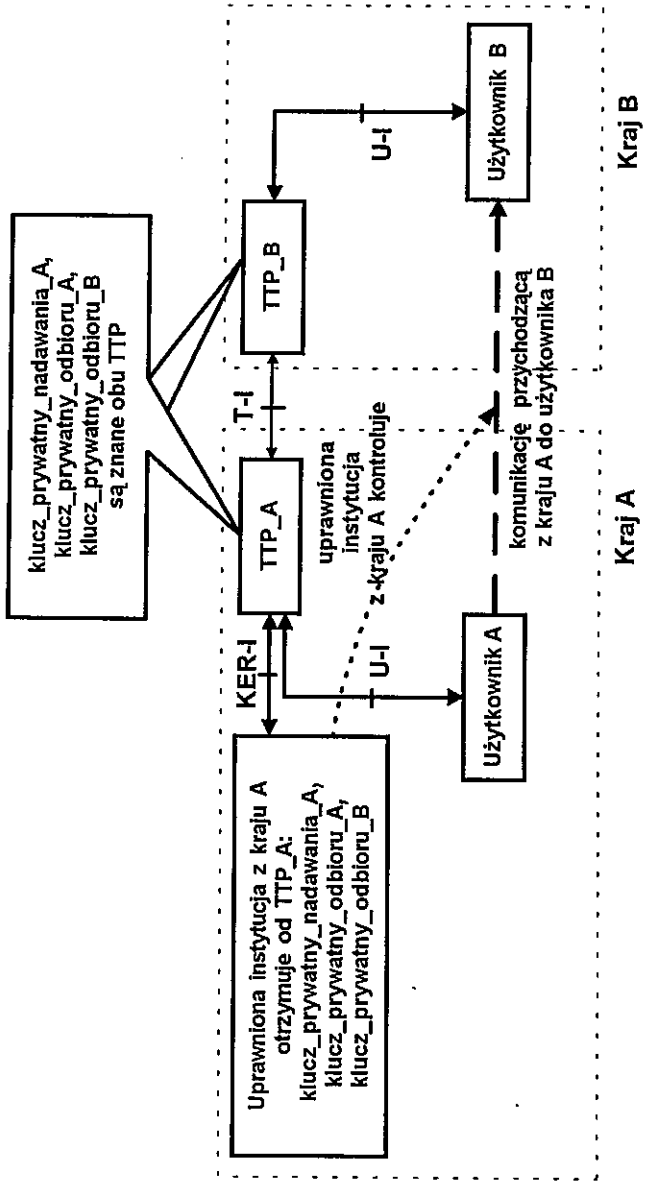
Własność odtworzenia klucza została w architekturze TTP zachowana, ponieważ TA oraz TB dysponują informacją wystarczającą do tego, aby móc odtworzyć klucz sesyjny k_{AB}.

Protokół JMW umożliwia na efektywne odtworzenie klucza przez TTP zarówno po stronie nadawania, jak i odbioru.

5. IMPLIKACJE ZASTOSOWANIA PROTOKOŁU JMW W MIĘDZYNARODOWEJ STRUKTURZE TTP

Odtworzenie dzielonego tajnego klucza jest możliwe przez TTP nadawcy (podmiotu A) i TTP odbiorcy (podmiotu B). TTP nadawcy może obliczyć klucz na podstawie znajomości zarówno „prywatnego klucza nadawcy", jak i „prywatnego klucza odbiorcy", podczas gdy TTP odbiorcy może obliczyć klucz na podstawie znajomości „prywatnego klucza odbiorcy". Wynika z tego, że TTP nadawcy (podmiotu A) ma pełną informację o jego kluczach, wykorzystywanych do nadawania i odbioru oraz dysponuje informacją o kluczu podmiotu B, wykorzystywanym do odbioru zaszyfrowanej wiadomości. Zgodnie z przyjętą zasadą *key recovery*, te informacje mogą być przekazane do uprawnionej agencji rządowej (EA_A).

Załóżmy sytuację, że użytkownik (podmiot) A znajduje się w kraju A, a użytkownik (podmiot) B - w kraju B. Uprawniona instytucja rządowa może kontrolować ruch przychodzący i wychodzący użytkowników w kraju A. Ale jednocześnie, uzyskując informację z TTP A o kluczu, wykorzystywanym przez użytkownika B do odbioru zaszyfrowanych wiadomości, może także kontrolować cały ruch przychodzący do użytkownika B z kraju A (rys. 5). W ten sposób instytucja rządowa z kraju A może kontrolować użytkownika w innym kraju, bez wiedzy uprawnionej instytucji rządowej oraz TTP w kraju B. Jeśli nie ma uzgodnień miedzy krajami A i B lub powszechnie akceptowanych, międzynarodowych rozwiązań prawnych, to sytuacja taka może szkodzić interesom kraju B.



Rys. 5. Międzynarodowe implikacje systemu kryptograficznego z odtwarzaniem kluczy

Konstrukcja interfejsu KER-I nie umożliwia powiadamiania użytkownika o uzyskaniu przez upoważnioną instytucję rządową jego prywatnych kluczy. Taki przypadek może stać w sprzeczności prawodawstwem danego kraju, w naszym przypadku z ustawą o danych osobowych, np. z art. 32 pkt 1 ust. 5 [14].

6. CZY W KONCEPCJI TTP MIEŚCI SIĘ KRYPTOGRAFIA KONTROLOWANA?

Zgodnie z definicją [7], ***zaufanie to związek między dwoma podmiotami, zbiór działań i polityka zabezpieczenia, w których podmiot x darzy zaufaniem podmiot y wtedy i tylko wtedy, gdy x ma przekonanie, że y będzie zachowywać się w dobrze zdefiniowany sposób (w odniesieniu do tych działań), tzn. taki, który nie narusza danej polityki zabezpieczenia.***

W systemach kryptograficznych z odtwarzaniem kluczy definicja zaufania jest inna. Zaufana trzecia strona (TTP) w tym systemie [9] to taka organizacja, która jest obdarzona zaufaniem zarówno przez użytkownika (podmiot), jak i uprawnioną instytucję! W żadnym razie nie spełnia ona definicji zaufania, w której są dwa, a nie trzy podmioty.

Elektroniczne realizacje usług komercyjnych, takich jak handel elektroniczny czy elektroniczna wymiana dokumentów, zakładają istnienie mechanizmów gwarantujących zawarte transakcje. Zastosowanie schematu odtwarzania kluczy podważa związek zaufania, jaki zachodzi między podmiotami. W świetle powyższej definicji dotyczy to np. gwarancji tożsamości stron (możliwość podszycia się) oraz niezaprzeczalności. Nie zostanie zachowane kryterium rozliczalności (jednoznaczności przyporządkowania klucza uwierzytelniającego oraz identyfikatora jego użytkownika - np. certyfikat klucza publicznego).

Z tego względu należy przyjąć, że kryptografia kontrolowana nie mieści się w koncepcji zaufanej trzeciej strony, którą można znaleźć w standardach ISO oraz dokumentach Komisji Europejskiej. Jeśli będzie istnieć konieczność tworzenia takich struktur, to nie należy ich nazywać zaufanymi trzecimi stronami.

Wewnętrzna struktura systemów z odtwarzaniem kluczy decyduje o tym, że są one mniej bezpieczne, bardziej kosztowne oraz trudniejsze w eksploatacji niż podobne systemy kryptograficzne bez tej funkcji. Powszechne wdrożenie systemów z odtwarzaniem kluczy spowoduje wzrost kosztów i obniżenie poziomu bezpieczeństwa przetwarzanej informacji. Obecnie nie istnieją na świecie systemy z odtwarzaniem kluczy, których skala i złożoność odzwierciedlałyby wymagania globalnej infrastruktury sieciowej. Wszelkie nie sprawdzone rozwiązania niosą ryzyko popełnienia błędów. Podejmując zatem wszystkie działania w zakresie wdrażania systemów z odtwarzaniem kluczy, obejmujące porozumienia międzynarodowe, standardy i regulacje, poza ograniczeniami prawnymi, należy brać pod uwagę także ograniczenia organizacyjne, techniczne i finansowe.

WYKAZ LITERATURY

1. Abelson H. i in.: The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption, http://www.crypto.com/key_study
2. Andrukiewicz E.: Zaufana trzecia strona (TTP) jako koncepcja bezpiecznej komunikacji w dobie społeczeństwa informacyjnego - zagadnienia społeczne, prawne, administracyjne i techniczne implementacji TTP w Polsce. Materiały konferencyjne - II Krajowa Konferencja Zastosowań Kryptografii, Enigma'98, Warszawa, 26 -28 maja 1998.
3. Dornan A.: Seeing Through Keyholes. Data Communications, Vol. 27, No. 8, July 1998.

4. http://ideath.parrhesia.com/wassenaar/wassenaar.html
5. ISO 7498-2: 1989 Information processing systems - Open Systems Interconnection - Basic Reference model - Part 2: Security Architecture, 1989 (krajowy odpowiednik: PN-2001/02:1993, Systemy przetwarzania informacji - Współdziałanie systemów otwartych (OSI) - Podstawowy model odniesienia - Architektura zabezpieczeń).
6. ISO/IEC 10181-1:1995 Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 1: Security Frameworks Overview.
7. ISO/IEC 13888:1997 Information technology - Security techniques - Non-repudiation - Part 1: General Model, 1997 (polskie tłumaczenie międzynarodowej normy przygotowywane w NKP nr 182).
8. Jefferies N., Mitchell C., Walker M.: A proposed architekture for trusted third party services, Cryptography: Policy and Algorithms, Lecture Notes in Computer Science, Vol. 229, 1996, pp. 98-104.
9. Licencing of Trusted Third Parties for the provision of encryption services - Public Consultation Paper, http://www.dti gov.uk/pubs/
10. Martin K.: Applying Cryptography within ASPeCT Project. Information Security Technical Report, Vol. 2, No. 4, 1998.
11. Matyas S.J.: Key Recovery Functional Model, http://www.kra.org
12. Patch K.: Clipper Flaw Foils Government 'Master Key', PC Week, 6 June, 1994.
13. Schneier B.: Kryptografia dla praktyków. WNT, Warszawa 1995.
14. Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. z 1997 r., nr 133, poz. 883.