# *Bezpieczeństwo w sieciach teleinformatycznych realizowane z udziałem zaufanej trzeciej strony (TTP)*

***Elżbieta Andrukiewicz***

*Zaprezentowano koncepcję oparcia bezpieczeństwa w sieciach teleinformatycznych na dwóch filarach: asymetrycznych technikach kryptograficznych oraz zaufanej trzeciej stronie. Wskazano usługi bezpieczeństwa realizowane za pomocą asymetrycznych technik kryptograficznych. Opisano sposób tworzenia podpisu cyfrowego oraz jego weryfikacji, a także strukturę zaufania do związku między kluczem publicznym a tożsamością jego właściciela. Zwrócono uwagę na inne usługi TTP, umożliwiające sprawdzenie wiarygodności podpisu w długim czasie, takie jak: usługa oznaczania czasu, notariat, archiwizacja i niezaprzeczalność. Omówiono pokrótce możliwe obszary zastosowań TTP oraz fundamenty, na których buduje się wiarygodność TTP. Przedstawiono dotychczasowe prace podjęte w Instytucie Łączności oraz zamierzenia dotyczące implementacji usług TTP.*

***zaufana trzecia strona (TTP), asymetryczne techniki kryptograficzne, podpis cyfrowy, infrastruktura klucza publicznego***

## Wstęp

Gwałtowny rozwój sieci teleinformatycznych w ostatnich latach umożliwił stosowanie nowych technik elektronicznych do działań realizowanych do tej pory za pośrednictwem tradycyjnych środków. Wiele codziennych czynności, które wymagały osobistego kontaktu stron, można już wykonać zdalnie. Coraz powszechniejsze stają się usługi bankowe na odległość, sprzedaż towarów i usług, systemy rezerwacji biletów. Jak jednak realizować takie usługi w bezpieczny sposób? Co więcej, w jaki sposób nowe techniki komunikacji mogą zrewolucjonizować i inne obszary działalności ludzkiej, chociażby relacje urząd – obywatel? W jaki sposób wreszcie mogą one przyczynić się do powstania kontaktów międzyludzkich nowego typu – wspólnych, wirtualnych debat (i głosowania) w sprawach dotyczących społeczności lokalnych, wspólnej nauki i rozrywki. Aktywność społeczna na wszystkich, wymienionych polach działania, realizowana za pomocą środków komunikacji elektronicznej, prowadzi w prosty sposób do społeczeństwa informacyjnego.

Akceptacja społeczna rzeczywistości informacyjnej musi jednakże wynikać z trzech podstawowych przesłanek: jedna z nich, to powszechność dostępu do środków komunikacji elektronicznej (gdzie można to znaleźć?), druga – powszechne uświadomienie i edukacja (jak tego używać?), trzecia – bezpieczeństwo komunikacji (czy to jest bezpieczne?). Aspekt socjologiczny bezpieczeństwa komunikacji elektronicznej jest, w opinii Autorki, niezwykle istotny. Przykładowo, przeciętnemu użytkownikowi sieci będzie trudno uwierzyć, że pojawiająca się na ekranie sekwencja znaków to naprawdę jego podpis cyfrowy – dowód jego tożsamości, który jest weryfikowalny w sposób natychmiastowy, obiektywny, automatyczny i niezawodny.

Bezpieczeństwo w sieciach teleinformatycznych polega na tym, że komunikujące się strony, nie znając siebie nawzajem, mogą wykonać czynność (zlecenie, kontrakt itp.) w taki sposób, aby żadna z tych stron nie mogła w przyszłości sfałszować jej treści lub zaprzeczyć swego uczestnictwa. Bezpieczeństwo w sieciach teleinformatycznych można implementować, opierając się na dwóch

filarach: zaawansowanych technikach kryptograficznych oraz instytucji, których idea jest znana od stuleci – zaufanych trzecich stron.

Zaufana trzecia strona jako fundament bezpieczeństwa komunikacji w sieci teleinformatycznej jest zasadniczym tematem niniejszego artykułu. Zastosowanie zaawansowanych technik kryptograficznych zostanie omówione jedynie w ogólnych zarysach.

## Asymetryczne techniki kryptograficzne

Asymetryczne techniki kryptograficzne wykorzystują dwa powiązane ze sobą przekształcenia, przekształcenie publiczne (definiowane przez klucz publiczny) i przekształcenie prywatne (definiowane przez klucz prywatny); te dwa przekształcenia charakteryzują się następującą własnością: jest obliczeniowo niewykonalne uzyskanie postaci przekształcenia prywatnego jedynie na podstawie znajomości postaci przekształcenia publicznego. Asymetryczną technikę kryptograficzną można wykorzystać w dwojaki sposób [5]:

– w systemie podpisywania, w którym przekształcenie prywatne jest przekształceniem podpisu, a przekształcenie publiczne służy do weryfikacji tego podpisu;
– w systemie szyfrowania, w którym przekształcenie publiczne służy do zaszyfrowania wiadomości, a przekształcenie prywatne do jej odszyfrowania.

Opierając się na obu typach przekształceń kryptograficznych można zbudować następujące usługi bezpieczeństwa:

1) w systemach podpisu:
   a) uwierzytelnienia użytkowników:
      – jednostronnego (nadawcy lub odbiorcy wiadomości),
      – wzajemnego (każda ze stron komunikacji uwierzytelnia drugą stronę);
   b) integralności wiadomości;
   c) niezaprzeczalności utworzenia wiadomości (tworzenie dowodu integralności i pochodzenia danych, który jest weryfikowalny przez trzecią stronę) w dowolnym momencie;
2) w systemach szyfrujących:
   a) poufności komunikacji;
   b) integralności komunikacji.

Zastosowanie asymetrycznych technik kryptograficznych może wyeliminować wiele zagrożeń występujących w komunikacji realizowanej w systemach teleinformatycznych, co przedstawiono w tablicy.

Najistotniejszym elementem bezpieczeństwa zastosowania asymetrycznych systemów kryptograficznych jest stworzenie wiarygodnego związku między kluczem publicznym a jego właścicielem. Tylko w takim przypadku istnieje możliwość weryfikacji podpisu cyfrowego dołączonego do dokumentu lub skuteczne zaszyfrowanie wiadomości.

W dalszym ciągu artykułu, dla uproszczenia, pominięto usługę poufności. Wszystkie stwierdzenia dotyczące problemu weryfikacji certyfikatów w zastosowaniach podpisu cyfrowego odnoszą się także do zastosowań szyfrujących. Inne dodatkowe aspekty zaufania do TTP realizujących usługę poufności można znaleźć np. w [1].

*Tabl. 1. Możliwość eliminacji zagrożeń*

| Zagrożenia | Usługi | | | |
|---|---|---|---|---|
| | Uwierzytelnienie podmiotów | Integralność danych | Niezaprzeczalność* | Poufność danych |
| Przechwycenie tożsamości | • | | | |
| Przechwycenie danych | | | | • |
| Maskarada (podszycie się) | • | | | |
| Powtórzenie | •(tożsamość) | •(dane) | • | |
| Manipulacja | | • | | |
| Zaprzeczenie | | | • | |

* *Realizacja usługi niezaprzeczalności wymaga implementacji dodatkowych usług omówionych w dalszej części artykułu.*

# Koncepcja zaufanej trzeciej strony (TTP)

**Zaufanie to związek między dwoma podmiotami, zbiór działań i polityka bezpieczeństwa, 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 bezpieczeństwa**.

W rozległej sieci teleinformatycznej nie ma możliwości realizacji takiego związku między każdą parą potencjalnych podmiotów – stron komunikacji elektronicznej. W tej sytuacji związek zaufania wynika z istnienia trzeciej strony (TTP) – podmiotu, który jest wiarygodny dla każdego z dwóch wymienionych wcześniej podmiotów w relacji dwustronnej.

Bardzo szerokie omówienie koncepcji zaufanej trzeciej strony można znaleźć w artykule [2].

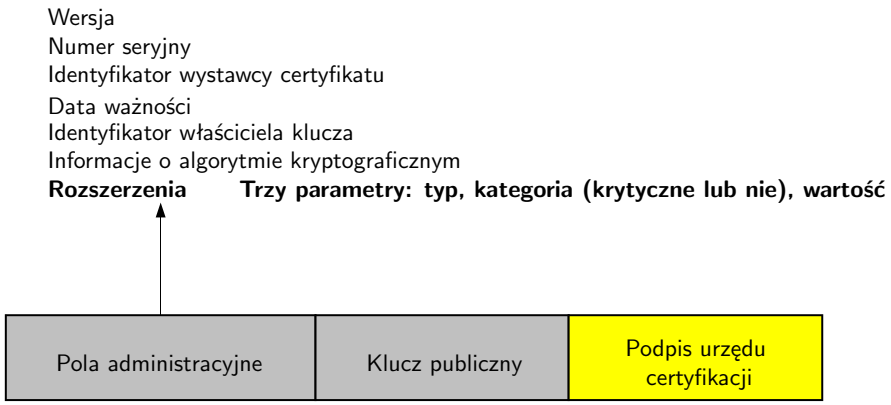
## *Urząd certyfikacji*

Warunkiem koniecznym wdrożenia asymetrycznych technik kryptograficznych w sieciach teleinformatycznych jest powstanie TTP darzonej zaufaniem przez potencjalnie dużą liczbę użytkowników sieci w zakresie świadczenia usług certyfikacji kluczy publicznych. Taka TTP jest wtedy urzędem certyfikacji (*Certification Authority*). Przez wydanie certyfikatu urząd gwarantuje autentyczność i niezaprzeczalne związanie klucza publicznego z tożsamością jego właściciela. Zgodnie z definicją przyjętą przez Komisję Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego (UNCITRAL) [9], certyfikat klucza publicznego powinien:

– umożliwiać identyfikację organu, który wydał certyfikat;
– określać jednoznacznie nazwę lub identyfikator podmiotu, który znajduje się w posiadaniu tego certyfikatu, lub urządzenia, lub elektronicznego agenta, który pracuje pod kontrolą tego podmiotu;
– zawierać publiczny klucz, który odpowiada kluczowi prywatnemu znajdującemu się w posiadaniu danego podmiotu;
– określać okres ważności tego certyfikatu (i zawierać ewentualne ograniczenia użytkowania klucza publicznego).

W odpowiedzi na zapotrzebowanie rynku powstało wiele rozwiązań dla certyfikatów kluczy publicznych. W ostatnim czasie dominującą rolę uzyskuje schemat certyfikacji opisany w zaleceniu ITU-T X.509v3 [7].

Podstawową strukturę certyfikatu w standardzie X.503v3 przedstawiono na rys. 1.




***Rys. 1.*** *Zawartość certyfikatu klucza publicznego wg zalecenia ITU-T X.509v3*

Gdy system teleinformatyczny jest rozległy i składa się z wielu domen bezpieczeństwa, niezależne urzędy certyfikacji mogą tworzyć strukturę, w której – na ściśle zdefiniowanych warunkach – następuje przekazywanie zaufania. W ten sposób, zamiast jednego urzędu powstaje ich ciąg, a zaufanie jest realizowane w postaci ścieżki dodatkowych certyfikatów wystawianych samym urzędom.

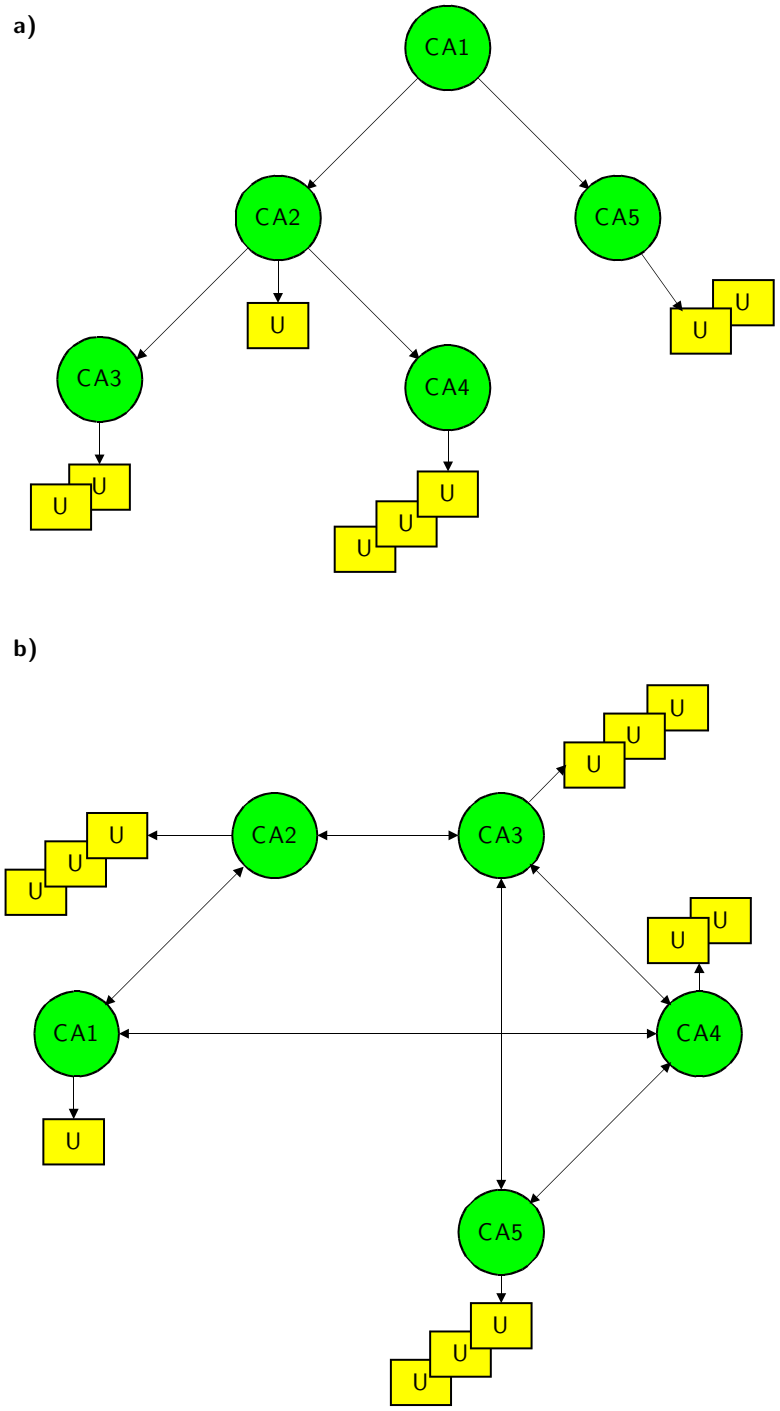
W ten sposób tworzy się strukturę organów certyfikacji, która może przybrać jedną z dwóch podstawowych form: struktury hierarchicznej (drzewa) oraz struktury certyfikacji wzajemnej (rys. 2).

W pierwszej z nich istnieje ścisła hierarchia organów certyfikacji, w której organ z wyższego poziomu hierarchii wystawia certyfikat dla klucza publicznego organu z następnego, niższego poziomu. Na samym szczycie drzewa istnieje organ pierwotny (tzw. *root*), któremu nikt certyfikatu wystawić już nie może. Integralność i uwierzytelnienie tego klucza muszą być zrealizowane za pomocą innych mechanizmów niż certyfikat.

W strukturze drugiego rodzaju organy certyfikacji wzajemnie wystawiają sobie i uznają certyfikaty.

Na pierwszy rzut oka struktura oparta na certyfikacji wzajemnej urzędów certyfikacji jest bardziej elastyczna i zapewnia minimalizację ścieżek certyfikacji. Niemniej jednak w momencie, gdy liczba tych urzędów jest bardzo duża, zarządzanie taką strukturą okazuje się zadaniem bardzo trudnym. Liczba wydawanych certyfikatów wzajemnych rośnie w postępie geometrycznym. Tak samo – liczba list unieważnionych certyfikatów. Samo sprawdzenie, czy dany certyfikat nie został unieważniony, wymaga przejścia po wielu węzłach struktury.

W strukturze hierarchicznej o wiele łatwiej zrealizować formalny nadzór nad realizacją wymagań stawianych urzędom certyfikacji. Urzędem sprawującym te funkcje, odpowiedzialnym jednocześnie za formułowanie wymagań, jest przeważnie urząd znajdujący się na szczycie hierarchii. W ten sposób w całej strukturze jest zagwarantowany poziom zaufania, który został określony przez urząd nadzorujący.




***Rys. 2.*** *Struktura urzędów certyfikacji: a) hierarchiczna; b) certyfikacji wzajemnej*

Należy wszakże nadmienić, że jednorodne struktury występują w praktyce rzadko. Istniejące struktury urzędów certyfikacji są przeważnie hierarchiczne, ale urzędy znajdujące się na szczycie poszczególnych hierarchii wystawiają sobie certyfikaty wzajemne. Jest to model, który można zastosować, np. przy wzajemnym uznawaniu ważności certyfikatów wystawianych w dwóch różnych krajach.

Szczegółowe opisy różnych modeli struktur certyfikacji można znaleźć np. w [3].

## *Rola certyfikatu klucza publicznego w procesie weryfikacji podpisu cyfrowego*

Proces tworzenia podpisanej wiadomości w systemie teleinformatycznym oraz weryfikacji podpisu cyfrowego przedstawiono na rys. 3. Przebiega on w następujący sposób:

- nadawca tworzy skrót wiadomości za pomocą tzw. funkcji skrótu[①];
- nadawca dokonuje przekształcenia kryptograficznego skrótu, tworząc w ten sposób podpis wiadomości;
- nadawca wysyła wiadomość wraz z jej podpisem do odbiorcy.

Odbiorca, otrzymując podpisaną wiadomość, musi znać klucz publiczny nadawcy, który umożliwi mu zweryfikowanie przedstawionego podpisu. Dysponuje też certyfikatem klucza publicznego nadawcy (może go otrzymać wraz z wiadomością lub uzyskać z publicznego repozytorium certyfikatów). Omówienie sposobów i technik dystrybucji certyfikatów kluczy publicznych wykracza poza obręb niniejszego artykułu. Proces akceptowania przedstawionego certyfikatu może wyglądać następująco:

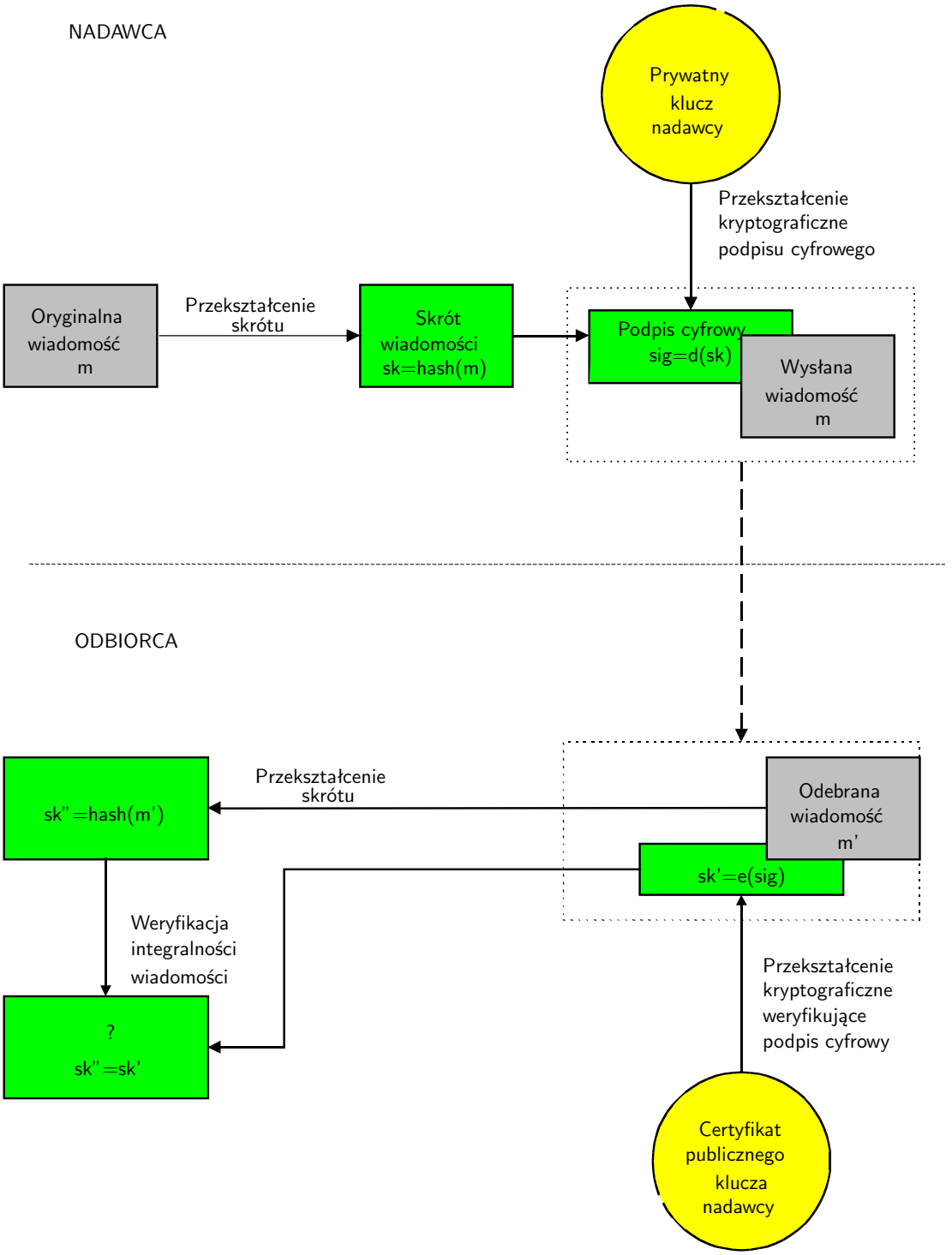
- odbiorca podpisanej wiadomości sprawdza, czy tożsamość tego, za kogo podaje się nadawca, jest identyczna z tożsamością zawartą w certyfikacie;
- odbiorca sprawdza, czy żaden z certyfikatów w rozpatrywanym ciągu nie został unieważniony oraz czy wszystkie certyfikaty znajdowały się w ich okresie ważności w momencie podpisania wiadomości;
- odbiorca sprawdza, czy w certyfikacie nie zostały zapisane ograniczenia używania klucza publicznego, które sprawiają, że nadawca nie ma odpowiednich uprawnień (np. do przeprowadzenia transakcji).

Uznając prawdziwość przedstawionego certyfikatu, odbiorca przystępuje do fazy weryfikacji wiadomości:

- za pomocą klucza publicznego nadawcy dokonuje przekształcenia, w wyniku którego otrzymuje skrót wysłanej wiadomości;
- oblicza skrót odebranej wiadomości;
- porównując wartości obu skrótów sprawdza, czy po podpisaniu wiadomość nie została zmieniona.

Jeśli wszystkie fazy weryfikacji zakończyły się sukcesem, to odbiorca ma podstawę do zaakceptowania podpisanej wiadomości.

① *Funkcja skrótu jest matematycznym przekształceniem, odwzorowującym dany ciąg bitów na inny ciąg bitów o skończonej długości, charakteryzującym się dwiema właściwościami: 1) dla danej wartości funkcji, znalezienie odpowiadającego argumentu tej funkcji jest obliczeniowo niewykonalne; 2) dla danego argumentu funkcji, znalezienie innego argumentu, dla którego wartość funkcji jest identyczna, jest obliczeniowo niewykonalne [6].*



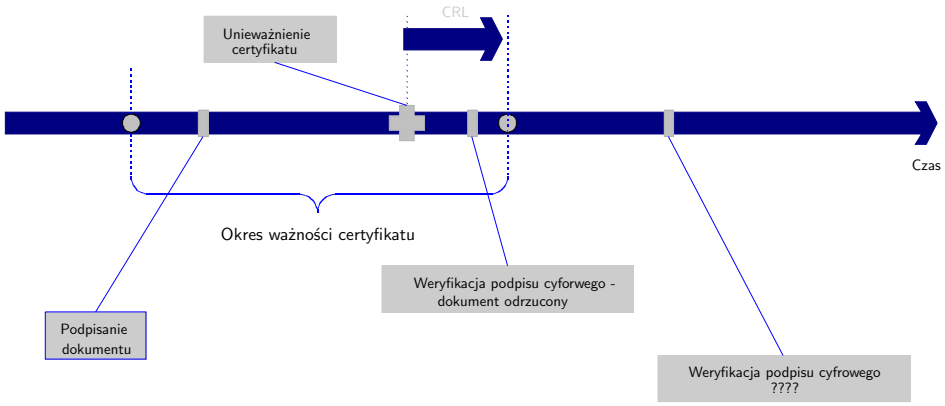

***Rys. 3.*** *Przekształcenie podpisu cyfrowego i jego weryfikacji*

Opisany proces jest określany jako krótkookresowa weryfikacja podpisu cyfrowego. Jest ona wystarczająca w całym kręgu zastosowań, które są znane pod zbiorczą nazwą „gospodarki elektronicznej" (*e-commerce*). Wszystkie te zastosowania mają jedną cechę charakterystyczną: celem jest sprawdzenie zdolności do realizacji transakcji w danej chwili lub w krótkim czasie (analogia z kartami kredytowymi jest tu oczywista).

Aby jednak sekwencja danych – uzyskana w wyniku kryptograficznego przekształcenia podpisującego i określana jako podpis cyfrowy – stała się pod względem prawnym równoważna podpisowi tradycyjnemu, musi zostać spełnionych wiele dodatkowych warunków. Jednym z nich jest możliwość weryfikacji podpisu cyfrowego w długim czasie.

## *Weryfikacja podpisu cyfrowego w długim czasie*

W wyżej opisanym schemacie stwierdzenie ważności podpisanego dokumentu po upływie ważności certyfikatu odpowiedniego klucza publicznego nie jest możliwe (rys. 4).




***Rys. 4.*** *Weryfikacja podpisu cyfrowego w długim czasie*

W istniejących hierarchiach urzędów certyfikacji weryfikacji podpisu cyfrowego można dokonać jedynie w okresie ważności certyfikatu klucza publicznego odpowiadającego kluczowi prywatnemu danego przekształcenia podpisu. Proces sprawdzenia, czy wskazany certyfikat nie został unieważniony przed upływem terminu jego ważności jest zwykle realizowany na podstawie listy unieważnionych certyfikatów (CRL)[①]. Ale certyfikat taki pozostaje na liście tylko do momentu, w którym upłynąłby jego normalny termin ważności. Po tym czasie pytanie o ważność podpisu cyfrowego na danym dokumencie nie znajdzie odpowiedzi.

Jeśli zachodzi potrzeba długookresowej weryfikacji podpisu cyfrowego, to poza strukturą urzędów certyfikacji powinny istnieć TTP, zapewniające dokumentom podpisanym cyfrowo wiarygodny znacznik czasowy oraz umożliwiające bezpieczne przechowywanie takich dokumentów. Wszystkie dalej omówione usługi, wraz z usługą certyfikacji, stanowią podstawę do realizacji **usługi niezaprzeczalności**.

① *Istnieją inne sposoby sprawdzenia ważności certyfikatów kluczy publicznych, np. za pomocą protokołu OCSP (Online Certificate Status Protocol) [8].*

### *Urząd oznaczania czasu*

Urząd oznaczania czasu jest zaufaną trzecią stroną dostarczającą poświadczenia istnienia dokumentu w momencie, w którym został wygenerowany znacznik czasu. Przykładowo, znacznik czasowy może być użyty do zweryfikowania faktu, że podpis cyfrowy został dołączony do dokumentu przed unieważnieniem certyfikatu klucza publicznego, co oznacza, że certyfikat może być użyty do weryfikacji tego podpisu. TTP oznaczania czasu musi dysponować wiarygodnym i niezawodnym źródłem czasu. Specyfiką działania takiego urzędu jest, że nie weryfikuje on danych, ale wyłącznie znacznik czasowy (przekształcenie kryptograficzne znacznika czasu jest realizowane na ciągu danych będącym skrótem wiadomości lub dokumentu).

### *Urząd notariatu*

Usługa elektronicznego notariatu umożliwia sprawdzenie i poświadczanie niektórych kategorii dokumentów (np. że dokument istniał w określonym momencie) w celu nadania tym dokumentom wiarygodności i autentyczności. Usługa ta może pełnić funkcje mediatora w przypadku sporu między podmiotami.

Pojęcie elektronicznego notariatu zawiera takie usługi TTP, jak: oznaczanie czasu, cyfrowa archiwizacja danych, niezaprzeczalność. Usługa ta może realizować rejestrowanie i przechowywanie dokumentów oznaczonych znacznikiem czasu oraz cyfrowym podpisem. Może też oferować rozszerzoną usługę długookresowej weryfikacji ważności danych. Proces weryfikacji realizowany przez TTP polega na dodaniu do zarejestrowanego dokumentu dodatkowej informacji w postaci tokena notarialnego.

Przykładowo TTP, działając jako organ notarialny, może dokonać weryfikacji certyfikatu (co rozwiązuje wyżej przedstawiony problem). Urząd notarialny weryfikuje ważność przedłożonego certyfikatu. W tym celu sprawdza całą ścieżkę certyfikacji od podmiotu, który podpisał certyfikat do zaufanego punktu w okresie od podpisania dokumentu do złożenia żądania weryfikacji tego podpisu (co może nastąpić po latach).

### *Urząd archiwizacji dokumentów podpisanych cyfrowo*

Usługa cyfrowej archiwizacji polega na rejestrowaniu elektronicznych dokumentów w taki sposób, aby zapis miał charakter zapisu stałego. Podstawowymi operacjami TTP, działającej jako rejestrator dokumentów, jest:

– składowanie dokumentów: TTP może przechowywać datowane wersje dokumentów na fizycznie zabezpieczonym nośniku przez oznaczony czas;

– wydawanie kopii dokumentów: usługa archiwizacji może wydać na żądanie podpisaną kopię zarejestrowanego dokumentu, łącznie z informacją o dacie zarejestrowania.

## Obszary zastosowań TTP

Sfery zastosowań usług TTP można znaleźć zarówno w sektorze publicznym, jak i prywatnym. W tej części artykułu przytoczono tylko niektóre, możliwe zastosowania usług TTP.

## Obszary zastosowań w sektorze publicznym

### Organy administracji rządowej i samorządowej

Nowe technologie umożliwiają wprowadzenie sieci teleinformatycznych jako środka komunikacji między urzędem a obywatelem. Wiele dokumentów istniejących w postaci papierowej może być przesyłanych elektronicznie z podpisem cyfrowym. Pierwszą praktyczną realizacją takiej usługi w Polsce jest elektroniczny obieg dokumentów miedzy ZUS-em a płatnikami składek ubezpieczeniowych. Inne usługi TTP otwierają cały szereg zastosowań, w których dokument musi mieć zdolność prawną przez wiele lat, np. akty urzędu stanu cywilnego, dokumenty ubezpieczeniowe czy choćby (najpowszechniejsze) zeznania podatkowe.

### Księgi notarialne i księgi wieczyste

Wykorzystanie cyfrowego podpisu w czynnościach notarialnych umożliwia zdalne podpisywanie dokumentów. Dokument przechowywany w postaci elektronicznej może być zweryfikowany na podstawie stwierdzenia ważności certyfikatu klucza publicznego w momencie jego podpisania (co mogło się zdarzyć przed wielu laty). Pieczęć notariusza może być zastąpiona jego podpisem cyfrowym i certyfikatem urzędu notarialnego.

### Rejestry znaków towarowych oraz patentów

Jednym z podstawowych kryteriów własności intelektualnej jest moment złożenia informacji do stosownego rejestru przez autora wynalazku czy projektu. Czynność ta, realizowana elektronicznie, wymaga uwierzytelnienia autora (usługa certyfikacji) oraz oznaczenia czasu otrzymania tej informacji (usługa oznaczania czasu). Usługa archiwizacji umożliwia składowanie tych informacji w postaci elektronicznej.

### Usługi pocztowe

Wiele organizacji pocztowych na świecie oferuje swym użytkownikom usługi certyfikacji w zakresie bezpiecznej wymiany dokumentów zarówno tradycyjnych usług (przesyłania teleksów i telegramów), jak i nowoczesnych (dokumentów poczty elektronicznej). Usługi te wymagają stosowania znaczników czasowych.

Warto przytoczyć przykład poczty USA, która – poza wyżej wspomnianymi usługami certyfikacji i oznaczania czasu – oferuje także usługi archiwizacji dokumentów elektronicznych (płaci się za określony okres przechowywania takiego dokumentu).

### Sądownictwo

Możliwości stosowania usług TTP w tym obszarze są niezmierzone. Praktycznie każda wymiana wiadomości sądowych wymaga uwierzytelnienia stron oraz oznaczenia czasem nadania/otrzymania. Ponadto, procedury w procesach karnych i cywilnych nakładają wymagania na jakość dowodów elektronicznych. Opatrzenie dokumentu podpisem cyfrowym i oznaczenie czasem może uwiarygodnić go w oczach sędziów.

### Publiczna opieka zdrowotna

Wraz z rozwojem zdalnych usług medycznych, np. zdalnej diagnostyki czy zdalnej analizy, rośnie znaczenie ochrony danych przesyłanych za pośrednictwem publicznych sieci teleinformatycznych. Usługa certyfikacji umożliwia bezpieczny i uwierzytelniony transfer informacji, oznaczanie czasu

– ustalenie wiarygodnej chronologii napływających informacji; usługa archiwizacji – bezpieczne przechowywanie kart chorobowych pacjentów.

## *Obszary zastosowań w sektorze prywatnym*

Niżej podane przykłady określają możliwe do przewidzenia obszary zastosowań dla prywatnych przedsiębiorstw i osób fizycznych.

### *Handel elektroniczny*

Jakkolwiek praktyczne implementacje zdalnego handlu (w postaci specyfikacji SSL lub SET) zakładają krótkookresową weryfikację podpisu cyfrowego, to dodatkowe usługi TTP mogą znacznie podnieść wiarygodność oferowanych serwisów. Realizacja usługi niezaprzeczalności stworzy podstawy do rozstrzygania potencjalnych sporów stron transakcji elektronicznych.

### *Zdalna praca*

Zdalna praca rodzi konieczność częstej wymiany dokumentów elektronicznych między pracownikiem a siedzibą firmy. Praca grupowa wymaga zwykle zapewnienia poufności, uwierzytelnienia nadawcy lub odbiorcy, integralności przesyłanych wiadomości oraz daty i czasu nadania/odbioru.

### *Transport*

Istnieją możliwości wprowadzenia sterowania przepływem towarów za pomocą elektronicznej wymiany dokumentów oraz udziału TTP w zapewnieniu bezpieczeństwa tym dokumentom. Przykładowo, usługa oznaczania czasu gwarantuje wiarygodność kontraktów zawierających terminy dostaw lub procedur logistycznych w sytuacjach, gdy zaangażowani są różni przewoźnicy oraz różne środki transportu.

### *Sektor finansowy (banki i towarzystwa ubezpieczeniowe)*

Specyfika branży bankowej stwarza wiele możliwości zastosowania usług TTP. Poza wymienionymi implementacjami protokołów płatniczych (SET) warto wspomnieć przykładowe aplikacje asymetrycznych technik kryptograficznych z wykorzystaniem kart inteligentnych, np. elektroniczną portmonetkę.

Wiele możliwości zastosowań znajduje się także w sektorze ubezpieczeniowym. Przykładowo, uwierzytelnienia stron oraz oznaczenia czasu wymaga elektroniczna procedura wystawiania polis ubezpieczeniowych.

## *Fundamenty bezpieczeństwa i zaufania [4]*

Koncepcja TTP opiera się na podstawowym założeniu, że usługa oferowana przez TTP zostanie zaakceptowana przez użytkowników, jeśli będzie dla nich wiarygodna. Zaufanie to wynika z przekonania, że TTP buduje swe usługi prawidłowo, zgodnie ze zdefiniowaną polityką bezpieczeństwa i warunkami umowy na świadczenie tych usług. To przekonanie może opierać się na następujących przesłankach:

a) TTP wypełnia zobowiązania wynikające z umowy ze swoimi klientami;
b) zasady odpowiedzialności TTP zostały jasno określone i zaakceptowane;
c) zgodność z prawem działalności TTP podlega stałej kontroli;
d) funkcje TTP są realizowane właściwie oraz zgodnie z jasno zdefiniowanym podziałem zadań i odpowiedzialności;

e) jakość procesów, działań oraz procedur jest zgodna ze stosownymi normami jakości (np. ISO 9000);

f) zarządzanie TTP uwzględnia aspekty zarządzania zabezpieczeniami, zapewniając m.in.:

   – odpowiednią identyfikację zagrożeń oraz mechanizmów zabezpieczeń,
   – regularne przeprowadzanie analizy ryzyka;

g) została wdrożona odpowiednia polityka bezpieczeństwa;

h) styk z użytkownikiem jest zdefiniowany w sposób odpowiedni do realizowanych funkcji oraz jest prawidłowo użytkowany;

i) działanie TTP podlega nadzorowi ze strony niezależnego organu w zakresie zgodności z zasadami udzielonej akredytacji.

Spełnienie wszystkich powyższych warunków powoduje, że TTP może oferować na rynku zaufanie, którego poziom jest sprawdzalny i weryfikowalny. **To jednak oznacza, że stworzenie TTP jest bardzo złożonym zadaniem, nie tylko pod względem technicznym, ale przede wszystkim organizacyjnym, prawnym i społecznym.**

# Prace podjęte w Instytucie Łączności w zakresie usług TTP

Prace nad zastosowaniem koncepcji TTP w sieciach teleinformatycznych rozpoczęły się w 1998 r.

1. Prowadząc prace koncepcyjne, dokonano wstępnej analizy możliwości technicznych, prawnych i organizacyjnych implementacji poszczególnych usług w Polsce. Efektem jest pierwsze w Polsce całościowe opracowanie dotyczące koncepcji TTP w sieciach teleinformatycznych [2].
2. W październiku 1998 r. przystąpiono do praktycznej implementacji pierwszej usługi TTP w postaci urzędu certyfikacji. Prace nad urzędem certyfikacji były kontynuowane w 1999 roku i objęły:

   – wykonanie testów zastosowania certyfikatów X.509v3 dla wybranych usług sieciowych: www, telnet, poczta elektroniczna;
   – opracowanie założeń realizacyjnych urzędu certyfikacji oraz wstępne określenie polityki bezpieczeństwa urzędu certyfikacji;
   – uruchomienie pilotażowej wersji urzędu certyfikacji działającego na potrzeby IŁ;
   – rozpoczęcie prac nad oprogramowaniem wspomagającym działanie urzędu certyfikacji, niezależnym od użytkowanych programów (podpisywanie dokumentów, weryfikacja podpisu cyfrowego).

## *Przewidywane kierunki działań*

W najbliższym czasie jest planowane podjęcie następujących prac.

1. Wdrożenie polityki bezpieczeństwa dla urzędu certyfikacji, rozpoczęcie działalności jako zaufana trzecia strona w zakresie usług certyfikacji (przy założeniu powszechności dostępu do tej usługi jest niezbędne nawiązanie współpracy w innymi instytucjami tak, aby stworzyć polską infrastrukturę kluczy publicznych).
2. Wybór i nawiązanie strategicznej współpracy z partnerem, który może zapewnić odpowiednią sieć punktów rejestracji na potrzeby urzędu certyfikacji.

3. Przystąpienie do realizacji usługi oznaczania czasu.
4. Rozpoczęcie prac nad innymi usługami niezbędnymi do realizacji usługi niezaprzeczalności.

# Podsumowanie

Instytucja, która chciałaby pełnić rolę zaufanej trzeciej strony w strukturze bezpiecznej komunikacji za pośrednictwem sieci komputerowych, musi spełniać dwa podstawowe kryteria:

– mieć możliwości techniczne,
– być wiarygodną.

Na całym świecie poszukuje się takich instytucji. W sposób naturalny w wielu krajach wybiera się pocztę. Poczta od stuleci pełni podobną rolę w świecie usług tradycyjnych, wymagających zaufania między komunikującymi się podmiotami. Na przykład, administracja rządowa USA widzi w roli TTP właśnie pocztę. Pilotowa struktura oferująca usługi oznaczania czasu, uwierzytelnienia oraz cyfrowej archiwizacji została uruchomiona przez pocztę USA w 1997 roku. Dalszy rozwój tego projektu nie spotkał się jednakże z poparciem kół biznesu, które nie przejawiają ochoty obdarzenia zaufaniem w zakresie prowadzenia handlu elektronicznego właśnie poczty.

Tworząc TTP należy mieć na względzie niezwykle wysokie wymagania, jakie musi spełniać zaufana trzecia strona, jednakże specyfika usług TTP polega także na tym, że można je oferować niezależnie jedna od drugiej – zatem, w naturalny sposób, mogą powstawać struktury TTP oferujące różne usługi lub jedna TTP wprowadzająca stopniowo coraz to nowe usługi. Obie metody poszerzania zastosowań zaawansowanych technik kryptograficznych w sieciach teleinformatycznych mogą okazać się skuteczne, jednak w warunkach polskich, szczególnie w dobie rozszerzającej się liberalizacji rynku teleinformatycznego, ta pierwsza ma zdecydowanie większe szanse realizacji.

## *Bibliografia*

[1] Andrukiewicz E.: *Czy w koncepcji zaufanej trzeciej strony (TTP) mieści się kryptografia kontrolowana?* Biuletyn Informacyjny IŁ, 1998, nr 7, s. 3–27

[2] Andrukiewicz E.: *Zaufana trzecia strona (TTP) jako koncepcja bezpiecznej komunikacji w dobie społeczeństwa informacyjnego – aspekty prawne, organizacyjne i techniczne*. Prace IŁ, 1998, nr 11, s. 7–83

[3] Berkovits Sh. i in.: *Public Key Infrastructure Study*. Final Report, NIST 1994

[4] ISO/IECTR 14516 *Guidelines on the use and management of Trusted Third Party services*

[5] ISO/IEC 11770-1:1997 *Key management*. Part 1: *Framework* (wydana jako polska norma PN-ISO/IEC 11770-1:1998 *Technika informatyczna – Techniki zabezpieczeń. Zarządzanie kluczami – Struktura*)

[6] ISO/IEC 14888-1:1998 *Digital signatures with appendix*. Part 1: *General*

[7] ITU-T X.509 (08/97): *Information technology – Open Systems Interconnection – The Directory: Authentication framework*

[8] Myers M., Ankney R., Malpani A., Galperin S., Adams C.: *Online Certificate Status Protocol – OCSP*. RFC 2560, June 1999

[9] UNCITRAL: *Draft uniform rules on electronic signatures*. September 1999

## Elżbieta Andrukiewicz

Dr inż. Elżbieta Andrukiewicz (1959) – absolwentka Wydziału Elektroniki Politechniki Warszawskiej (1983); długoletni pracownik naukowy Instytutu Łączności w Warszawie (1983–1999), obecnie pracownik BPT Telbank SA (od 2000); autorka licznych publikacji; ekspert ISO; zainteresowania naukowe: teleinformatyka, bezpieczeństwo systemów informatycznych.
e-mail: Elzbieta.Andrukiewicz@telbank.pl