PRACE INSTYTUTU ŁĄCZNOŚCI

1998
111

PRACE INSTYTUTU ŁĄCZNOŚCI

INSTYTUT ŁĄCZNOŚCI NR 111

WARSZAWA 1998

ISSN 0020-451X

Redaktor: mgr Krystyna Juszkiewicz

Skład komputerowy: techn. Danuta Pol, techn. Grażyna Woźnica

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

SPIS TREŚCI

KOMUNIKAT

СОДЕРЖАНИЕ

СООБЩЕНИЕ

CONTENTS

STATEMENT

SOMMAIRE

COMMUNIQUE

INHALTSVERZEICHNIS

MITTEILUNG

Elżbieta Andrukiewicz

003.26

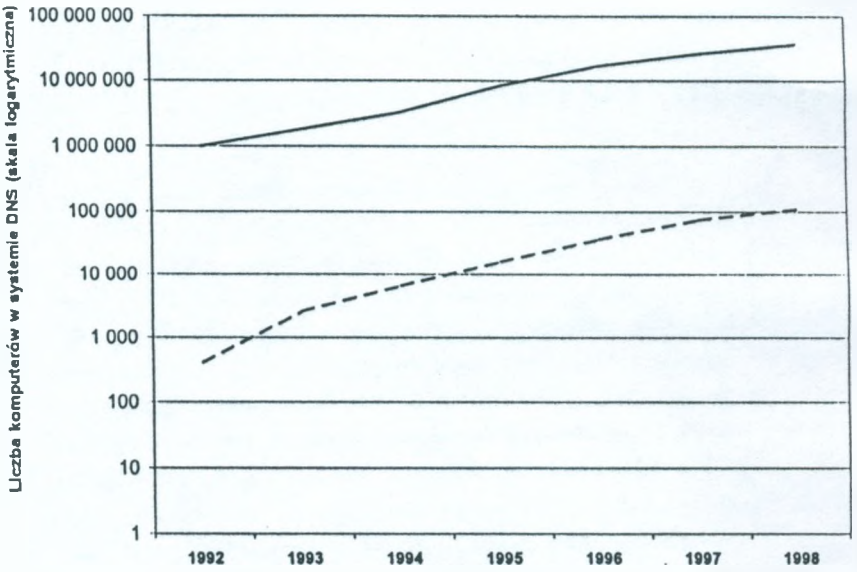
ZAUFANA TRZECIA STRONA (TTP), OFERUJĄCA USŁUGI BEZPIECZNEJ KOMUNIKACJI W DOBIE SPOŁECZEŃSTWA INFORMACYJNEGO - WARUNKI PRAWNE, ORGANIZACYJNE I TECHNICZNE

Przedstawiono koncepcję zaufanej trzeciej strony - instytucji gwarantującej bezpieczeństwo komunikacji w globalnych sieciach komputerowych za pomocą metod i narzędzi kryptograficznych. Omówiono podstawy prawne tworzenia instytucji tego rodzaju w Europie, problemy organizacyjne oraz zagadnienie zabezpieczenia samych instytucji TTP. Zaprezentowano usługi TTP oparte na przekształceniu podpisu cyfrowego i jego weryfikacji. Podkreślono, że do podstawowych usług TTP należą: zarządzanie kluczami kryptograficznymi, zarządzanie certyfikatami, usługa oznaczania czasu, usługa niezaprzeczalności, elektroniczny notariat. Poddano też analizie stan polskiego prawodawstwa w zakresie usług związanych z podpisem cyfrowym. Wskazano również trudności związane z wyborem w Polsce instytucji, która mogłaby pełnić rolę TTP.

1. ZAUFANE TRZECIE STRONY JAKO GWARANCJA BEZPIECZNEJ KOMUNIKACJI W SIECIACH KOMPUTEROWYCH

W ostatnich latach jesteśmy świadkami niezwykłego rozwoju ogólnoświatowej sieci komputerowej. Internet staje się powszechnym środkiem komunikacji międzyludzkiej. W pierwszej połowie lat dziewięćdziesiątych liczba komputerów dołączonych do Internetu

z każdym rokiem podwajała się (rys. 1). Jak wynika z wykresu, podobne tempo wzrostu (uwzględniając kilkuletnie przesunięcie na skali czasu) można zaobserwować także w Polsce.



Rys. 1. Dynamika wzrostu liczby komputerów dołączonych do Internetu*)

——— - świat – – – – - Polska

Globalny zasięg oraz dynamiczny rozwój powodują, że Internet staje się platformą komunikacji społeczeństwa informacyjnego końca dwudziestego wieku. Za jego pośrednictwem można już zrealizować usługi globalnej, publicznej sieci komputerowej. Do nich trzeba zaliczyć:

*) Źródło: Network Wizards, http://www.nw.com

- elektroniczny handel i usługi związane z nim bezpośrednio, takie jak: elektroniczne płatności (*Electronic Funds Transfer* - EFT) oraz elektroniczną wymianę dokumentów (*Electronic Data Interchange* - EDI);
- pracę na odległość (*teleworking*);
- zdalne nauczanie;
- elektroniczny notariat.

Możliwości, jakie oferuje globalna sieć komputerowa w zakresie komunikacji społecznej mogą stać się fundamentem społeczeństwa informacyjnego pod warunkiem powszechnej akceptacji nowych technik i metod pracy. Tej powszechnej akceptacji, mimo niezwykle dynamicznego rozwoju, Internet nie ma i nie będzie miał, jeśli rozwój ten będzie miał tak żywiołowy charakter, jak dotychczas.

1.1. Potrzeba bezpiecznej komunikacji w dobie społeczeństwa informacyjnego

Można postawić tezę, którą postaram się udowodnić na przykładzie handlu elektronicznego i pracy na odległość, że jakkolwiek usługi sieci globalnej rozwijają się szybko, to jednak znacznie wolniej niż przewidywały to wcześniejsze prognozy.

Jak podano w [2], całkowita sprzedaż elektroniczna produktów oraz usług w USA w 1995 r. wynosiła 518 mln dolarów. Prognozy na rok 2000 wahają się między 10 a 100 mld dolarów. Okazuje się, że 85% największych przedsiębiorstw amerykańskich (*America Fortune 1000*) ma swe serwery WWW i rocznie wydaje średnio między 0,75 a 1,25 mln dolarów, ale nie prowadzi elektronicznego handlu! Jest to na razie domena małych firm i transakcji o małej wartości.

Jeśli prześledzić prognozy dotyczące pracy na odległość, jakie pojawiały się od początku lat siedemdziesiątych, to należy stwierdzić,

że w miarę upływu lat zmniejszała się przewidywana liczba tak zatrudnionych [2]. Początkowo niektórzy futuryści uważali, że w 1990 r. wszyscy Amerykanie będą pracować w domu. Dekadę później informowano, że do 2000 r. w USA będzie to ok. 40% pracowników. Pod koniec lat osiemdziesiątych szacowano zaś, że w 2000 r. udział pracowników na odległość w ogólnym rynku pracy krajów rozwiniętych wyniesie 10÷15% (w zależności od kraju). Im bliżej do końca wieku, tym prognozy są skromniejsze.

Obecnie podaje się, że 10% przedsiębiorstw w USA zatrudnia pracowników na odległość. W krajach Unii Europejskiej jest to 5% (szacowana liczba takich pracowników w całej Unii Europejskiej wynosi 1,25 mln, w tym najwięcej w Wielkiej Brytanii i we Francji).

Dlaczego tak się dzieje?

Z przeprowadzonych ankiet [11] wynika, że spośród respondentów:

- 54% doświadczyło utraty informacji w ciągu ostatnich dwóch lat;
- 78% podobnie (jeśli zaliczyć straty spowodowane wirusami komputerowymi);
- większość respondentów nie potrafiła oszacować strat;
- 25% oszacowało je na 250 tysięcy dolarów USA;
- kilka procent - na więcej niż 1 mln dolarów USA;
- 85% respondentów uważa, że w ciągu ostatnich pięciu lat wzrosło ryzyko związane z bezpieczeństwem komunikacji w Internecie;
- 89% uważa, że byliby skłonni korzystać z usług Internetu, jeśli mieliby przekonanie, że są one bezpieczne.

Można zaryzykować zatem twierdzenie, że **na rozwój Internetu kładzie się cieniem brak standardów, poczucie niepewności, przekonanie, że nie jest to bezpieczne narzędzie komunikacji.**

To odczucie potwierdzają fakty [2]. W 1996 r. z 648 613 publicznych serwerów WWW mniej niż 1% miało możliwości przeprowadzenia "bezpiecznych transakcji" - 65 407 realizowało protokół SSL, ale tylko 3 239 z nich realizowało swe usługi korzystając z zaufanej trzeciej strony.

1.2. Co to jest zaufana trzecia strona?

Gwałtowny rozwój Internetu jest obecnie jego największym problemem. Internet stoi na rozdrożu. Linia podziału przebiega między jedną częścią użytkowników sieci, zwolenników wolności słowa i nieskrępowanego rozpowszechniania idei za pośrednictwem globalnej sieci komputerowej a drugą, która uważa, że ta nieskrępowana wolność jest główną przeszkodą do prawdziwego rozwoju powszechnych usług i społeczeństwa informatycznego. Dylemat ten można sformułować następująco.

Jak wyznaczyć równowagę między prawem jednostki do bezpiecznej, zgodnej z prawem, działalności w sieci komputerowej a prawem społeczeństwa do wykrywania i przeciwdziałania czynom niezgodnym z prawem oraz ochrony narodowych interesów?

Jedną z koncepcji, która mogłaby przyczynić się do nadania nowego impulsu rozwojowi powszechnych, globalnych i bezpiecznych usług komunikacji w sieciach komputerowych jest wykorzystanie do tego celu kryptografii. Usługi, których bezpieczeństwo gwarantowałyby stosowane techniki kryptograficzne, byłyby oferowane przez instytucję zwaną **zaufaną trzecią stroną** (TTP - *Trusted Third Party*).

Definicję zaufanej trzeciej strony można sformułować następująco [18].

Zaufana strona trzecia (TTP) to usługa lub organizacja, która ma zaufanie innych podmiotów*) w zakresie wszelkich podejmo-

*) Podmiot (*entity*), zgodnie z definicją zawartą w [12], jest to aktywna jednostka uczestnicząca w wymianie informacji. Podmiotem jest przeważnie określany proces (program, procedura), realizujący 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".

wanych przez nią działań związanych z bezpieczną komunikacją w sieci komputerowej.

W dalszej części niniejszego artykułu zostaną przedstawione prawne, organizacyjne i techniczne aspekty budowy tego zaufania.

1.3. Jak budować zaufanie?

Zgodnie z definicją [22], **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.**

Co powoduje, że TTP można zaufać? Wiele warunków musi spełnić organizacja, która chce pełnić rolę zaufanej trzeciej strony.

1.3.1. Jakie aspekty polityki bezpieczeństwa muszą być rozstrzygnięte w przypadku TTP?

Przekonanie, że TTP zapewnia usługi gwarantujące bezpieczeństwo komunikacji powinno przybrać postać formalnego dokumentu, określonego mianem "Polityki zabezpieczenia". Dokument ten musi zawierać cele, zasady, dyrektywy i procedury w odniesieniu do ogólnych zadań TTP oraz poszczególnych, oferowanych usług. Polityka zabezpieczenia powinna być realizowana na podstawie procesu zarządzania zabezpieczeniami systemu informatycznego, którego szczegółowy opis można znaleźć w [1].

1.3.2. Zarządzanie zabezpieczeniem systemu informatycznego TTP

Polityka zabezpieczenia systemu informatycznego powinna zawierać:

- ogólne zasady określone po raz pierwszy w wytycznych OECD (patrz pkt 2.4.1);
- właściwą strukturę organizacyjną przedsiębiorstwa ze szczególnym uwzględnieniem służb zabezpieczenia;
- poprawnie zdefiniowane procesy zarządzania zabezpieczeniem, w tym: prawidłową ocenę ryzyka opartą na szczegółowej analizie ryzyka oraz poprawny wybór i wdrożenie mechanizmów zabezpieczeń.

Ponadto, polityka ta powinna zawierać dyrektywy odnoszące się do:
- standardów, tj. tam, gdzie usługi zabezpieczeń są standaryzowane,
- klasyfikacji informacji,

a także procedury określające postępowanie w następujących sytuacjach:
- przeprowadzania audytów (wewnętrznych i zewnętrznych),
- utrzymania ciągłości działania w sytuacjach awaryjnych i katastrofalnych,
- naruszenia zabezpieczeń TTP,
- odtworzenia stanu sprzed katastrofy lub naruszenia.

1.3.3. Akredytacja

Akredytacja jest to uzyskanie od upoważnionego urzędu świadectwa formalnej zgodności systemu informatycznego i oferowanych usług z polityką bezpieczeństwa w warunkach eksploatacyjnych. Proces akredytacji składa się z przeglądu dokumentacji i odbioru technicznego.

Proces akredytacji powinien gwarantować sprawdzenie:
- zgodności z międzynarodowym i narodowym prawem,
- zgodności z normami technicznymi,
- zgodności z polityką bezpieczeństwa,
- zgodności z branżowymi i wewnętrznymi normami.

1.3.4. Jakość usług

Strona TTP powinna spełniać ogólne wymagania gwarantujące jakość usług przez realizację celów zabezpieczenia: poufności, integralności, dostępności, uwierzytelnienia, rozliczalności. Ponadto, TTP powinna wprowadzić politykę jakości i system jakości zgodny z serią norm ISO 9000.

1.3.5. Integralność organizacji i jej uregulowania prawnego

Strona TTP wymaga odpowiedniego prawodawstwa określającego cel i zasady jej funkcjonowania. Należy rozwiązać problem ewentualnych zasad udzielania licencji na działalność w roli TTP. Prawo powinno gwarantować niezależność TTP od innych podmiotów i niepodzielność świadczonych usług. Zagadnienie to szerzej omówiono w pkt. 2.

1.3.6. Zakres odpowiedzialności TTP

- **Zobowiązania kontraktowe**

Odpowiedzialność TTP musi być jasno określona formalną umową z klientem. Zobowiązania TTP muszą dotyczyć gwarantowania jakości oferowanych usług.

Zobowiązania TTP muszą być spójne z możliwościami finansowymi i gwarancjami wypłacalności (zobowiązania TTP powinny być objęte ubezpieczeniem).

- **Zobowiązania prawne**

Strona TTP powinna przestrzegać zasad określonych w dokumentach przedstawionych w pkt. 2. W ogólności, dotyczą one:
- demokracji,
- wolności przepływu informacji,

- ochrony danych i prywatności,
- ochrony własności intelektualnej, w tym praw autorskich,
- wykorzystania urządzeń kryptograficznych (na podstawie prawodawstwa krajowego),
- uprawnionego przechwytywania oraz legalnego dostępu do (szyfrowanych) danych.

Musi istnieć droga rozstrzygania sporów między TTP i jej klientami. Zgodność z prawem i zobowiązania prawne mają istotny wpływ na projekt i implementację TTP.

2. USŁUGI TTP W ZAKRESIE UWIERZYTELNIENIA I INTEGRALNOŚCI ELEKTRONICZNEJ KOMUNIKACJI

2.1. Fundamentalny podział usług kryptograficznych

Zgodnie z klasyfikacją wprowadzoną w dokumentach ISO [21], system kryptograficzny oferuje dwie podstawowe kategorie usług kryptograficznych: usługi uwierzytelniania i usługi szyfrowania (rys. 2). Usługi szyfrowania są wykorzystywane w celu zapewnienia kryptograficznej ochrony informacji, tzn. poufności danych. Usługi

Rys. 2. Klasyfikacja usług kryptograficznych

uwierzytelniania są w pierwszym rzędzie wykorzystywane w celu uwiarygodnienia podmiotów, źródła danych, integralności danych i niezaprzeczalności.

2.1.1. Usługi uwierzytelniania i klucze

Usługi uwierzytelniania zapewniają wiarygodność komunikujących się ze sobą podmiotów, uwierzytelnienie źródła danych, niezaprzeczalność i integralność danych. Usługi te mogą wykorzystywać takie mechanizmy, jak:

- **pieczętowanie**[*]) **jednostki danych**, obejmujące tworzenie kryptograficznej wartości kontrolnej w celu zapewnienia integralności danych, np. generację kodu uwierzytelniającego wiadomość (MAC) za pomocą algorytmu symetrycznego;
- **podpisywanie jednostki danych**, obejmujące tworzenie podpisu cyfrowego w celu uwierzytelnienia źródła danych, zapewnienia integralności danych lub niezaprzeczalności;
- **weryfikacja zapieczętowanej jednostki danych**, obejmująca obliczenie kryptograficznej wartości kontrolnej danych i porównanie jej z odpowiednią wartością kontrolną (dowód integralności danych);
- **weryfikacja podpisanej jednostki danych**, obejmująca weryfikację podpisu cyfrowego w celu określenia, czy był on utworzony przez tego, który podaje się za twórcę wiadomości i/lub jako dowód integralności danych.

---

[*]) Zgodnie z definicją zawartą w [18] (jest to norma starsza niż przytaczana w tekście), pieczęć to kryptograficzna wartość kontrolna, która gwarantuje integralność, ale nie chroni przed oszustwem odbiorcy (tzn. nie zapewnia niezaprzeczalności). Gdy pieczęć jest związana z elementem danych, to mówi się o nim, że jest zapieczętowany. W ujęciu tej definicji pieczętowanie nie ogranicza się tylko do symetrycznych technik kryptograficznych. Należy zwrócić uwagę, że jeśli TTP wykorzysta przekształcenie pieczętujące, to zapewni w ten sposób usługę niezaprzeczalności (patrz pkt 6).

W obrębie usługi uwierzytelniania procesy podpisywania i pieczętowania wykorzystują informację, która jest albo prywatna (tzn. jednoznaczna i poufna) dla twórcy wiadomości, albo tajna i znana jedynie twórcy wiadomości i jej odbiorcy; proces weryfikacji wykorzystuje albo procedury i informację, które są publicznie dostępne, ale z których nie można wydedukować prywatnej informacji twórcy wiadomości, albo sekret, który jest znany twórcy wiadomości i jej odbiorcy. Cechą charakterystyczną podpisywania jest to, że podpis cyfrowy może powstać jedynie z użyciem prywatnej informacji twórcy wiadomości, jego **klucza prywatnego**. Zatem, jeśli podpis cyfrowy zostanie zweryfikowany przy użyciu **klucza publicznego** twórcy wiadomości, w konsekwencji jest to dowód wobec trzeciej strony (np. organu notarialnego), że tylko jednoznacznie wskazany posiadacz prywatnej informacji mógł stworzyć ten podpis.

Usługa uwierzytelniania wykorzystuje dwa z trzech typów kluczy:
- **klucz pieczętujący**: wspólny **klucz tajny**;
- **klucz podpisujący**: jednoznaczny **klucz prywatny**, który jest związany z twórcą wiadomości;
- **klucz weryfikujący**: **klucz publiczny** lub **klucz tajny**.

W przypadku technik symetrycznych usługa uwierzytelniania wykorzystuje klucz pieczętujący i klucz weryfikujący, które są reprezentowane przez ten sam klucz tajny. W przypadku technik asymetrycznych usługa uwierzytelniania wykorzystuje klucz podpisujący i klucz weryfikujący, które są reprezentowane przez parę kluczy, składającą się z klucza publicznego i prywatnego.

2.1.2. Usługi szyfrowania i klucze

Usługi szyfrowania w pierwszym rzędzie zapewniają poufność danych, ale też ich integralność. W zależności od użytej techniki, usługi szyfrowania mogą obejmować usługi zabezpieczenia, takie jak uwierzytelnianie i niezaprzeczalność. Usługi szyfrowania wykorzystują dwa podstawowe mechanizmy:

- **zaszyfrowanie**, które na podstawie danych wejściowych tworzy tekst zaszyfrowany;
- **odszyfrowanie**, które 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 za pomocą dwóch różnych, ale związanych ze sobą kluczy, tzn. klucza publicznego i prywatnego.

W [4] podział usług kryptograficznych uznano za niezwykle istotny. Istnieje zasadnicza zgodność w kwestii zasad realizacji struktur TTP, oferujących usługi uwierzytelnienia i integralności oparte na podpisie cyfrowym, czyli z zastosowaniem asymetrycznych technik kryptograficznych.

Niemożliwe natomiast jest osiągnięcie w najbliższej przyszłości zgody w sprawie zasad realizacji usług poufności przez TTP (por. pkt 9).

2.2. Co to jest podpis cyfrowy?

W myśl przytoczonych definicji, TTP może oferować usługi gwarantujące uwierzytelnienie i integralność w komunikacji między podmiotami, wykorzystując do tego celu przekształcenie **podpisu cyfrowego** oparte na asymetrycznych technikach kryptograficznych. Jednakże, czy to podstawowe pojęcie jest przez wszystkich tak samo rozumiane? Okazuje się, że niekoniecznie. Oto kilka definicji podpisu cyfrowego.

1. **Dane dołączone do (lub przekształcenie kryptograficzne) jednostki danych, umożliwiające odbiorcy jednostki danych wery-**

fikację źródła pochodzenia oraz integralność tej jednostki oraz chroniące przed jej sfałszowaniem, np. przez odbiorcę.

Jest to najstarsza znana definicja podpisu cyfrowego znajdująca się w normie międzynarodowej [12].

2. **Dane dołączone do wiadomości, umożliwiające odbiorcy weryfikację źródła pochodzenia oraz integralność tych danych.**

   Ta definicja pochodzi z dokumentu brytyjskiego [23], zawierającego propozycję struktury zaufanej trzeciej strony oferującej usługę poufności.

3. **Pieczęć dołączona do cyfrowych danych, generowana przez prywatny klucz podpisu. Pieczęć ta określa właściciela klucza podpisu oraz gwarantuje integralność danych weryfikowaną za pomocą związanego klucza publicznego, zawartego w certyfikacie klucza podpisu wydanego przez organ certyfikujący.**

   Jest to definicja pochodząca wprost z niemieckiej ustawy [8] o podpisie cyfrowym.

4. **Przekształcenie kryptograficzne danych, umożliwiające odbiorcy danych sprawdzenie autentyczności i integralności danych oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę.**

   Definicja o takim brzmieniu została zamieszczona w pierwszej polskiej normie terminologicznej [29] z zakresu zabezpieczeń systemu informatycznego, wydanej w 1997 r.

W myśl powyższych definicji przez to samo pojęcie rozumie się zarówno "dane", jak i "przekształcenie kryptograficzne". Jednakże, taka interpretacja może prowadzić do zasadniczych nieporozumień w momencie definiowania struktury, zawierającej TTP świadczącej usługi uwierzytelnienia i integralności! Problem dotyczy zakresu odpowiedzialności TTP oraz podmiotu, czyli w tym kontekście osoby - użytkownika. Jeśli podpis cyfrowy to "dane", to za dane odpowiada ich właściciel (gestor), czyli użytkownik. Jeśli natomiast mówimy o "przekształceniu kryptograficznym", to za postać przekształcenia odpowiada TTP!

Jednoznacznego rozstrzygnięcia wymaga zatem kwestia rozróżnienia między tymi dwoma pojęciami. Wydaje się konieczne odróżnienie "podpisu cyfrowego" rozumianego jako sekwencja danych od "przekształcenia podpisu cyfrowego", które jest funkcją matematyczną. Tylko w pierwszym przypadku można mówić o formie równoważności podpisu cyfrowego i podpisu tradycyjnego, odręcznego. Bez uściślenia pojęcia "podpisu cyfrowego" będzie bardzo trudno wprowadzić do prawa całą sferę pojęć definiujących działania realizowane za pomocą komputerów, np.: elektroniczny dokument, elektroniczny kontrakt, elektroniczna faktura i elektroniczna wymiana informacji.

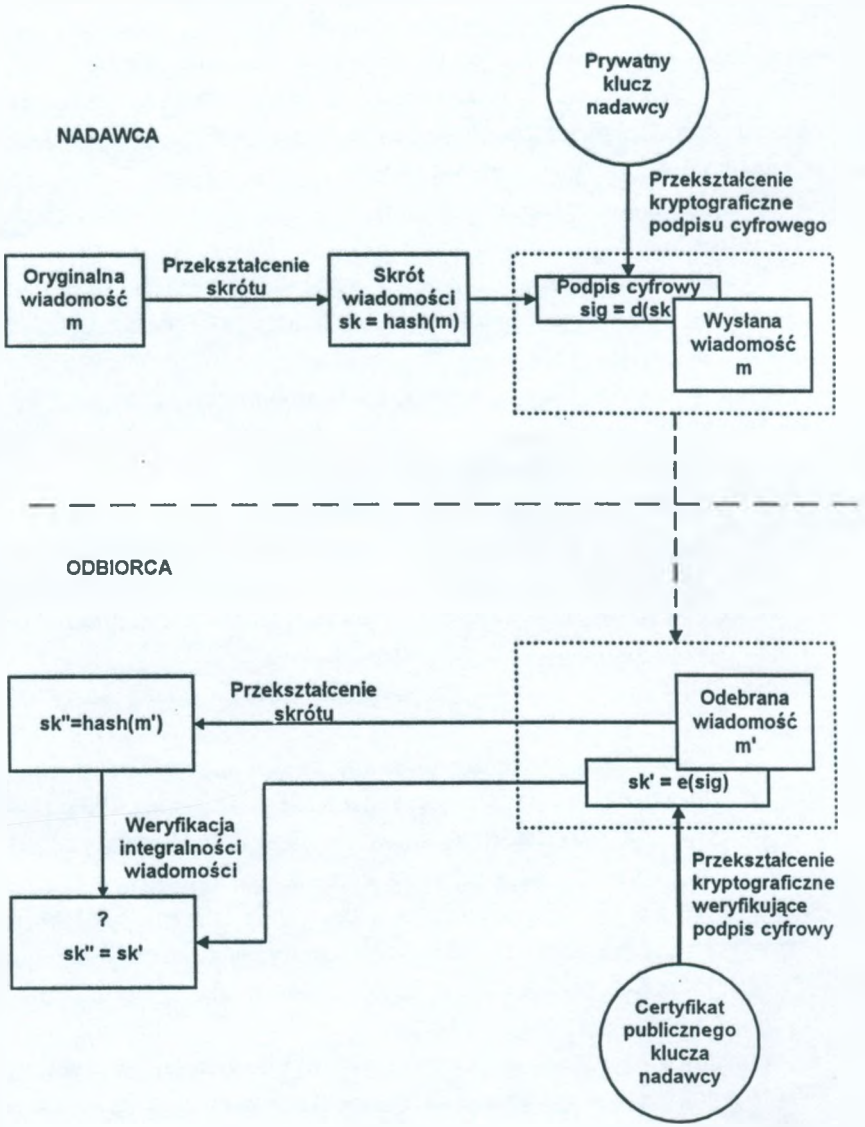
Warto zwrócić uwagę na bardzo zawężającą definicję, zawartą w niemieckiej ustawie. Już dziś można zaobserwować trudności w uzgadnianiu pojęć, np. na forum ISO (zastosowanie określenia "pieczęć", które we wszystkich nowych dokumentach ISO służą do określenia postaci przekształcenia opartego na symetrycznych technikach kryptograficznych - patrz pkt 2.1.1). Niemcy są najbardziej zaawansowanym krajem europejskim w dziedzinie upowszechniania struktur opartych na certyfikatach publicznych kluczy oraz podpisie cyfrowym, dlatego ich interpretacja standardów w tym zakresie może zdominować i nasze akty prawne.

Również definicja zawarta w polskiej normie wymaga uaktualnienia, gdyż taka postać, jaka jest proponowana w cytowanej polskiej normie, praktycznie uniemożliwia osadzenie pojęcia podpisu cyfrowego w naszym prawodawstwie.

Na rys. 3 zaprezentowano, zgodnie z wyżej przedstawioną interpretacją, przekształcenie **podpisu cyfrowego** i jego weryfikację.

2.3. Co to jest certyfikat klucza publicznego?

Stwierdzenie poprawności i autentyczności podpisu cyfrowego jest niemożliwe bez klucza publicznego, realizującego przekształcenie weryfikujące (rys. 3). Nie wystarczy jednak zastosować dowolny klucz publiczny - podmiot weryfikujący podpis cyfrowy musi mieć



Rys. 3. Schemat przekształcenia podpisu cyfrowego i jego weryfikacji

pewność, że klucz publiczny jest autentyczny (tzn. pochodzi z jedynej możliwej pary kluczy kryptograficznych, umożliwiającej za pomocą drugiego klucza - klucza prywatnego - utworzenie weryfikowanego podpisu cyfrowego). Powszechnie stosowaną metodą zapewnienia autentyczności klucza publicznego jest tworzenie i rozpowszechnianie certyfikatów kluczy publicznych. Usługę tę realizują zaufane trzecie strony, określane mianem organów certyfikacji (CA - *Certification Authority*).

Zgodnie z definicją podaną w [34], certyfikatem publicznego klucza jest sekwencja danych, która charakteryzuje się następującymi właściwościami:

- umożliwia identyfikację organu, który wydał certyfikat;
- określa jednoznacznie nazwę lub identyfikator podmiotu, który znajduje się w posiadaniu tego certyfikatu, lub urządzenia, lub elektronicznego agenta, który pracuje pod kontrolą tego podmiotu;
- zawiera publiczny klucz, który odpowiada kluczowi prywatnemu znajdującemu się w posiadaniu danego podmiotu;
- określa okres ważności tego certyfikatu (i zawiera ewentualne ograniczenia użytkowania klucza publicznego);
- jest podpisany za pomocą prywatnego klucza organu, który wydał certyfikat.

Certyfikat może zawierać wiele innych dodatkowych informacji.

W odpowiedzi na zapotrzebowanie różnych organizacji powstało wiele rozwiązań certyfikatów kluczy publicznych. W ostatnim czasie dominującą rolę uzyskuje schemat certyfikacji, opisany w zaleceniu ITU-TX.509v3 [37]. Stanowi on podstawę działania protokołów internetowych SSL i S-HTTP [32]. Schemat ten jest szczególnie godny uwagi, ponieważ przewidziano jego zastosowanie w ogólnoeuropejskiej strukturze podpisu cyfrowego [5].

Podstawową strukturę certyfikatu przedstawiono w tablicy 1. Nazwy pól podano zgodnie z zastosowaną w zaleceniu X.509 notacją ASN.1 [13]. W opisie pominięto szczegółową analizę pól rozszerzenia, które mogą w takim certyfikacie występować.

Tablica 1

Podstawowa struktura certyfikatu wg zalecenia X.509v3

Nazwa pola	Opis i zawartość pola
version	wersja certyfikatu X509 (v1, v2 lub v3)
serialNumber	numer seryjny certyfikatu
signature	identyfikator algorytmu podpisu cyfrowego
issuer	nazwa organu certyfikacji, który wydał certyfikat
validity	okres ważności certyfikatu: data początkowa i końcowa
subject	nazwa podmiotu, któremu wydano certyfikat
subjectPublicKey Info	identyfikator algorytmu, w którym certyfikowany klucz publiczny będzie używany oraz sam klucz publiczny (sekwencja bitowa)
issuerUnique Identifier	jednoznaczny identyfikator organu certyfikacji (tylko wersja v2 lub v3)
subjectUnique Identifier	jednoznaczny identyfikator podmiotu, któremu wydano certyfikat (tylko wersja v2 i v3)
extensions	pole (opcjonalne), zawierające rozszerzenia (tylko wersja v3) i m.in. umożliwiające umieszczenie certyfikatu w strukturze certyfikacji (hierarchicznej lub wzajemnej)

Zarządzanie certyfikatami kluczy publicznych, obejmujące cały zestaw usług oferowanych przez TTP pełniącą rolę organu certyfikacji, zostanie omówione w pkt. 5.

2.4. Podstawowe akty i dokumenty

W tym punkcie zostaną pokrótce scharakteryzowane podstawowe dokumenty, będące w społeczeństwie informacyjnym podstawą bez-

piecznej komunikacji, opartej na technikach kryptograficznych, a w szczególności koncepcji zaufanych trzecich stron. Dokumenty te mają zasadnicze znaczenie dla tworzenia prawnych, społecznych i organizacyjnych zasad budowy TTP.

2.4.1. Wytyczne OECD w zakresie zabezpieczeń systemów informatycznych

W dziedzinie zabezpieczenia systemów informatycznych pierwszym dokumentem o zasięgu ponadnarodowym był wydany w 1992 r. dokument [31]. W wielu późniejszych dokumentach jest on przywoływany jako źródło podstawowych unormowań.

W wytycznych sformułowano dziewięć podstawowych zasad zabezpieczenia systemów informatycznych. Zasady te muszą znaleźć się w dokumencie, który określa politykę zabezpieczenia każdej TTP.

1. **Zasada rozliczalności** (*Accountability Principle*) - obejmuje zdolność przypisania odpowiedzialności właścicielom, dostawcom, użytkownikom systemów informatycznych, jak również innym podmiotom (kierownictwo, programiści, dostawcy sprzętu i oprogramowania utrzymaniowego, wewnętrzni oraz zewnętrzni audytorzy itp.).
2. **Zasada świadomości** (*Awareness Principle*) - jest to, zgodne z prawem, zainteresowanie użytkowników bezpieczeństwem systemu informatycznego.
3. **Zasada etyki** (*Ethics Principle*) - wprowadza zasady życia społecznego do dziedziny użytkowania systemów informatycznych i ich zabezpieczania. Włącza też te zasady do wychowania i edukacji.
4. **Zasada multidyscyplinarności** (*Multidisciplinary Principle*) - określa pełny zakres potrzeb i możliwości zabezpieczenia systemów informatycznych.

5. **Zasada proporcjonalności** (*Proportionality Principle*) - nie każdy system wymaga pełnego zabezpieczenia; poziom i typ zabezpieczenia powinien odpowiadać powadze i prawdopodobieństwu szkody, jaka może się zdarzyć.
6. **Zasada integralności** (*Integration Principle*) - bezpieczeństwa systemu informatycznego nie można rozpatrywać niezależnie od reszty systemu. Problem zabezpieczenia występuje we wszystkich fazach cyklu informacyjnego: zbierania, przetwarzania, składowania, transmitowania i usuwania.
7. **Zasada aktualności** (*Timeliness Principle*) - potencjalne szkody mogą rozprzestrzeniać się z wielką szybkością; wspólne działania muszą być zatem podejmowane bez zbędnej zwłoki (przedsiębiorstwa o różnej strukturze własności i w różnych krajach).
8. **Zasada uaktualnienia szacowania** (*Reassessment Principle*) - wyraża dynamiczny charakter zmian zachodzących w systemach informatycznych. Szacowanie wartości zasobów informatycznych, analizę ryzyka należy powtarzać okresowo.
9. **Zasada demokracji** (*Democracy Principle*) - interes właścicieli, operatorów, producentów i użytkowników musi być postrzegany przez pryzmat zasad użytkowania i przepływu informacji w demokratycznych państwach prawa.

W wytycznych OECD sformułowano po raz pierwszy problem budowania zaufania i odpowiedzialności prawnej za przestępstwa popełnione w "cyberprzestrzeni".

2.4.2. Porozumienie z Wassenaar

Porozumienie [10] zostało podpisane w 1996 r. i zastąpiło COCOM. Wśród krajów, które podpisały ten układ, jest również Polska. W zakresie nas interesującym dotyczy ograniczeń eksportu produktów kryptograficznych. W porozumieniu zdefiniowano dwie listy: podstawową, produktów wrażliwych i (podlistę) bardzo wrażli-

wych. Kraje podpisujące zgodziły się na wymianę informacji o udzielonych odmowach w zakresie licencji eksportowych towarów grupy drugiej [3].

2.4.3. Ochrona danych osobowych

Ochrona danych osobowych została w Europie zapoczątkowana w Szwecji w latach siedemdziesiątych. Stojąc wobec problemu międzynarodowego transferu danych osobowych, w 1980 r. Rada Europy uchwaliła konwencję, w której kraje podpisujące zobowiązały się do wprowadzenia do swego prawodawstwa zapisów gwarantujących ochronę danych. Ustalono zasadę, że przy spełnieniu określonych warunków nie będzie można zakazać eksportu danych.

Na początku lat dziewięćdziesiątych powstała sytuacja, w której tylko sześciu spośród jedenastu członków Unii Europejskiej wprowadziło u siebie tę konwencję. Państwa członkowskie stanęły w obliczu zagrożenia, że w Zjednoczonej Europie nastąpi blokada przepływu danych. Kraje, które ratyfikowały konwencję (np. Francja), mogłyby zakazać eksportu danych osobowych do Belgii lub Włoch, wprowadzając w ten sposób kłopotliwe bariery dla rozwoju wolnego handlu. Aby usunąć te przeszkody, w 1995 r. Rada i Parlament Europejski wydały dyrektywę, dotyczącą ochrony przetwarzania danych osobowych oraz wolnego przepływu tych danych [6].

Dyrektywa nie odnosi się bezpośrednio do obywateli Unii ani unijnych organizacji. Jest ona skierowana do 15 krajów członkowskich i stawia formalne wymaganie wprowadzenia postanowień dyrektywy do krajowego ustawodawstwa, wyznaczając jednocześnie termin na październik 1998 r.

Dyrektywa normuje zasady dostępu do danych osobowych, określa warunki, w których może nastąpić odmowa dostępu do danych. Precyzuje też prawo do wolności dysponowania własną informacją. Ponadto dyrektywa wprowadza zakaz transferu danych osobowych do

krajów, których ochrona tych danych jest „nieadekwatna". Wzorując się na tej dyrektywie, polski parlament uchwalił w zeszłym roku ustawę o ochronie danych osobowych, która weszła w życie 30 kwietnia 1998 r. Od połowy 1998 r. nad bezpieczeństwem przetwarzania danych osobowych (ze szczególnym uwzględnieniem osobowych ewidencji komputerowych) czuwa Generalny Inspektor Ochrony Danych Osobowych.

Ochrona danych osobowych rozciągnięta na użytkowników Internetu może stanowić poważny impuls do rozwoju bezpiecznej komunikacji za pośrednictwem sieci komputerowych. TTP z natury rzeczy musi gwarantować bezpieczeństwo danych osobowych swoich użytkowników.

2.4.4. Zalecenia Rady (OECD), dotyczące wytycznych polityki w zakresie kryptografii

W 1997 r. został wydany dokument [30], stanowiący podstawę współpracy międzynarodowej w zakresie upowszechniania kryptografii. Ma on podstawowe znaczenie dla koncepcji TTP, gdyż definiuje zasady wprowadzania usług kryptograficznych do sieci komputerowych.

- **Cele tworzenia zalecenia**

Tworząc to zalecenie brano pod uwagę następujące cele:
- promowanie stosowania kryptografii;
- wzmacnianie zaufania do struktur informacyjnych i telekomunikacyjnych, systemów oraz sieci i sposobów ich użytkowania;
- pomoc w zabezpieczaniu danych, ochrona prywatności w krajowych i globalnych strukturach informacyjnych oraz telekomunikacyjnych, systemach i sieciach;
- promowanie legalnych zastosowań kryptografii bez niepotrzebnego narażania dobra publicznego i bezpieczeństwa narodowego;

- promowanie współpracy między sektorem publicznym a prywatnym przy tworzeniu i wdrażaniu kryptografii w kraju oraz na forum międzynarodowym na poziomie polityki, metod, środków, praktyk i procedur;
- wzbogacanie handlu międzynarodowego przez promowanie efektywnych, zdolnych do współdziałania*), mobilnych**) i przenaszalnych***) systemów kryptograficznych;
- promowanie międzynarodowej współpracy na poziomie rządów, środowisk biznesowych i naukowych oraz organizacji standaryzacyjnych, mającej na celu skoordynowane użytkowanie systemów kryptograficznych.

● **Pryncypia określone w zaleceniu**

1. **Zaufanie dla metod kryptograficznych**

Metody kryptograficzne powinny cieszyć się zaufaniem, aby użytkownicy mogli bezpiecznie używać systemów informacyjnych i telekomunikacyjnych.

Zaufanie to powinno być budowane na podstawie wolnej gry sił rynkowych, niemniej jednak jest to także zadanie rządów i organizacji standaryzujących. Polega ono na formułowaniu kryteriów oceny metod kryptograficznych oraz tworzenia warunków, w których metody te mogą być poddane weryfikacji.

---

*) Zdolność do współdziałania (*interoperability*) - techniczna zdolność metod kryptograficznych do współpracy.

**) Mobilność (*mobility*) - techniczna zdolność metod kryptograficznych do funkcjonowania w różnych krajach lub strukturach informacyjnych i telekomunikacyjnych.

***) Przenaszalność (*portability*) - techniczna zdolność metod kryptograficznych do pracy w wielu systemach.

2. Wybór metod kryptograficznych

Użytkownicy powinni mieć prawo do wyboru dowolnej, akceptowanej prawnie, metody kryptograficznej.

Podstawowym kryterium wyboru metod kryptograficznych powinny być indywidualne wymagania użytkownika w zakresie zabezpieczenia systemów i danych. Użytkownicy powinni mieć możność wyboru różnych metod kryptograficznych i systemów zarządzania kluczami kryptograficznymi do realizacji różnych celów zabezpieczenia. W celu ochrony interesu publicznego, jakim jest ochrona danych osobowych lub handel elektroniczny, rządy mogą wymagać, aby metody kryptograficzne osiągały odpowiedni poziom zabezpieczenia. Kontrola metod kryptograficznych przez rządy nie powinna wykraczać poza minimum niezbędne do wypełnienia obowiązku ochrony dobra publicznego i w żadnym razie nie powinna ograniczać swobody wyboru metody kryptograficznej.

3. Kierunek rozwoju metod kryptograficznych wyznaczany przez rynek

Kierunek rozwoju metod kryptograficznych powinien odzwierciedlać potrzeby, wymagania i zakres odpowiedzialności osób, przedsiębiorstw i rządów.

Rozwój oraz oferta metod kryptograficznych powinny być determinowane przez wymagania otwartej konkurencji. Takie podejście gwarantuje nadążanie za zmieniającą się technologią, wymaganiami użytkowników oraz szybką reakcję na pojawiające się nowe zagrożenia dla bezpieczeństwa systemów informacyjnych i telekomunikacyjnych. Również rozwój międzynarodowych standardów technicznych, kryteriów i protokołów związanych z metodami kryptograficznymi powinien podążać w kierunkach wyznaczanych przez rynek.

4. **Standardy dla metod kryptograficznych**

Należy opracowywać i wprowadzać w życie standardy techniczne, kryteria i protokoły dla metod kryptograficznych, zarówno krajowe jak i międzynarodowe.

W odpowiedzi na potrzeby rynku, uznane, międzynarodowe organizacje standaryzacyjne, rządy, eksperci z kół biznesu, powinni podjąć współpracę w celu opracowywania oraz upublicznienia zdolnych do współdziałania standardów technicznych, kryteriów i protokołów dla metod kryptograficznych. Jeśli powstają krajowe standardy w tej dziedzinie, to powinny one być zgodne ze standardami międzynarodowymi tak, aby realizować globalną zdolność do współdziałania, mobilności i przenaszalności.

5. **Ochrona prywatności i danych osobowych**

Przy formułowaniu krajowej polityki, a także przy implementacji i użytkowaniu metod kryptograficznych należy respektować fundamentalne prawa do prywatności, obejmujące poufność komunikowania się i ochrony danych osobowych.

Metody kryptograficzne mogą skutecznie zapewnić ochronę prywatności, w tym poufność komunikowania się i ochronę tożsamości podmiotów. Użycie metod kryptograficznych prowadzi do minimalizacji baz danych, zawierających dane osobowe oraz gwarantuje bezpieczeństwo transakcji realizowanych za pomocą mediów elektronicznych. Jednocześnie, wykorzystanie metod kryptograficznych zapewniających integralność danych i uwierzytelnienie podmiotów - stron transakcji wymaga gromadzenia danych osobowych. Systemy takie powinny być w odpowiedni sposób zaprojektowane, z uwzględnieniem odpowiednich mechanizmów ochrony prywatności danych.

6. **Dostęp do danych na mocy prawa**

Krajowa polityka w zakresie kryptografii może dopuszczać dostęp osób trzecich, na mocy prawa, do tekstu otwartego,

który został zaszyfrowany lub do kluczy kryptograficznych, umożliwiających odszyfrowanie tekstu zaszyfrowanego. Taka polityka musi w najwyższym możliwym stopniu respektować inne pryncypia zawarte w niniejszym zaleceniu.

Osoba lub podmiot żądający na mocy prawa dostępu do tekstu otwartego, który został zaszyfrowany lub kluczy kryptograficznych, umożliwiających odszyfrowanie takiego tekstu musi mieć prawomocny tytuł do uzyskania tekstu otwartego. Taki tekst nie może być użyty w żadnym innym celu niż ten, który został określony w postępowaniu prawnym. Warunki, w których taki dostęp byłby możliwy, powinny być jasno określone oraz upublicznione w taki sposób, aby użytkownicy, właściciele kluczy oraz dostawcy metod kryptograficznych mogli łatwo zapoznać się z nimi. Systemy zarządzania kluczami powinny zawierać rozwiązania, które zapewnią równowagę miedzy interesem użytkowników a interesem publicznym, reprezentowanymi przez uprawnione agencje rządowe. Proces przetwarzania danych na potrzeby uprawnionych agencji rządowych musi rozróżniać klucze kryptograficzne, które są wykorzystywane do ochrony poufności (szyfrowania) oraz klucze kryptograficzne wykorzystywane do innych celów (np. do ochrony integralności, uwierzytelnienia lub niezaprzeczalności).

7. Zakres odpowiedzialności prawnej

Niezależnie od tego, czy jest narzucona warunkami kontraktu, czy wynika z mocy ustawy, odpowiedzialność prawna podmiotów oferujących usługi kryptograficzne lub przechowujących albo udostępniających klucze kryptograficzne powinna być jasno określona.

Należy określić także odpowiedzialność użytkowników w przypadku niewłaściwego użycia własnych kluczy kryptograficznych.

Odpowiedzialność podmiotu przechowującego klucze nie powinna obejmować przypadku przekazania uprawnionej stronie trzeciej tekstu otwartego lub kluczy kryptograficznych, umożliwiających odszyfrowanie tekstu wcześniej zaszyfrowanego, jeśli odbyło się to zgodnie z procedurą prawną. Podmiot, który uzyskał dostęp na powyższych zasadach musi przyjąć odpowiedzialność za niewłaściwe wykorzystanie tych wiadomości.

8. **Współpraca międzynarodowa**

Rządy powinny nawiązać współpracę w celu skoordynowania polityki w zakresie kryptografii. Jako część tych wysiłków, rządy powinny usuwać lub unikać tworzenia rozwiązań, które w imię tej polityki mogłyby się stać barierą dla wolnego handlu.

Aby propagować szeroką akceptację dla kryptografii na arenie międzynarodowej oraz umożliwić w pełni rozwój ogólnoświatowych sieci informacyjnych i telekomunikacyjnych, rządy poszczególnych krajów powinny w najwyższym możliwym stopniu koordynować prowadzoną przez siebie politykę w zakresie kryptografii. Krajowe systemy zarządzania kluczami powinny tam, gdzie to konieczne, dopuszczać międzynarodowe wykorzystanie kryptografii. Uprawniony dostęp do danych w sieciach międzynarodowych powinien być realizowany na podstawie dwu- i wielostronnej współpracy oraz porozumienia. Żaden rząd nie powinien zabraniać wolnego przepływu szyfrowanych danych przechodzących przez obszar jego jurysdykcji, jedynie na podstawie zasad określonych w polityce w zakresie kryptografii. Aby wspierać rozwój wolnego handlu, rządy powinny unikać opracowywania polityki w zakresie kryptografii oraz procedur postępowania, które prowadziłyby do powstania nieuzasadnionych barier dla dostępności metod kryptograficznych na arenie międzynarodowej.

2.4.5. Struktura prawna elektronicznej wymiany informacji

W obrębie UNCITRAL*) są prowadzone prace dotyczące utworzenia podstaw prawnych do elektronicznej wymiany informacji. W 1996 r. powstał dokument (*Model Law*) [9], zawierający wytyczne do tworzenia prawa krajowego dotyczącego handlu elektronicznego. W dokumencie tym są definiowane pojęcia "zapisu", "kontraktu", "podpisu" i "poświadczenia" w elektronicznej postaci.

W 1997 r. wydano oddzielny dokument dotyczący samego podpisu cyfrowego [34]. Zaproponowano w nim rozwiązania prawne, umożliwiające wprowadzenie do prawodawstwa takich zagadnień, jak: podpis elektroniczny, podpis cyfrowy, certyfikat, organ certyfikujący, wzajemne respektowanie podpisów cyfrowych i certyfikatów klucza publicznego na arenie międzynarodowej.

Na szczególną uwagę zasługuje sformułowanie warunku, że podpis cyfrowy musi być jednoznacznie powiązany z osobą, która go dołączyła do elektronicznej wiadomości. Oznacza to, że prawdopodobieństwo utworzenia przez drugą osobę takiego samego podpisu cyfrowego, w celu jego sfałszowania lub innych nielegalnych działań, jest pomijalnie małe. Ponadto, przez weryfikację podpisu cyfrowego, dokonaną za pomocą certyfikowanego klucza publicznego, właściciel tego podpisu jest zidentyfikowany w sposób natychmiastowy, automatyczny i obiektywny. Warto zauważyć, że warunków takich nie spełnia zwykły podpis ręczny (często nieczytelny).

Przy takich założeniach prawnych oraz przy spełnieniu wymagań technicznych, umożliwiających realizację usług kryptograficznych, takich jak integralność, autentyczność i niezaprzeczalność (omówionych w dalszej części artykułu), można uznać moc prawną transakcji elektronicznej, dokonanej za pomocą podpisu cyfrowego.

---

*) Komisja Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego.

2.5. Budowa bezpiecznej struktury europejskiej TTP

Rok 1997 jest początkiem budowy ogólnoeuropejskiej struktury TTP, realizującej usługi uwierzytelnienia i integralności na podstawie przekształcenia kryptograficznego podpisu cyfrowego. W deklaracji ministrów uczestniczących w konferencji pt. "Globalne sieci informacyjne" [7] czytamy:

(38) [Ministrowie] podkreślają potrzebę stworzenia prawnej i technicznej struktury w Europie i na szczeblu międzynarodowym, która zapewnia: zgodność oraz buduje zaufanie oparte na cyfrowym podpisie, jest niezawodnym i przezroczystym sposobem realizacji integralności i autentyczności danych, dokumentów i wiadomości na potrzeby handlu elektronicznego i elektronicznych transakcji między organizacjami i obywatelami.

Stanowisko Komisji Europejskiej jest następujące [4].

W celu właściwego wykorzystania komercyjnych możliwości, jakie daje elektroniczna komunikacja za pośrednictwem sieci otwartych, należy stworzyć bezpieczne i wiarygodne środowisko. Współczesne techniki kryptograficzne są powszechnie uznawane za środki, które mogą zagwarantować transakcjom elektronicznym bezpieczeństwo i zaufanie. Dwa podstawowe zastosowania technik kryptograficznych to podpis cyfrowy oraz szyfrowanie. (...) Podpis cyfrowy może pomóc w udowodnieniu autentyczności oraz integralności danych, szyfrowanie może pomóc utrzymać poufność danych, składowanych lub transmitowanych. (...) Komisja uważa, że ważne dla krajów członkowskich jest rozróżnienie między usługami cyfrowego podpisu a usługami szyfrowania, ponieważ różne reguły oraz różne cele oddzielają wspomniane dwa aspekty zastosowania technik kryptograficznych.

Obecnie obserwuje się znaczne przyspieszenie prac nad międzynarodowymi normami dotyczącymi usług opartych na cyfrowym podpisie oraz elektronicznych transakcji i dokumentów. Propozycja dyrektywy Parlamentu Europejskiego i Rady dotyczącej wspólnej

struktury dla podpisu elektronicznego [5] wyznacza datę 1 stycznia 2001 r. jako termin zakończenia prac przygotowawczych w zakresie rozwiązań prawnych, regulacyjnych i administracyjnych związanych z umocowaniem struktur podpisu cyfrowego.

Z uwagi na brak porozumienia międzynarodowego w zakresie stosowania technik kryptograficznych do realizacji usługi poufności i związanej z tym konieczności ustanowienia zasad dostępu uprawnionych instytucji do danych, które zostały zaszyfrowane, usługa poufności została czasowo wyłączona z obszaru zastosowania tych technik do zapewnienia bezpiecznej komunikacji w sieciach komputerowych. Należy dodać, że - z punktu widzenia np. handlu elektronicznego - znacznie ważniejsze są usługi integralności, uwierzytelnienia i niezaprzeczalności, które mogą być realizowane na podstawie przekształcenia kryptograficznego podpisu cyfrowego.

Problem usługi poufności oferowanej przez TTP omówiono w pkt. 9. Natomiast stan prawny w Polsce w zakresie podpisu cyfrowego oraz bezpiecznej komunikacji w sieciach komputerowych opartej na technikach kryptograficznych przedstawiono w pkt. 10.

3. KOMUNIKACJA TTP Z UŻYTKOWNIKAMI

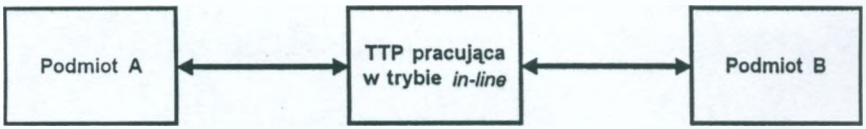
Przed klasyfikacją usług TTP należy określić, w jaki sposób podmioty mogą komunikować się ze swoją zaufaną trzecią stroną. Komunikacja między zaufaną trzecią stroną a podmiotami korzystającymi z jej usług może przebiegać w trzech konfiguracjach pracy: *in-line*, *on-line* i *off-line*.

Każdy z wyżej wymienionych trybów współdziałania w istotny sposób wpływa na rodzaj usług oferowanych przez TTP oraz ich parametry, takie jak: aktualność komunikowania się, odmowa usługi, rejestrowanie poświadczeń (patrz usługa niezaprzeczalności - pkt 4.2), opóźnienie dostarczenia informacji.

Poszczególne usługi TTP będą omówione w dalszej części niniejszego artykułu, z uwzględnieniem cech charakterystycznych, wynikających z trybu współdziałania TTP oraz komunikujących się podmiotów.

3.1. Usługi TTP w trybie *in-line*

Strona TTP pracująca w trybie *in-line* jest ustawiona w torze komunikacyjnym między podmiotami. Taki tryb pracy może być przydatny w sytuacji, gdy komunikujące się ze sobą podmioty należą do różnych domen zabezpieczenia, tzn. nie stosują tej samej polityki zabezpieczenia, tych samych mechanizmów zabezpieczenia itp. (ścisła definicja domeny zabezpieczenia zostanie przytoczona w pkt. 5.2), co powoduje, że nie mogą zrealizować bezpośrednio bezpiecznej wymiany informacji. Tę rolę przejmuje TTP, pośrednicząc w wymianie każdej wiadomości (rys. 4).



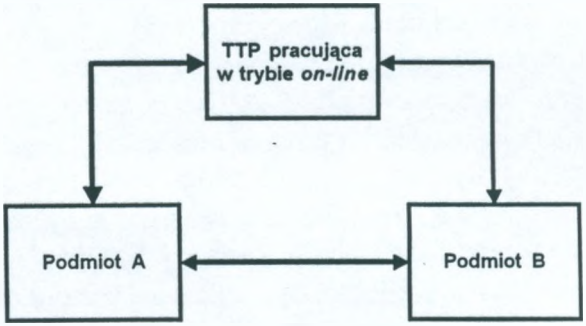
Rys. 4. Praca TTP w trybie *in-line*

TTP pracująca w trybie *in-line* może świadczyć usługi uwierzytelnienia, translacji (np. w procesie dystrybucji kluczy), niezaprzeczalności, kontroli dostępu, integralności i poufności.

3.2. Usługi TTP w trybie *on-line*

Strona TTP uczestniczy we wszystkich fazach chronionej komunikacji, jednakże nie jest ustawiona w torze komunikacyjnym między podmiotami. Na żądanie jednego lub obu podmiotów TTP dostarcza

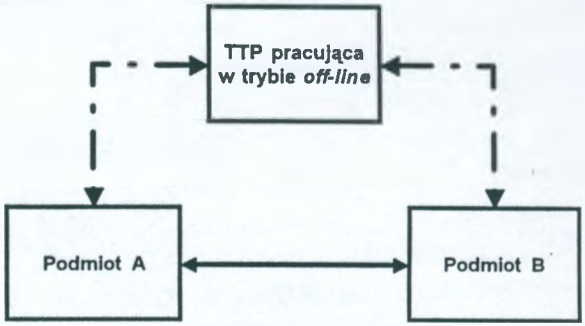
lub rejestruje informacje związane z zabezpieczeniem komunikacji (rys. 5). TTP pracująca w trybie *on-line* może świadczyć usługi uwierzytelnienia, certyfikacji, niezaprzeczalności, kontroli dostępu, oznaczania czasu, integralności i poufności.



Rys. 5. Praca TTP w trybie *on-line*

3.3. Usługi TTP w trybie *off-line*

W tym trybie pracy TTP nie uczestniczy bezpośrednio w procesie komunikowania się podmiotów. Usługi TTP są świadczone w drodze



Rys. 6. Praca TTP w trybie *off-line*

oddzielnej komunikacji (rys. 6). Usługi TTP w trybie *off-line* obejmują uwierzytelnienie, niezaprzeczalność i dystrybucję kluczy.

4. ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Zarządzanie kluczami kryptograficznymi jest jednym z podstawowych aspektów działania zaufanej trzeciej strony. TTP pracująca w trybie *on-line* może działać jako serwer zarządzania kluczami na potrzeby kryptograficznych usług poufności lub integralności (np. na potrzeby kryptograficznej funkcji skrótu). W zależności od sposobu generowania klucza i jego parametrów może to być centrum dystrybucji (klucz jest generowany przez samą TTP) lub translacji (klucz jest generowany przez jeden z podmiotów i transmitowany z jednoczesnym poświadczeniem przez TTP).

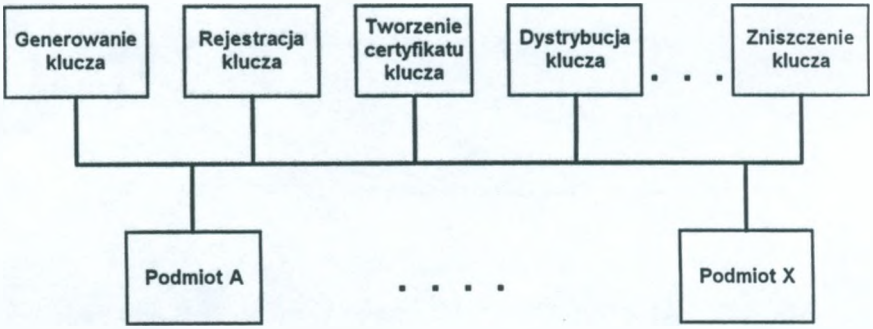
Szczegółowa koncepcja zarządzania kluczami oparta na modelu cyklu życia klucza została przedstawiona, np. w [21]. W niniejszym artykule zaprezentowano jedynie ogólny opis tych usług.

4.1. Usługi zarządzania kluczami

Zarządzanie kluczami opiera się na podstawowych usługach: generacji, rejestracji, certyfikacji, dystrybucji, instalacji, przechowywania, tworzenia kluczy pochodnych, archiwizowania, unieważnienia, usunięcia klucza z rejestru i zniszczenia. Usługi te mogą być częścią systemu zarządzania kluczami lub mogą być dostarczane przez innych dostawców usług. W zależności od rodzaju usługi jej dostawca powinien spełniać określone wymagania w zakresie zabezpieczenia (np. zabezpieczenia wymiany), tak aby być wiarygodnym dla wszystkich zainteresowanych podmiotów.

Na rys. 7 przedstawiono system, w którym wszystkie usługi zarządzania kluczami zostały umieszczone na tym samym poziomie i mogą być użyte przez różne podmioty (osoby lub procesy). Pod-

mioty te mogą wykorzystywać różne usługi zarządzania kluczami w różnych zastosowaniach, zgodnie z własnymi potrzebami.



Rys. 7. Usługi zarządzania kluczami kryptograficznymi

4.1.1. Generowanie klucza

Generowanie klucza jest usługą przywoływaną w celu bezpiecznego tworzenia kluczy dla określonego algorytmu kryptograficznego. Wynika z tego, że proces generowania kluczy nie może ulec manipulacji, a tworzenie kluczy następuje w nieprzewidywalny sposób oraz jest zgodne z założonym rozkładem prawdopodobieństwa. Rozkład jest narzucony przez algorytm kryptograficzny, dla którego klucz jest tworzony, oraz przez wymagany poziom ochrony kryptograficznej. Generowanie niektórych kluczy (np. kluczy master) wymaga specjalnej ostrożności, ponieważ znajomość tych kluczy umożliwia dostęp do wszystkich kluczy związanych lub pochodnych.

4.1.2. Rejestracja klucza

Usługa rejestracji klucza powoduje związanie klucza z podmiotem. Jest realizowana przez organ rejestracji i zwykle znajduje zastoso-

wanie w symetrycznych technikach kryptograficznych. Gdy podmiot chce zarejestrować klucz, powinien skontaktować się z organem rejestracji. Rejestracja klucza obejmuje żądanie rejestracji i potwierdzenie rejestracji. Organ rejestracji prowadzi rejestr kluczy i związanych z nimi informacji, w sposób gwarantujący odpowiedni poziom zabezpieczenia. Organ rejestracji realizuje operacje rejestracji i usunięcia klucza z rejestru.

4.1.3. Tworzenie certyfikatu klucza

Usługa tworzenia certyfikatu klucza zapewnia związanie klucza publicznego z podmiotem i jest realizowana przez organ certyfikacji. Po zaakceptowaniu żądania certyfikacji klucza, organ certyfikacji tworzy certyfikat klucza. Definicję certyfikatu klucza publicznego omówiono w pkt. 2.3, natomiast zarządzanie certyfikatami - w pkt. 5.

4.1.4. Dystrybucja klucza

Usługa dystrybucji klucza jest zbiorem procedur, umożliwiających przekazywanie, w bezpieczny sposób, kluczy oraz informacji z nimi związanych upoważnionym podmiotom. Udział zaufanych trzecich stron w procesie dystrybucji kluczy zostanie przedstawiony w pkt. 4.2. Szczegółowy opis protokołów dystrybucji klucza, w zależności od przyjętej techniki kryptograficznej, wykracza poza zakres niniejszego opracowania. Można je znaleźć np. w [21].

4.1.5. Instalacja klucza

Przed użyciem klucza zawsze jest wymagana usługa instalacji klucza. Instalacja klucza oznacza utworzenie klucza w obrębie zasobów systemu zarządzania kluczami w sposób, który chroni klucz przed naruszeniem zabezpieczenia.

4.1.6. Przechowywanie klucza

Usługa przechowywania klucza zapewnia bezpieczne składowanie kluczy przeznaczonych do aktualnego użytkowania, przewidzianych do użycia w najbliższym czasie lub będących kopiami bezpieczeństwa. Fizyczne odseparowanie zwykle stosowanych urządzeń i nośników, na których są przechowywane klucze, ma wiele zalet. W zależności od znaczenia kluczy, mogą one być chronione z użyciem jednego z następujących mechanizmów:

- fizycznego zabezpieczenia (np. przez przechowywanie kluczy w urządzeniach odpornych na penetrację lub na zewnętrznych nośnikach, takich jak dyskietka lub karta pamięci;
- szyfrowania za pomocą kluczy, które same są chronione z użyciem fizycznych zabezpieczeń;
- ochrony dostępu do kluczy za pomocą haseł lub kodów PIN.

Powinna istnieć możliwość wykrycia każdej próby naruszenia zabezpieczenia materiału kluczowego.

4.1.7. Tworzenie kluczy pochodnych

Usługa tworzenia kluczy pochodnych powoduje powstanie potencjalnie dużej liczby kluczy z użyciem: tajnego klucza początkowego, zwanego kluczem podstawowym, jawnych, zmiennych danych oraz procesu przekształcenia (który niekoniecznie ma być tajny). Wynikiem tego procesu jest klucz pochodny. Klucz podstawowy wymaga specjalnej ochrony. Proces tworzenia kluczy pochodnych powinien być nieodwracalny i nieprzewidywalny, tak aby gwarantować, że naruszenie zabezpieczenia klucza pochodnego nie spowoduje ujawnienia klucza podstawowego lub jakiegokolwiek innego klucza pochodnego.

4.1.8. Archiwizacja klucza

Usługa archiwizacji klucza zapewnia proces bezpiecznego, długoterminowego przechowywania kluczy po okresie ich normalnego użytkowania. Usługa archiwizacji może korzystać z usługi przechowywania danych, ale są dopuszczalne inne implementacje, np. składowanie bez możliwości natychmiastowego dostępu. Odzyskiwanie archiwizowanych kluczy może okazać się potrzebne w przypadku konieczności potwierdzenia lub odrzucenia określonych żądań. Taka sytuacja może zdarzyć się w terminie dużo późniejszym niż termin zaprzestania normalnego użytkowania klucza.

4.1.9. Unieważnienie klucza

Usługa unieważnienia klucza zapewnia bezpieczną deaktywację klucza, którego zabezpieczenie zostało naruszone (lub zachodzi podejrzenie takiego naruszenia). Usługa ta jest potrzebna w przypadku kluczy, których termin ważności wygasł. Unieważnienie klucza jest potrzebne także wtedy, gdy zmieniły się okoliczności dotyczące jego właściciela. Unieważniony klucz może być wykorzystany tylko do odszyfrowania i weryfikacji. Usługa unieważnienia klucza nie jest stosowana w schematach opartych na certyfikacji, ponieważ tam czas życia klucza jest ograniczony terminem wygaśnięcia certyfikatu.

4.1.10. Usunięcie klucza z rejestru

Usługa usunięcia klucza z rejestru jest procedurą wykonywaną przez organ rejestracji. Powoduje ona zerwanie powiązania między kluczem a podmiotem. Usługa ta jest częścią procesu zniszczenia (por. pkt 4.1.11). Gdy podmiot chce usunąć klucz z rejestru, powinien skontaktować się z organem rejestracji.

4.1.11. Zniszczenie klucza

Usługa zniszczenia klucza zapewnia proces bezpiecznego usuwania kluczy, które nie są już dłużej potrzebne. Zniszczenie klucza oznacza likwidację wszystkich zapisów dotyczących informacyjnych obiektów zarządzania kluczami w taki sposób, że żadna informacja, która pozostałaby po zniszczeniu, nie umożliwi odzyskania zniszczonego klucza. Proces ten obejmuje także zniszczenie wszystkich kopii archiwalnych. Jednakże przed zniszczeniem kopii kluczy powinna być przeprowadzona procedura sprawdzająca, czy nie zajdzie potrzeba ponownego użycia któregoś z materiałów archiwalnych chronionych przez te klucze.

4.2. Udział zaufanych trzecich stron w procesie dystrybucji kluczy kryptograficznych

Podstawowym zadaniem TTP jest umożliwienie bezpiecznej komunikacji między podmiotami, które darzą ją zaufaniem. TTP może zatem uczestniczyć w procesie przesyłania certyfikatów lub uzgodnienia kluczy kryptograficznych. Można rozróżnić wtedy dwa przypadki:

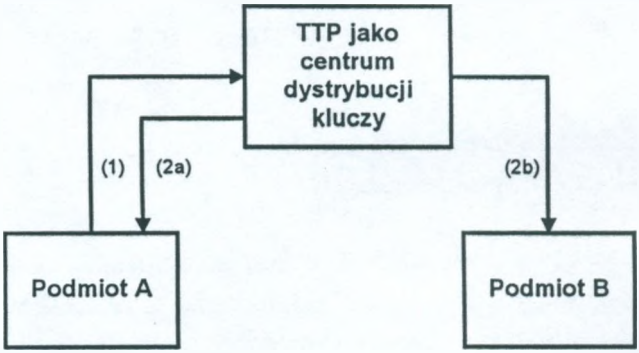
- dwa komunikujące się ze sobą podmioty należą do jednej domeny zabezpieczenia*),
- dwa komunikujące się ze sobą podmioty należą do różnych domen.

Schematy przedstawione na rys. 8 i 9 odnoszą się zarówno do usługi przekazywania tajnych kluczy kryptograficznych, jak i do certyfikatów kluczy publicznych.

---

*) Domena zabezpieczenia - zbiór elementów, polityka zabezpieczenia i zbiór działań związanych z zabezpieczeniem, w których ten zbiór elementów podlega polityce zabezpieczenia, a sama polityka zabezpieczenia jest realizowana przez organ zabezpieczenia [18].

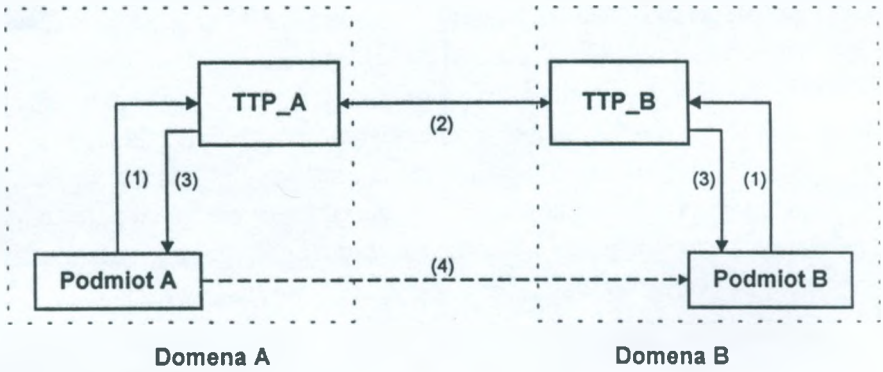
Przypadek gdy dwa komunikujące się ze sobą podmioty mają wspólną zaufaną trzecią stronę, został zilustrowany na rys. 8. W opisywanej sytuacji TTP pełni rolę centrum generowania i dystrybucji kluczy kryptograficznych (np. sesyjnych lub kluczy publicznych w postaci certyfikatów). Centrum może komunikować się w bezpieczny sposób z oboma podmiotami. Jeżeli na żądanie jednego z podmiotów (1) klucz zostanie wygenerowany, to centrum dystrybucji kluczy przejmuje odpowiedzialność za jego bezpieczną dystrybucję do obu podmiotów (2a) i (2b).



Rys. 8. TTP jako centrum dystrybucji kluczy

Drugi przypadek jest bardziej złożony. Zakładamy, że w każdej domenie zabezpieczenia istnieje zaufana trzecia strona: w jednej TTP_A, która jest wiarygodna dla podmiotu A, w drugiej TTP_B, która jest wiarygodna dla podmiotu B. Jeżeli podmioty stosują technikę asymetryczną w celu wymiany informacji, a nie mają dostępu do wspólnej usługi katalogu, który oferuje certyfikaty kluczy publicznych, to każdy z podmiotów kontaktuje się z własną TTP w celu uzyskania certyfikatu klucza publicznego swego partnera - por. rys. 9(1). Organy certyfikacji dla podmiotów A i B wymieniają między sobą certyfikaty kluczy publicznych podmiotów A i B (2),

a następnie przesyłają stosowny certyfikat, każdy do swego podmiotu (3). W efekcie, podmioty A i B mają możliwość wzajemnej weryfikacji za pomocą autentycznego certyfikatu klucza publicznego drugiej strony lub ustanowienia klucza sesyjnego do poufnej komunikacji.



Rys. 9. Dystrybucja kluczy kryptograficznych między dwiema domenami

W przypadku gdy komunikujące się podmioty stosują technikę symetryczną, każdy z nich powinien ponadto skontaktować się ze swoim organem, w bezpieczny sposób (1), aby otrzymać tajny klucz do komunikacji między nim a organem. Organy uzgadniają między sobą klucz tajny (2), który ma być użyty przez oba podmioty. Jeden organ rozsyła klucz do obu podmiotów, wykorzystując drugi organ jako centrum dystrybucji.

W przypadku gdy TTP podmiotów A i B nie mają między sobą ani związku wzajemnej wiarygodności, ani bezpośredniej drogi komunikacji, łańcuch takiej wiarygodności można wyodrębnić na podstawie schematu certyfikacji (hierarchicznej lub wzajemnej - patrz pkt 5).

W niniejszym punkcie przedstawiono ogólną koncepcję dystrybucji kluczy kryptograficznych z udziałem TTP. Proces dystrybucji kluczy jest realizowany za pomocą protokołów. Szczegółowe implementacje procesu dystrybucji kluczy wykraczają poza zakres niniejszego opracowania.

Obecnie toczą się dyskusje, czy do usług zarządzania kluczami można zakwalifikować usługę odtwarzania klucza *(key recovery)*. Jedni twierdzą, że w oczywisty sposób należy ona do tego zbioru, bo dotyczy kluczy kryptograficznych. Inni, do grona których zalicza się także autorka opracowania, wychodzą z klasycznej definicji zarządzania kluczami kryptograficznymi, która opiera się namodelu cyklu życia klucza. W modelu tym nie występuje stan odpowiadający usłudze odtwarzania klucza. Proponują zatem rozważać odtwarzanie klucza jako przypadek wyjątkowy. Zgodnie z tym poglądem, szczegółowe omówienie tego niezwykle ważnego aspektu procesu dystrybucji kluczy kryptograficznych znajdzie się w pkt. 9.

5. ZARZĄDZANIE CERTYFIKATAMI

Aby móc skorzystać z olbrzymiej większości usług oferowanych w bezpiecznej sieci wymagających znajomości publicznego klucza, użytkownik musi otrzymać go w postaci, która gwarantowałaby jego autentyczność. Publiczne klucze są rozpowszechniane w sieci w postaci certyfikatów. Definicję certyfikatu przedstawiono w pkt. 2.3.

Należy podkreślić, że autentyczność certyfikatu publicznego klucza opiera się na przekształceniu kryptograficznym sekwencji danych, które wiąże jednoznacznie klucz publiczny danego użytkownika z innymi informacjami w taki sposób, że sfałszowanie tego certyfikatu jest przekształceniem matematycznym obliczeniowo niewy-

konalnym. Przekształcenie to jest realizowane za pomocą prywatnego klucza organu certyfikacji, certyfikat zatem jest weryfikowany przy użyciu powszechnie dostępnego, publicznego klucza organu certyfikacji.

Administrowanie i świadczenie przez organ certyfikacji (CA) usług, takich jak: generacja certyfikatów z lub bez usługi generacji kluczy, dystrybucja certyfikatów, odnowienie, uaktualnienie i unieważnienie certyfikatów, stwierdzenie ważności (walidacja) certyfikowanego klucza, certyfikacja atrybutów, nosi nazwę **zarządzania certyfikatami**.

5.1. Organ certyfikacji

Organ certyfikacji jest zaufaną trzecią stroną, która realizuje wiele funkcji związanych publicznymi kluczami kryptograficznymi oraz podstawowym zastosowaniem przekształcenia publicznego klucza, jakim jest podpis cyfrowy. Zadaniem organu certyfikacji jest zidentyfikowanie właściciela oraz cech jego publicznego klucza w taki sposób, aby być wiarygodnym dla swoich abonentów. Wiarygodność ta opiera się na użyciu odpowiednich mechanizmów i urządzeń kryptograficznych oraz na profesjonalnym zarządzaniu i procedurach kontrolnych. Wiarygodność ta może być potwierdzona przez niezależną funkcję audytu (wewnętrzną, zewnętrzną lub obu typów), której rezultat jest podawany abonentom do wiadomości.

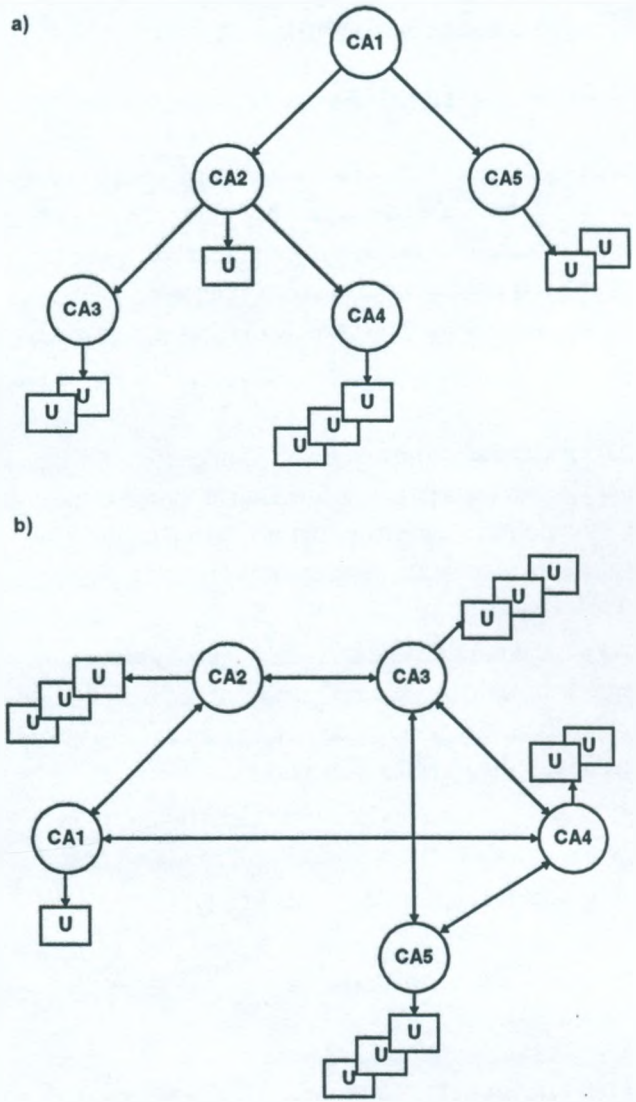
W szczególności organ CA jest odpowiedzialny za niżej podany zakres usług.

1. Identyfikowanie podmiotów, których informacje o kluczu publicznym są przedstawiane do certyfikacji.
2. Zapewnienie jakości pary kluczy asymetrycznych wykorzystywanych do tworzenia certyfikatów kluczy publicznych.

3. Zabezpieczenie procesu certyfikacji oraz klucza prywatnego wykorzystywanego do podpisywania informacji o kluczach publicznych.
4. Zarządzanie danymi systemowymi, które mają być zawarte w informacji o kluczu publicznym, takimi jak: numer seryjny certyfikatu klucza publicznego, identyfikator organu certyfikacji itp.
5. Przyporządkowanie i sprawdzanie terminu ważności.
6. Informowanie podmiotu identyfikowanego w informacji o kluczu publicznym, że certyfikat klucza publicznego został wydany. Sposób przekazywania tej informacji powinien być niezależny od sposobu przekazywania informacji o publicznym kluczu do CA.
7. Zapewnienie, że dwa różne podmioty nie mają przyporządkowanego tego samego identyfikatora, co gwarantuje ich rozróżnialność.
8. Utrzymanie i publikowanie list unieważnionych certyfikatów.
9. Rejestrowanie wszystkich etapów procesu generacji certyfikatów kluczy publicznych.

Jeden organ CA może certyfikować informację o kluczu publicznym innego CA w celu utworzenia certyfikatu klucza publicznego. Na rys. 10 przedstawiono hierarchiczną i wzajemną strukturę ścieżek certyfikacji. Warto zauważyć, że w przypadku hierarchicznej struktury organów certyfikacji uwierzytelnienie może zawierać łańcuch certyfikatów kluczy publicznych. Jednakże, pierwszy certyfikat klucza publicznego w takim łańcuchu powinien być otrzymany i uwierzytelniony za pomocą innych środków niż certyfikaty kluczy publicznych.

Szczegółowe omówienie struktury certyfikatów wydawanych innym organom certyfikującym oraz ograniczenia ścieżki certyfikacji zawarte w samych certyfikatach wykraczają poza zakres niniejszego artykułu. Więcej szczegółów można znaleźć, np. w [24÷27].



Rys. 10. Struktura organów certyfikacji
a) certyfikaty hierarchiczne; b) certyfikaty wzajemne
CA - organ certyfikacji, U - użytkownik

5.2. Usługi zarządzania certyfikatami

5.2.1. Generacja certyfikatów

Proces generacji certyfikatów kluczy publicznych odbywa się przed rozpoczęciem użytkowania pary kluczy asymetrycznych. Usługa generacji certyfikatów może być poprzedzona generacją pary kluczy, która przebiega zgodnie z procesem opisanym w pkt. 4.1.1.

Proces generacji certyfikatów składa się z następujących etapów.

1. Sprawdzenia, czy informacja o kluczu publicznym nie zawiera błędów.
2. Zaakceptowania informacji o publicznym kluczu; wymagania towarzyszące akceptacji informacji o kluczu publicznym są elementem polityki zabezpieczenia organu certyfikacji oraz organizacji samego organu; aspekty te wykraczają poza zakres niniejszego opracowania.
3. Przygotowania i dodania danych wymaganych przez system zarządzania certyfikatami klucza publicznego; opcjonalnie organ certyfikacji CA może generować parę(y) kluczy asymetrycznych przeznaczonych dla określonych podmiotów.
4. Obliczenia podpisu cyfrowego certyfikatu klucza publicznego. Algorytm może też obejmować obliczenie wartości funkcji skrótu.
5. Wprowadzenia zapisu do rejestru audytu.

5.2.2. Odnowienie certyfikatu

Zmiana atrybutów (dodatkowych informacji) zawartych w certyfikacie publicznego klucza, które nie mają znaczenia krytycznego dla ważności samego certyfikatu, np. zmiana nazwy lub miejsca pracy, nie powoduje konieczności powtórzenia całego procesu generacji certyfikatu. Można wygenerować nowy certyfikat z uaktualnionymi

atrybutami, ale zawierający stary publiczny klucz. Oczywiście, stary certyfikat musi zostać unieważniony. Procedura ta ma tę zaletę, że nie zachodzi potrzeba przekazywania podmiotowi nowych wartości kluczy.

5.2.3. Uaktualnienie certyfikatu

Istnieją dwie metody uaktualnienia certyfikatu.

1. W miejsce starego jest wydawany nowy certyfikat; wartość publicznego klucza, który jest przedmiotem certyfikacji, nie zmienia się (jest to procedura odnowienia certyfikatu, opisana w poprzednim punkcie). Metoda ta jest zwykle stosowana, gdy zbliża się koniec terminu ważności certyfikatu. Natomiast, nie należy jej użyć, gdy:
   - został ujawniony prywatny klucz danego podmiotu;
   - algorytm publicznego klucza zastosowany do utworzenia pary kluczy nie gwarantuje bezpieczeństwa podpisów cyfrowych, wygenerowanych za pomocą tej pary kluczy, na nowy okres ważności certyfikatu.
2. Została wygenerowana nowa para kluczy, publiczny klucz wymaga zatem wydania nowego certyfikatu.

Zasady stosowania obu metod uaktualnienia oraz tryb rejestracji powinny być określone w polityce zabezpieczenia organu certyfikacji.

5.2.4. Dystrybucja i przechowywanie certyfikatów

Po wygenerowaniu certyfikatu klucza publicznego nie ma potrzeby podejmowania specjalnych środków w celu zapewnienia jego poufności lub integralności. W celu zapewnienia łatwości dostępu użytkowników, certyfikaty kluczy publicznych mogą być przechowywane w publicznym katalogu. Jest to usługa TTP, opisana w pkt. 8.2.

5.2.5. Unieważnienie certyfikatu

Certyfikaty mogą być unieważnione przez wydający je organ certyfikacji CA przed wygaśnięciem ich terminu ważności. Przyczyn unieważnienia może być wiele, włączając w to wymienione poniżej:
- naruszenie zabezpieczenia klucza prywatnego podmiotu,
- żądanie odwołania certyfikatu złożone przez podmiot,
- zmiana umocowania prawnego podmiotu,
- zakończenie działalności podmiotu,
- błędna identyfikacja podmiotu,
- naruszenie zabezpieczenia klucza prywatnego organu CA,
- zakończenie działalności organu CA.

Przy unieważnieniu certyfikatu należy przeprowadzić procedurę i zapewnić środki komunikacyjne w celu szybkiego odwołania:
- jednego lub wielu certyfikatów kluczy publicznych jednego lub wielu podmiotów;
- zbioru wszystkich certyfikatów kluczy publicznych wydanych przez organ CA na podstawie jednej pary kluczy asymetrycznych, używanej przez CA do podpisywania informacji o kluczach publicznych;
- wszystkich certyfikatów kluczy publicznych wydanych przez organ CA, niezależnie od wykorzystywanych funkcji pary kluczy asymetrycznych.

Dwa ostatnie wymagania umożliwiają unieważnienie certyfikatów kluczy publicznych w przypadku, gdy nastąpiło naruszenie zabezpieczenia klucza prywatnego organu CA (lub zachodzi takie podejrzenie) albo gdy para kluczy asymetrycznych wykorzystywanych do podpisywania certyfikatów kluczy publicznych została zmieniona. Niezależnie od tego, czy certyfikaty publicznych kluczy wygasły, czy zostały unieważnione, kopie starych certyfikatów powinny być przechowywane przez zaufaną trzecią stronę przez czas określony praktyką biznesową i uregulowaniami prawnymi.

W przypadku gdy w wyniku naruszenia zabezpieczenia klucza prywatnego (rzeczywistego lub podejrzewanego) certyfikat klucza publicznego zostanie unieważniony, nie może on już być ponownie wykorzystywany, z wyjątkiem weryfikacji i odszyfrowania. Cały materiał dotyczący klucza zawarty i chroniony przez certyfikat klucza publicznego (bez względu na typ) powinien być wymieniony tak szybko, jak jest to możliwe.

Unieważnienie certyfikatu można zrealizować dwiema metodami.

1. Za pomocą listy unieważnionych certyfikatów

   Lista unieważnień zawiera opatrzoną znacznikami czasowymi listę kolejnych numerów lub identyfikatorów tych certyfikatów kluczy publicznych, które zostały unieważnione przez organ CA. W listach unieważnień są stosowane dwa rodzaje znaczników czasowych:

   - data i czas, kiedy organ CA wydał unieważnienie;
   - data i czas naruszenia zabezpieczenia (rzeczywistego lub podejrzewanego).

   Data wyżej określona, jeśli jest znana, ułatwia przeprowadzenie audytu wiadomości, których dotyczyło naruszenie zabezpieczenia. Certyfikat klucza publicznego pozostaje na liście unieważnień co najmniej do chwili wygaśnięcia jego terminu ważności. Stosowanie znaczników czasowych jest sprawą krytyczną, ponieważ umożliwia oznaczenie momentu, w którym nastąpiło zerwanie związku między kluczem publicznym podmiotu a jego identyfikatorem.

   Od momentu unieważnienia certyfikatu klucza publicznego, na skutek rzeczywistego lub podejrzewanego naruszenia zabezpieczenia, informacja podpisywana odpowiednim kluczem prywatnym nie jest już traktowana jako ważna, jeśli jej podpisanie nastąpiło po podejrzewanej dacie naruszenia lub jeśli nie można w sposób jednoznaczny określić daty podpisu. Informacja nie może być zaszyfrowana z użyciem klucza publicznego, który został unieważniony.

2. Przez wydanie certyfikatu unieważnienia (rzadziej spotykana)

   W rejestrze certyfikatów następuje zamiana certyfikatu publicznego klucza przez certyfikat unieważnienia.

Tryb unieważnienia (natychmiastowe lub wstrzymanie ważności do czasu potwierdzenia przyczyny unieważnienia), metody realizacji unieważnienia, sposób powiadamiania użytkowników o unieważnionych certyfikatach zależy od przyjętej przez organ certyfikacji polityki zabezpieczenia.

5.2.6. Stwierdzenie ważności certyfikatu

Podmiot otrzymujący za pośrednictwem usługi katalogu (lub w inny sposób) certyfikat publicznego klucza musi mieć środki umożliwiające jego weryfikację. Może to zrobić trzema metodami.

1. Jeśli zastosowano metodę publikowania listy unieważnionych certyfikatów - przeszukanie katalogu certyfikatów oraz tej listy. Wadą tej metody jest prawdopodobieństwo istnienia opóźnienia między momentem unieważnieniem a uaktualnieniem listy unieważnionych certyfikatów.
2. Jeśli zastosowano metodę wydawania certyfikatów unieważnień - przeszukanie jedynie katalogu certyfikatów i sprawdzenie w odszukanym rekordzie "wskaźnika unieważnienia". Również w tym przypadku występuje prawdopodobieństwo opóźnienia aktualizacji katalogu.
3. Wystawienie żądania weryfikacji ważności certyfikatu do TTP, pracującego w trybie *on-line*. Metoda ta eliminuje niebezpieczeństwo opóźnienia uaktualnienia baz danych.

5.2.7. Certyfikat atrybutów

Niektóre atrybuty (dodatkowe informacje towarzyszące publicznemu kluczowi) mogą zmieniać się częściej niż inne. Aby uniknąć

konieczności wystawiania nowego certyfikatu, należy dokonać rozdzielenia atrybutów. Do certyfikatu publicznego klucza należy zatem włączyć te atrybuty, które nie zmieniają się często, natomiast dla pozostałych utworzyć oddzielną strukturę danych. Najczęściej stosowanym rozwiązaniem jest certyfikat atrybutów [37]. Certyfikaty atrybutów wystawione dla danego podmiotu są powiązane jednoznacznie z jego certyfikatem publicznego klucza (zawierają wyróżniający identyfikator podmiotu lub numer seryjny certyfikatu publicznego klucza).

Wystawcą certyfikatów atrybutów nie musi być ten sam organ, który wystawia certyfikaty publicznych kluczy. Jednakże, rozdzielenie tych organów ma poważne konsekwencje prawne, organizacyjne i techniczne (np. problem uwierzytelnionej wymiany informacji o powiązaniu certyfikatów, unieważnieniu certyfikatów), które muszą być uwzględnione przy definiowaniu zasad działania i współpracy tych organów.

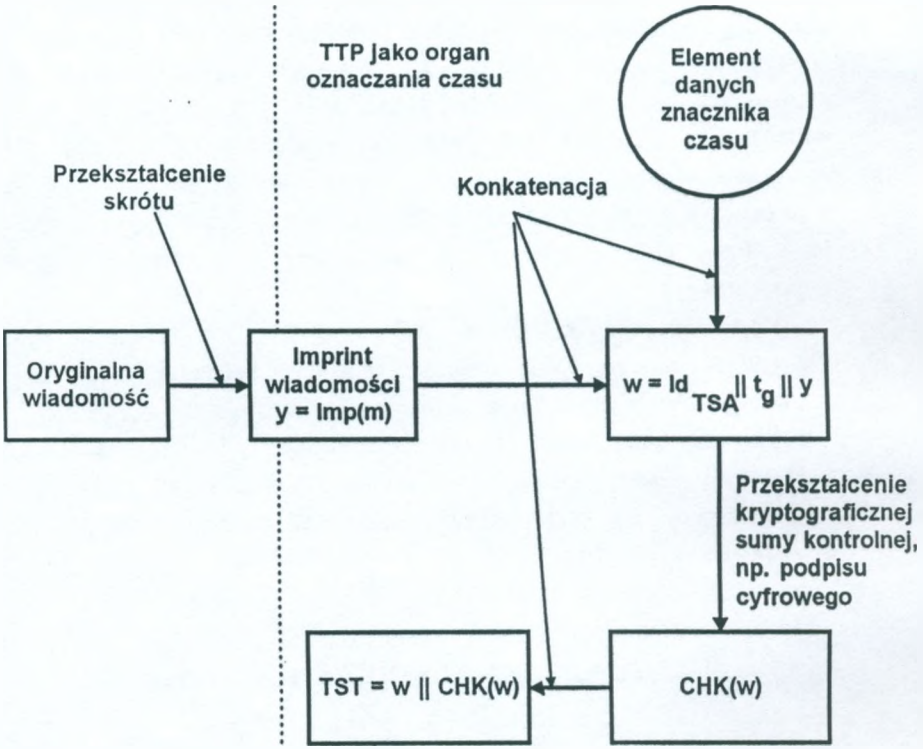
6. PODSTAWOWE USŁUGI TTP - OZNACZANIE CZASU I NIEZAPRZECZALNOŚĆ

Dwie usługi TTP należy zaliczyć do podstawowych, tzn. takich, które najdosłowniej realizują związek zaufania miedzy TTP a jej użytkownikami. Są to usługa oznaczania czasu oraz niezaprzeczalności. Usługi te muszą być włączone w skład innych usług gwarantujących zabezpieczenie komunikujących się między sobą podmiotów, np. zarządzanie certyfikatami czy elektroniczny notariat.

6.1. Usługa oznaczania czasu

6.1.1. Pojęcie znacznika czasu

Większość usług TTP potrzebuje weryfikacji czasu zdarzenia. Usługa dodawania znacznika czasowego polega na zastosowaniu



Rys. 11. Token znacznika czasowego

t_g - dane znacznika czasowego określające moment jego generacji,
Id_{TSA} - identyfikator wyróżniający organu oznaczania czasu,
TST - token znacznika czasowego

kryptograficznego przekształcenia wiążącego elektroniczny dokument z sekwencją danych, określającą moment w odniesieniu do wiarygodnego wzorca czasowego. Zastosowanie znacznika czasowego umożliwia wykrycie próby oszustw, takich jak: podstawienie starej wiadomości oraz wsteczne datowanie. Ponieważ każdy mechanizm oznaczania czasu zależy od autentyczności, wiarygodności i niezawod-

ności stosowanego wzorca czasowego, usługa ta jest często dostarczana przez inną, niezależną zaufaną trzecią stronę.

Metoda tworzenia znacznika czasowego została przedstawiona na rys. 11. W sensie technicznym znacznik przybiera postać tokena*). Szczegółowy opis protokołów dystrybucji znacznika czasowego z zastosowaniem różnych technik kryptograficznych wykracza poza zakres niniejszego opracowania. Można je znaleźć, np. w [28].

6.1.2. Organ oznaczania czasu

Organ oznaczania czasu jest zaufaną trzecią stroną dostarczającą poświadczenia istnienia dokumentu w momencie, w którym został wygenerowany znacznik czasu. Przykładowo, ten znacznik 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. Znacznik czasowy może być również stosowany w usługach elektronicznego notariatu w celu oznaczenia momentu przedłożenia dokumentu. Znacznik czasowy jest niezbędnym elementem rejestrowania elektronicznych transakcji.

Od TTP oznaczającej czas wymaga się, aby:

- weryfikowała tylko znacznik czasowy; nie może ona weryfikować np. danych, które są opatrzone tym znacznikiem;
- po uzyskaniu wiarygodnego żądania, generowała token znacznika czasowego;
- realizowała przekształcenie znacznika czasowego tylko do reprezentacji wiadomości (np. uzyskanej po zastosowaniu funkcji skrótu);

*) Token - sekwencja danych związanych z określoną komunikacją między podmiotami, która zawiera informacje przekształcone przy użyciu technik kryptograficznych [17].

- klucz prywatny TTP oznaczającej czas był wykorzystywany wyłącznie do tego celu.

6.2. Usługi niezaprzeczalności

Celem usług niezaprzeczalności jest dostarczenie weryfikowalnego dowodu pochodzenia, przedłożenia, przekazania i dostarczenia danych lub zarejestrowanego poświadczenia [20, 22]. Zaufane trzecie strony mogą realizować różne usługi niezaprzeczalności, a w poszczególnych fazach powstawania poświadczeń niezaprzeczalności - pełnić różne role.

6.2.1. Rola TTP w procesie generacji poświadczenia

Poświadczenie jest to sekwencja danych, która umożliwia utworzenie dowodu zaistniałego zdarzenia lub działania. Poświadczenie może być zatem użyte w celu rozstrzygnięcia sporu między podmiotami. W pewnym uproszczeniu, w zależności od zastosowanej techniki kryptograficznej, poświadczenie przybiera postać:

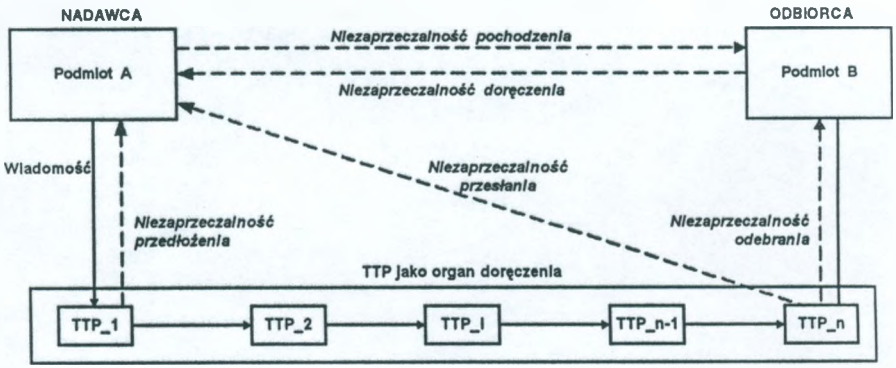
- dla symetrycznych technik kryptograficznych:
  bezpiecznej koperty (*secure envelope*) $SENV_x(y) = y||CHK_x(y)$ (do sekwencji danych y jest dołączana ich kryptograficzna wartość kontrolna $CHK_x(y)$ utworzona w wyniku przekształcenia za pomocą *tajnego* klucza x [16]);
- dla asymetrycznych technik kryptograficznych:
  podpisu cyfrowego $SIG_x(y) = y||CHK_x(y)$ (do sekwencji danych y jest dołączana ich kryptograficzna wartość kontrolna CHKx(y) utworzona w wyniku przekształcenia cyfrowego podpisu realizowanego za pomocą *prywatnego* klucza x [15]).

Zastosowanie bezpiecznej koperty w usługach niezaprzeczalności wymaga zaangażowania TTP, pracującego w trybie *on-line*. Poświad-

czenie utworzone dzięki przekształceniu realizowanym za pomocą tajnego klucza może być utworzone tylko przez TTP.

Gdy poświadczenie jest oparte na przekształceniu podpisu cyfrowego, jest niezbędne zaangażowanie TTP, pracującego w trybie *off-line* - jako organu gwarantującego prawdziwość pary kluczy kryptograficznych.

Na rys. 12 przedstawiono realizację specyficznych usług niezaprzeczalności wymaganych w procesie komunikowania się dwóch podmiotów.



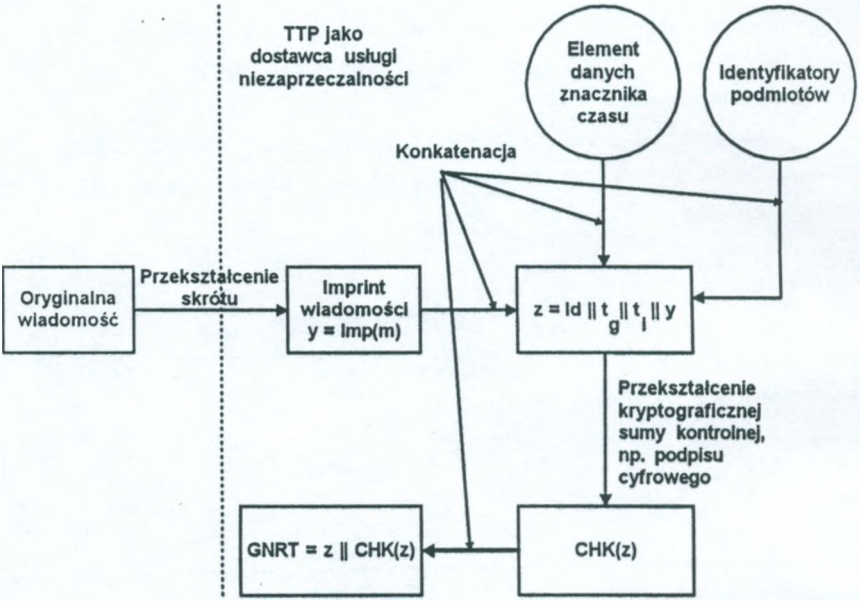
Rys. 12. Rodzaje usług niezaprzeczalności

6.2.2. Rola TTP w kolejnych fazach realizacji usługi niezaprzeczalności

- **Faza generacji poświadczenia**

Na rys. 13 pokazano proces generacji poświadczenia. W sensie technicznym poświadczenie przybiera postać tokena. Dla lepszego zrozumienia, w postaci tokena niezaprzeczalności pominięto część identyfikatorów, które decydują o typie poświadczenia oraz kilka

innych szczegółowych pól, które nie wpływają na charakter jego działania.



Rys. 13. Ogólny token niezaprzeczalności

t_g - dane znacznika czasowego określającego moment generacji poświadczenia, t_i - dane znacznika czasowego określającego moment zdarzenia lub działania, Id - sekwencja identyfikatorów wyróżniających podmiotów, GNRT - ogólny token niezaprzeczalności

W fazie generacji poświadczenia TTP może działać jako:

- organ generacji tokena: TTP tworzy token dowolnego typu na podstawie tokenu otrzymanego od jednego z podmiotów lub innych zaufanych stron trzecich;
- organ oznaczania czasu: TTP tworzy znacznik czasowy określający moment wygenerowania tokena niezaprzeczalności;

- organ notariatu: TTP dostarcza poświadczeń dotyczących właściwości podmiotów uczestniczących w wymianie informacji lub składowanych danych; w szczególności organ notariatu ma uprawnienia do wydłużenia czasu życia danego tokena poza termin ważności;
- organ monitorujący: TTP monitoruje działania i zdarzenia w procesie realizacji usługi niezaprzeczalności oraz tworzy poświadczenia dla tych działań i zdarzeń.

● **Faza przekazania, składowania i odtwarzania poświadczenia**

W tej fazie następuje transfer poświadczeń między podmiotami lub przechowywanych w miejscu składowania poświadczeń. W obu przypadkach TTP może realizować działania tej fazy jako:

- organ dostarczający, pracując w trybie *in-line* dla poświadczenia niezaprzeczalności przedłożenia i niezaprzeczalności przekazania;
- organ składujący rekordy poświadczeń w celu późniejszego wykorzystania.

● **Faza weryfikacji poświadczenia**

TTP jako organ weryfikujący pracuje w trybie *on-line*. Jeśli token został utworzony przy użyciu symetrycznych technik kryptograficznych, udział TTP w procesie weryfikacji jest niezbędny. Gdy do celów niezaprzeczalności wykorzystano przekształcenie podpisu cyfrowego, TTP może:

- zweryfikować podpis cyfrowy, stwierdzając ważność certyfikatu klucza publicznego danego podmiotu i dokonując przekształcenia za pomocą tego klucza;
- w momencie przedstawienia poświadczenia, zweryfikować certyfikat publicznego klucza, który był ważny w momencie generacji poświadczenia (może to nastąpić po latach);

- zweryfikować listy unieważnień certyfikatów publicznych kluczy w celu stwierdzenia, czy są ważne w momencie przedstawienia poświadczenia (może to nastąpić po latach);
- zweryfikować znacznik czasowy w poświadczeniu wygenerowanym przez jeden z podmiotów.

Należy podkreślić, że potrzeba realizacji usługi niezaprzeczalności występuje jedynie w wyjątkowych sytuacjach, tzn. gdy zaistnieje spór między komunikującymi się podmiotami. Konieczność udziału zaufanej trzeciej strony jest w takim przypadku oczywista. Ponieważ gwarancja niezaprzeczalności musi obejmować cały okres ważności informacji, która jest przedmiotem wymiany, TTP powinna zapewnić organizacyjne i techniczne warunki długoterminowego przechowywania poświadczeń, czyli świadczyć usługę elektronicznego notariatu (patrz pkt 7).

7. ELEKTRONICZNY NOTARIAT

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

Przez pojęcie elektronicznego notariatu są rozumiane 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 stwierdzania ważności danych. Proces weryfikacji realizowany przez TTP polega na dodaniu do zarejestrowanego dokumentu dodatkowej informacji weryfikującej.

Przykładowo, TTP działając jako organ notarialny, może dokonać weryfikacji certyfikatu. Organ notarialny weryfikuje ważność przedłożonego certyfikatu. W tym celu sprawdza całą ścieżkę certyfikacji

od podmiotu, który podpisał certyfikat do zaufanego punktu. Organ notarialny może polegać na wszystkich odpowiednich listach unieważnień lub nawiązać w tym celu komunikację z organem certyfikacji. Wynik weryfikacji certyfikatu jest opatrywany znacznikiem czasowym i odsyłany żądającemu weryfikacji w postaci tokenu notariatu.

Od organu notarialnego wymaga się, aby:

- weryfikował poprawność przedłożonego podpisu cyfrowego przy użyciu odpowiedniej informacji o statusie podpisu i certyfikatów publicznych kluczy oraz tworzył podpisany token notarialny poświadczający ważność podpisu;
- weryfikował ważność przedłożonego certyfikatu oraz jego status unieważnienia w określonym momencie przy użyciu odpowiedniej informacji o statusie i certyfikatów publicznych kluczy oraz tworzył podpisany token notarialny poświadczający ważność certyfikatu;
- weryfikował poprawność przedłożonych danych z uwzględnieniem prowadzonej w tym zakresie polityki (tzn. czy stwierdza prawdziwość samych danych, czy legalność przedłożonego kontraktu);
- podpisywał każdy wydany token przy użyciu klucza podpisu stosowanego wyłącznie w tym celu;
- zawarł w tokenie swój wyróżniający identyfikator oraz dane o przedmiocie weryfikacji (certyfikat, cyfrowy podpis, dane).

7.1. Generacja i składowanie poświadczeń

Generacja poświadczeń jest realizacją usługi niezaprzeczalności. Szczegółowe informacje dotyczące roli TTP w procesie generacji poświadczeń podano w pkt. 6.2.1.

Komunikujące się podmioty mogą żądać od TTP nie tylko wygenerowania poświadczenia, ale także jego składowania, a następnie odtworzenia, nieraz po latach. Składowanie poświadczeń jest częścią usługi cyfrowej archiwizacji.

7.2. Usługa cyfrowej archiwizacji

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.

Autentyczność zarejestrowanych dokumentów nie zależy w pierwszym rzędzie od technik kryptograficznych, takich jak podpis cyfrowy, ale raczej od środków fizycznego zabezpieczenia nośników elektronicznych danych.

Długookresowa (wieloletnia) cyfrowa archiwizacja dokumentów, np. danych osobowych lub akt sądowych, wymaga spełnienia następujących warunków technicznych:

- należy regularnie dokonywać odświeżenia nośnika (np. wykorzystywanego w napędach taśmowych);
- w trakcie całego okresu przechowywania danych, do których musi być zapewniony dostęp, może nastąpić konieczność wymiany technicznego wyposażenia zapewniającego ten dostęp; w takiej sytuacji należy wykonać kopie zapasowe archiwizowanych dokumentów, a następnie przenieść dane na nowy nośnik;
- aby móc poprawnie interpretować odzyskiwane dokumenty, należy dołączyć do nich dodatkowe informacje, takie jak: format danych dokumentu (np. ASCII, Postscript, HTML), nazwa pliku i data utworzenia. Należy ponadto zapewnić oprogramowanie obsługujące te formaty danych.

8. INNE USŁUGI TTP

8.1. Identyfikacja i uwierzytelnianie

Uwierzytelnienie za pośrednictwem TTP jest rozwiązaniem przydatnym w środowisku rozproszonym, w którym dany podmiot, pracujący w lokalnej stacji roboczej, chce uzyskać zdalny dostęp do serwera.

Usługa uwierzytelnienia może obejmować uwierzytelnienie podmiotów (użytkowników) lub danych. Szczegółowe informacje o protokołach oraz mechanizmach realizacji usługi uwierzytelnienia można znaleźć w [17, 19]. W większości przypadków należy zapewnić dostępność tej usługi w trybie *on-line*.

8.1.1. Uwierzytelnienie w trybie *on-line*

Gdy zachodzi konieczność uwierzytelnienia podmiotów w sieci liczącej wielu użytkowników, wprowadzenie TTP może znacznie uprościć usługę wzajemnego uwierzytelnienia. W ten sposób następuje znaczne zmniejszenie ilości informacji uwierzytelniającej, koniecznej do przesyłania w sieci. TTP pracująca w trybie *on-line* uczestniczy w każdej operacji uwierzytelnienia.

Mechanizmy uwierzytelnienia wykorzystujące symetryczne techniki kryptograficzne zakładają, że każdy podmiot dzieli tajny klucz z każdym innym podmiotem. W sieci złożonej z n użytkowników wymaga to wygenerowania i rozesłania $n(n\text{-}1)/2$ kluczy. Obecność TTP jako dostawcy usługi uwierzytelnienia redukuje tę liczbę do n tajnych kluczy. W tej konfiguracji każdy z n podmiotów dzieli tajny klucz z TTP.

Usługa uwierzytelnienia może być realizowana w dwóch wariantach:

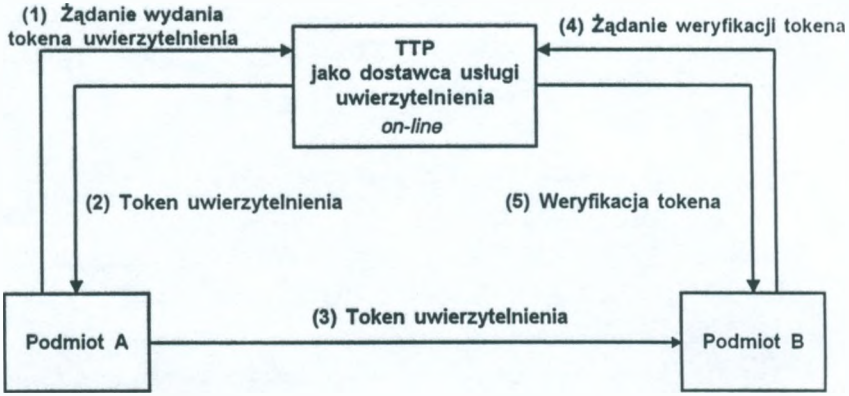
- aby podmiot mógł dokonać samodzielnie uwierzytelnienia, potrzebuje od TTP tokenu uwierzytelnienia [33]; ten token jest następnie wykorzystywany w procedurze uwierzytelnienia, opisanej w dalszej części opracowania;
- podmiot, który chce uwierzytelnić się wobec innego podmiotu, przesyła mu bezpośrednio zapieczętowaną wiadomość; ponieważ podmiot weryfikujący nie ma żadnej możliwości stwierdzenia ważności tej wiadomości (podmioty nie dysponują wspólnym kluczem), zwraca się do TTP, aby w jego imieniu dokonała uwierzytelnienia i powiadomiła go o wyniku swego postępowania.

Usługa uwierzytelnienia z udziałem TTP składa się z dwóch faz:

- fazy wstępnej, w której następuje właściwa identyfikacja podmiotów wobec TTP oraz przekazanie materiału kluczy kryptograficznych;
- fazy właściwego uwierzytelnienia; zakłada się, że podmiot A musi uwierzytelnić się wobec TTP jako lokalnego dostawcy usługi uwierzytelnienia. Po pozytywnym uwierzytelnieniu TTP przekazuje podmiotowi A potrzebne dane uwierzytelniające wobec podmiotu B.

Procedura uwierzytelnienia według wariantu pierwszego przebiega zatem następująco (rys. 14).

1. Podmiot A wysyła do dostawcy usługi (TTP) żądanie danych uwierzytelniających (1) wraz z informacjami, umożliwiającymi jego uwierzytelnienie wobec tego dostawcy (np. hasło, token generowany przy użyciu karty inteligentnej).
2. TTP weryfikuje tożsamość i odsyła podmiotowi A odpowiedni token (2), który umożliwia uwierzytelnienie wobec podmiotu B oraz uzyskanie dostępu do serwera lub aplikacji po stronie podmiotu B. Token ten może zawierać znacznik czasowy, klucz sesyjny, materiał kryptograficzny do celów uwierzytelnienia.
3. Podmiot A przesyła do B otrzymany token (3).



Rys. 14. Procedura uwierzytelnienia z udziałem TTP w trybie *on-line*

4. Podmiot B odsyła tę wiadomość do TTP (4), która dokonuje weryfikacji (za pomocą wspólnego z B klucza, służącego do uwierzytelnienia).
5. Jeśli otrzymany od B token jest taki sam, jak token wygenerowany przez TTP, weryfikacja kończy się powodzeniem (5), a podmiot B udostępnia podmiotowi A zasoby, których ten żąda.
6. Jeśli wymagane jest uwierzytelnienie wzajemne, podmiot B powinien uwierzytelnić się wobec podmiotu A za pomocą identycznej procedury, jak ta opisana w pkt. 1÷5.

8.1.2. Usługa uwierzytelnienia w trybie *off-line*

Usługi uwierzytelnienia *off-line* są oparte na asymetrycznych technikach kryptograficznych w połączeniu z usługami zarządzania certyfikatami (opisanymi w pkt. 5).

TTP, pracująca w trybie *off-line* tworzy i rozprowadza (wcześniej) certyfikaty uwierzytelnienia, które podmiot B może użyć do stwier-

dzenia ważności wymiany danych uwierzytelniających. Certyfikat może być przechowywany przez podmiot B, zostać przesłany przez podmiot A w trakcie procesu uwierzytelnienia lub być pobrany przez podmiot B z publicznego katalogu.

8.1.3. Usługa uwierzytelniania w trybie *in-line*

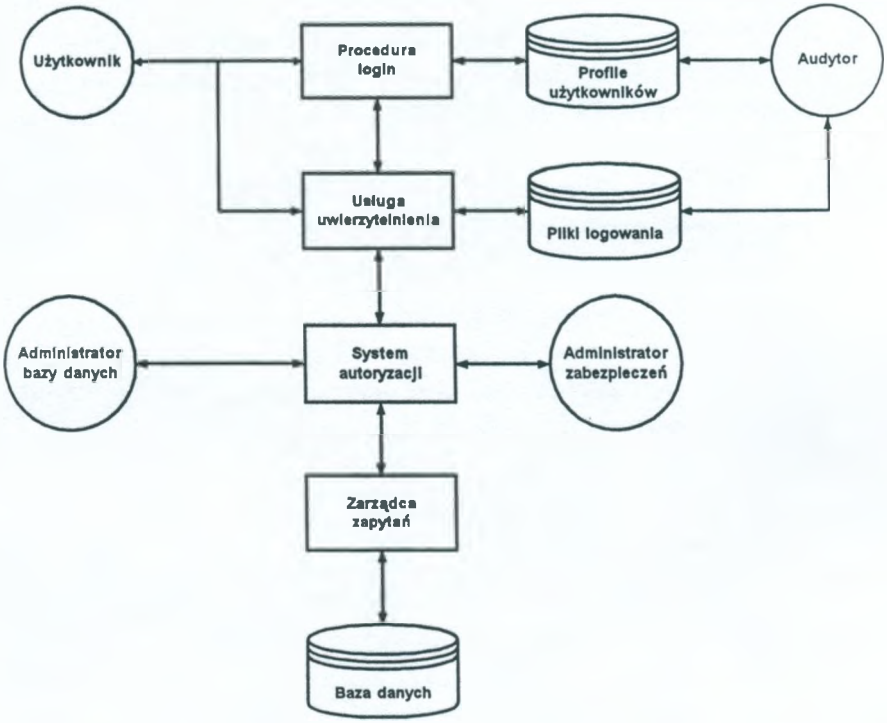
Gdy TTP pracuje w trybie *in-line*, proces uwierzytelnienia składa się z dwóch faz, z których każda zawiera jedną lub więcej wymian informacji. W pierwszej fazie podmiot A uwierzytelnia się wobec TTP. W drugiej fazie (jeśli pierwsza zakończyła się powodzeniem) TTP uwierzytelnia się wobec podmiotu B, gwarantując jednocześnie tożsamość podmiotu A.

8.2. Katalog

Usługi zabezpieczenia komunikacji są oparte na aktualnej i wiarygodnej informacji, np. certyfikatach publicznych kluczy, listach unieważnień certyfikatów, certyfikatach atrybutów, rejestrach elektronicznych transakcji. Informacje te można uzyskać za pomocą usługi katalogu.

Zgodnie z definicją podaną w [14], katalog jest zbiorem otwartych systemów, współpracujących ze sobą w celu utworzenia logicznej bazy danych. Baza danych zawiera obiekty, które są identyfikowane dzięki wyróżniającym identyfikatorom. Działanie usługi katalogu przedstawiono na rys. 15.

Po procedurze rejestrowania i zakończonym sukcesem procesie uwierzytelnienia podmiot jest poddany procedurze autoryzacji, w której są sprawdzane jego prawa dostępu do bazy danych. Podmiot uzyskuje dostęp do katalogu tylko wtedy, gdy zdefiniowane wcześniej prawa dostępu na to zezwalają. W innym przypadku system autoryza-



Rys. 15. Architektura usługi rejestru (katalogu)

cji wysyła komunikat o błędzie dostępu. Wszelkie próby dostępu zakończone niepowodzeniem powinny być odnotowane w pliku rejestru (log).

Zapytania do bazy danych, które uzyskały autoryzację są przetwarzane przez zarządcę zapytań. Zadaniem zarządcy jest odebranie zapytania, przekazanie go do bazy danych oraz odesłanie odpowiedzi do podmiotu, który sformułował zapytanie.

Zarządzanie zabezpieczeniem usługi katalogu realizują trzy podmioty:

- administrator zabezpieczenia, który jest odpowiedzialny za zdefiniowanie zasad autoryzacji, zgodnych z polityką zabezpieczenia; zasady autoryzacji mogą być różne, np. usługa katalogu może być publicznie dostępna lub ograniczona do zamkniętej grupy podmiotów;
- audytor, który okresowo dokonuje przeglądu rejestrów w celu wykrycia naruszeń zabezpieczeń lub nieupoważnionych użytkowników;
- administrator bazy danych, odpowiedzialny za utrzymanie tej części bazy danych, w której jest składowana informacja związana z zabezpieczeniem; podmiot ten ma prawo dostępu do bazy danych w zakresie odczytu, zapisu oraz usunięcia tej informacji z bazy danych.

Informacja z bazy danych może być rozpowszechniana w dwóch trybach dostępu:

- w trybie *off-line*, oznaczającym okresową, automatyczną dystrybucję informacji do abonentów;
- w trybie *on-line*, oznaczającym dystrybucję na żądanie podmiotu (np. katalog zdefiniowany w [14]).

8.3. Personalizacja

Usługa personalizacji obejmuje szyfrowanie materiału kryptograficznego za pomocą tokenów zabezpieczenia, np. kart „elektronicznych". Materiał kryptograficzny zawiera między innymi tajne klucze, publiczne klucze, certyfikaty oraz liczby pseudolosowe. Materiał kryptograficzny musi być zapisywany w urządzeniach odpornych na penetrację, a dostęp do zapisanych danych ma jedynie określony, zidentyfikowany i uwierzytelniony podmiot. Usługa powinna realizować ponadto rejestrację personalnych tokenów oraz autoryzowanych właścicieli danych.

8.4. Alarmowanie

Usługa alarmowania zapewnia podmiotom odpowiednią reakcję na zachodzące zdarzenia związane z naruszeniem zabezpieczeń. Usługa raportowania zdarzeń i zarządzania alarmami może być realizowana w następujący sposób.

1. Jeśli zdarzył się incydent, stosowna informacja jest przekazywana do podmiotu, który jest odpowiedzialny za to zdarzenie lub je wykrył; wcześniej TTP dowiaduje się o incydencie na skutek:
   - otrzymania informacji alarmowej od podmiotów lub
   - automatycznego nadzoru, np. za pomocą śledzenia komunikacji albo uzyskania informacji pośrednio, od innych podmiotów, np. o czasowym braku dostępu.
2. Po incydencie TTP powinna przeprowadzić analizę wpływu zdarzenia na inne, powiązane organizacje, analizy i studia, umożliwiające zapobieżenie podobnym incydentom w przyszłości.

Proces zarządzania informacją alarmową może być realizowany, np. przez przekazanie informacji alarmowej do innych podmiotów lub TTP. Informacja ta może dotyczyć utraty prywatnego klucza organu certyfikacji lub naruszenia zabezpieczenia prywatnego klucza podmiotu.

9. USŁUGA POUFNOŚCI OFEROWANA PRZEZ TTP

Cała gama usług poprzednio opisywana realizowała kryptograficzne usługi uwierzytelnienia, niezaprzeczalności i integralności.

A co z usługą poufności?

Usługi kryptograficzne w swojej istocie kojarzą się z szyfrowaniem. W jaki jednak sposób TTP może zapewnić usługę poufności, będąc dla swoich użytkowników zaufaną trzecią stroną i gwarantując uprawnionym instytucjom dostęp do zaszyfrowanych danych swoich

klientów (realizując jednocześnie zasadę równowagi zdefiniowaną w pkt. 1.2).

Innymi słowy, czy zaufana trzecia strona gwarantująca dostęp uprawnionych instytucji do zaszyfrowanych danych, które są własnością klientów, spełnia warunki definicji zaufania podanej w pkt. 1.3?

Poniżej zostanie przedstawiony osobisty pogląd autorki artykułu na tę kwestię.

9.1. Koncepcja kryptografii kontrolowanej - zarys ogólny

Pokrótce zostaną omówione podstawowe pojęcia z zakresu kryptografii kontrolowanej. Ponieważ jest to zupełnie nowa dziedzina kryptologii, terminy i ich definicje nie są jeszcze ustabilizowane.

Systemy kryptograficzne z możliwością odtwarzania kluczy (*key recovery*) umożliwiają dostęp do tekstu jawnego poza normalnym procesem zaszyfrowania i odszyfrowania. Systemy z odtwarzaniem kluczy zakładają przechowywanie takich kluczy przez podmioty prywatne (zwane nieraz, nieprawidłowo, zaufanymi trzecimi stronami). System kryptograficzny z możliwością odtwarzania kluczy charakteryzują dwie cechy:

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

Ostatnio zaproponowano następujący podział systemów kryptograficznych z odtwarzaniem. Podstawą tej klasyfikacji jest metoda odtwarzania kluczy.

W systemach kryptograficznych z przechowaniem klucza (*key escrow*) kopia tajnego klucza (realizacji usługi poufności) znajduje się w posiadaniu upoważnionej trzeciej strony lub jest podzielona na

dwie albo więcej części, z których każda jest w posiadaniu innego podmiotu. Na żądanie uprawnionej instytucji kopia ta (lub jej część) jest przekazywana tej instytucji.

W systemach kryptograficznych z zapakowanym kluczem (*key encapsulation*) parametry odtwarzania klucza są dołączane do zaszyfrowanych danych. Trzecia strona nie przechowuje klucza lub informacji związanych z kluczem bezpośrednio, ale jest w posiadaniu własnych kluczy, które są stosowane w procesie odtwarzania. Na żądanie uprawnionej instytucji trzecia strona przekazuje te parametry.

9.2. Czy w koncepcji TTP mieści się kryptografia kontrolowana?

Zgodnie z definicją podaną w pkt. 1.3, zaufanie to związek między dwoma podmiotami wyznaczony przez ściśle zdefiniowany zakres działań oraz reguły postępowania określone mianem polityki zabezpieczenia.

W systemach kryptograficznych z odtwarzaniem kluczy definicja zaufania jest inna. Zaufana trzecia strona (TTP) w tym systemie [23] to taka organizacja, która jest obdarzona zaufaniem zarówno przez użytkownika, jak i uprawnioną instytucję! W żadnym razie nie spełnia ona definicji zaufania, w której są dwa, a nie trzy podmioty.

Elektroniczne realizacje funkcji 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. Wszelkie działania w zakresie wdrażania systemów z odtwarzaniem kluczy, obejmujące: porozumienia międzynarodowe, standardy i regulacje, poza ograniczeniami prawnymi, muszą brać pod uwagę także ograniczenia organizacyjne, techniczne i finansowe.

10. UTWORZENIE TTP W POLSCE

10.1. Stan polskiego prawodawstwa

Stan polskiego prawodawstwa nie umożliwia w chwili obecnej jakiekolwiek osadzenia TTP w strukturze prawnej. Brakuje aktów prawnych podstawowego znaczenia. Do nich należy zaliczyć w pierwszym rzędzie uregulowania prawne dotyczące:

- równouprawnienia transakcji elektronicznych i tradycyjnych na podstawie odpowiednich konstrukcji prawnych dotyczących podpisu cyfrowego;
- uprawnionego przechwytywania ruchu telekomunikacyjnego i zasad legalnego dostępu do przechowywanych danych (np. szyfrowanych);
- tajemnicy państwowej i służbowej;

- przestępstw popełnianych za pośrednictwem sieci komputerowych;
- zasad ewentualnego licencjonowania TTP.

Pewne elementy struktury prawnej, określającej podstawy funkcjonowania TTP, jednak już istnieją. Jest to ustawa o ochronie praw autorskich i praw pokrewnych [35], ustawa o ochronie danych osobowych [36] oraz zmiany w kodeksie karnym dotyczące przestępstw popełnionych z użyciem komputera [38]. Są to akty prawne uchwalone bardzo niedawno. Poza ustawą o ochronie praw autorskich, dopiero co weszły w życie: ustawa o ochronie danych osobowych z dniem 30 kwietnia 1998 roku, zmiany w prawie karnym - 1 września 1998 roku. W opinii autorki artykułu zmiany w prawie karnym są niewystarczające, nie da się bowiem efektywnie ścigać przestępstw z użyciem komputera bez odpowiednich porozumień międzynarodowych. Przestępstwa dokonane za pośrednictwem sieci komputerowych mają, z natury swojej, charakter globalny i trudno jest je ścigać, opierając się tylko na prawie karnym (z artykułów o kradzieży i niszczeniu mienia).

Należy stwierdzić, że faza rozwoju komunikacji elektronicznej w Polsce nie umożliwia jeszcze odpowiedniego osadzenia TTP w rzeczywistości społecznej, prawnej i ekonomicznej. W chwili obecnej nie istnieją jeszcze podstawy prawne w postaci porozumień międzynarodowych oraz standardów dotyczących struktury TTP na poziomie ponadnarodowym oraz oferowanych przez nią usług. Jednakże z tempa i rodzaju prac podejmowanych przez organizacje standaryzujące oraz rządy niektórych krajów, a także Unię Europejską, wynika, że w najbliższym czasie pojawią się dojrzałe, kompleksowe propozycje w tym zakresie.

10.2. Kto może pełnić rolę TTP?

W przededniu rewolucji, której rezultatem będzie powstanie społeczeństwa informacyjnego, należy pilnie poszukiwać metod zapewnie-

nia powszechnego dostępu do sieci komputerowych i zasobów informacyjnych. Intencją autorki artykułu było pokazanie, w jaki sposób tworzyć usługi, które w bezpieczny sposób zrealizują elektroniczny model zaufania w wielu aspektach codziennej działalności: prawnej, społecznej i ekonomicznej. W wielu przypadkach udział strony trzeciej upraszcza uciążliwe procedury i podnosi efektywność działań. Przykładowo, jeśli użytkownik sieci komputerowej pragnie sprawdzić ważność dokumentu, dla którego podpis cyfrowy utworzono za pomocą prywatnego klucza, to musi dokonać sprawdzenia certyfikatu publicznego klucza. Publiczny klucz umożliwi mu weryfikację podpisu cyfrowego. Jeśli rzecz dotyczy dokumentu sprzed lat, to sprawdzenie musi objąć archiwizowane listy certyfikatów oraz listy unieważnionych certyfikatów. Zadanie to może wykonać zaufana trzecia strona. TTP sprawdzi ścieżkę certyfikacji od najwyższego poziomu aż do punktu, który cieszy się jego zaufaniem, dokona przeglądu list unieważnionych certyfikatów oraz certyfikatów, których termin ważności upłynął. O wyniku poszukiwań powiadomi zainteresowanego użytkownika. W ten sposób zostanie zrealizowany związek zaufania między podmiotem a TTP.

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

- mieć możliwości techniczne,
- być wiarygodną.

Na całym świecie poszukuje się takich instytucji. W sposób naturalny wybór w wielu krajach pada na pocztę. Poczta od stuleci pełni podobną rolę w świecie usług tradycyjnych, wymagających zaufania miedzy komunikującymi się podmiotami. Na przyklad 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 zeszłym 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. Do roli tej aspirują banki, notariaty oraz operatorzy telekomunikacyjni. Na pewno banki oraz operatorzy telekomunikacyjni mają możliwości techniczne, ale brakuje im wiarygodności.

Organizacja usług TTP to problem bardzo skomplikowany. Należy jednakże podkreślić, że w zakresie każdej z omówionych w punktach 4÷9 usług potrzebna jest zaufana trzecia strona. Usługi te mogą być zatem świadczone przez instytucje w różnym zakresie. Można, tak jak poczta amerykańska, oferować na początku tylko kilka z nich.

10.3. Jak rozpocząć prace nad TTP w Polsce?

Rozpoczynając prace nad TTP w Polsce należy rozpatrzyć niżej podane kwestie.

1. Problem TTP w Polsce to w pierwszym rzędzie **problem prawny**. Jak wspomniano wcześniej (pkt 10.1), nie istnieją w naszym kraju podstawy prawne, umożliwiające upowszechnienie form elektronicznych transakcji, obiegu dokumentów, płatności. Bez podjęcia pilnych kroków w tym zakresie będzie niezwykle trudno dołączyć się do ogólnoeuropejskiej struktury TTP, oferującej usługi uwierzytelnienia i integralności.
2. W opinii autorki artykułu, będącej ekspertem ISO, pracującym nad zagadnieniami związanymi ze standaryzacją usług TTP, **większość norm** znajduje się na etapie wstępnych uzgodnień i upłynie jeszcze trochę czasu, zanim uzyskają swą dojrzałą postać. Natomiast prace nad niektórymi problemami szczegółowymi (np. struktura organów certyfikacji) są prowadzone bardzo intensywnie.
3. Znaleźć w Polsce instytucję, która byłaby zdolna pełnić rolę TTP, jest chyba jeszcze trudniej, niż gdzie indziej. Wydaje się, że Poczta Polska nie ma możliwości technicznych i organizacyjnych

niezbędnych do przedsięwzięć tego typu. Prace związane z tworzeniem **struktury certyfikacji publicznych kluczy** prowadzi kilka instytucji, m.in.: Krajowa Izba Rozliczeniowa, kilka banków, Urząd Ochrony Państwa, NASK. Jednakże banki nie są zainteresowane świadczeniem usług powszechnych, ich zainteresowanie koncentruje się na własnych klientach. Inne instytucje nie spełniają drugiego podstawowego kryterium: wiarygodności.

4. **Instytut Łączności, jako instytucja niezależna, o statusie jednostki naukowo-badawczej mógłby stać się nie tylko ośrodkiem propagującym idee społeczeństwa informacyjnego, ale także realizującym jeden z jej przejawów - instytucję zaufanej trzeciej strony.**

WYKAZ LITERATURY

1. Andrukiewicz E.: Zarządzanie zabezpieczeniem systemu informatycznego. Prace IŁ, nr 108, 1997.
2. Cameron D.: Security Issues for the Internet and the World Wide Web. Computer Technology Research Corp., Charleston, USA, 1997.
3. Clark A.: Cryptographic Controls - The Eternal Triangle. Computers and Security, Vol. 15, No. 7, 1997.
4. Com(97) 503: Ensuring Security and Trust in Electronic Communication Towards a European Framework for Digital Signatures and Encryption.
5. Com(98)297 final: Proposal for a European Parliament and Council Directive on a common framework for electronic signatures.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the processing of personal data, and on the free movement of such data.
7. European Ministerial Conference, Bonn 6-8.07.97, http://www2.echo.ln/bonn/final.html
8. Federal Act Establishing the General Conditions for Information and Communication Services - Information and Communication Services Act (Informations- und Kommunikationsdienste-Gesetz - IuKDG), 1 August, 1997, http://www.iid.de/rahmen/iukdgebt.html

9. Hill R., Walden I.: The Draft UNCITRAL Model Law for electronic commerce: issues and solutions, http://www.batnet.com/modellaw.html
10. http://ideath.parrhesia.com/wassenaar/wassenaar.html
11. Information Week 10/96.
12. 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).
13. ISO/IEC 8824-1:1994 Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.
14. ISO/IEC 9594-1:1993 Information technology - Open Systems Interconnection - The Directory - Overview of concepts, models and services.
15. ISO/IEC 9796:1997 Information technology - Security techniques - Digital signature giving message recovery (wszystkie części).
16. ISO/IEC 9797:1994 Information technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm.
17. ISO/IEC 9798:1995 Information technology - Security techniques - Entity Authentication Mechanisms (wszystkie części).
18. ISO/IEC 10181-1:1995 Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 1: Security Frameworks Overview.
19. ISO/IEC 10181-2:1995 Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 2: Authentication.
20. ISO/IEC 10181-4:1996 Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 4: Non-Repudiation.
21. ISO/IEC 11770:1997 Information technology - Security services - Key management (wszystkie części - polskie tłumaczenie międzynarodowej normy przygotowywane przez NKP nr 182).
22. ISO/IEC 13888:1997 Information technology - Security services - Non-repudiation - Part 1: General Model, 1997 (polskie tłumaczenie międzynarodowej normy przygotowywane przez NKP nr 182).

23. Licencing of Trusted Third Parties for the provision of encryption services - Public Consultation Paper, http://www.dti/gov.uk/pubsl.
24. PKI Part I: Internet Public Key Infrastructure: Part I: X.509 Certificate and CRL Profile, Internet Draft, 1997 (work in progress) /Housley R., Ford W., Solo D./.
25. PKI Part II: Internet Public Key Infrastructure: Part II: Operational Protocols, Internet Draft, March 1997 /Boeyen S., Housley R., Howes T., Myers M., Richard P./.
26. PKI Part III: Internet Public Key Infrastructure: Part III: Certificate Management Protocols, Internet Draft, June 1997 /Farrell S., Adams C., Ford W./.
27. PKI Part IV: Internet Public Key Infrastructure: Part IV: Certificate Policy and Certification Practice Framework, Internet Draft, March 1997 /Chokhani S., Ford W./.
28. PKI Part V: Internet Public Key Infrastructure: Part V: Time Stamp Protocols, Internet Draft, July 1997 /Adams C., Cain P., Pinkas D., Zuccherato R./.
29. Pn-2000: 1997 Przetwarzanie informacji - Zabezpieczenia w systemach informatycznych - Terminologia.
30. Recomendation of the Council concerning guidelines for cryptography policy, 27 March 1997, http://www.oecd.org/dsti/iccp/cryptoe.html
31. Recommendation of the Council concerning guidelines for the security of information systems, 26 November 1992.
32. Reid J.: Plugging the holes in Host-based applications. Computers & Security, Vol. 15, No. 8, August 1996.
33. RFC 1510: The Kerberos Network Authentication Services. IETF, September 1993.
34. UNCITRAL: Draft Uniform rules on electronic signatures.
35. Ustawa z dn. 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. Dz. U. z 1994 r., nr 24, poz. 83.
36. Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. z 1997 r., nr 133, poz. 883.
37. X509v3: ITU-T Draft Recommendation X.509: The Directory - Authentication Framework, 1997.
38. Ziółkowska M.: Ochrona informacji i systemów komputerowych w nowym prawie karnym. Netforum, nr 1, 1998.

Эльжбета Андрукевич

ДОВЕРЕННАЯ ТРЕТЬЯ СТАРОНА (TTP), ПРЕДОСТАВЛЯЮЩАЯ УСЛУГИ БЕЗОПАСНОЙ КОММУНИКАЦИИ В ЭПОХУ ИНФОРМАТИЧЕСКОГО ОБЩЕСТВА – ЮРИДИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ ВОПРОСЫ

Р е з ю м е

Представлено концепцию доверенной - третьей стороны (TTP) организации гарантирующей безопасность коммуникации в глобальных компютерных сетях при использовании методов и средств криптографии. Рассмотрено юридические основы создания в Европе организаций етого типа, проблеммы организации и вопросы защиты этих организаций. Описано услуги TTP основанные на преобразовании цифровой подписи и проверки этой подписи. Подчеркнуто что к основным видам услуг TTP относятся управление криптографическими ключами, управление сертификатами, услуга определения времени, услуга неоспоримости, электронный нотариат. Дается также анализ состояния польской юрисдикции в области услуг связанных с электронной распиской. Обращается внимание на трудности выбора организации выполняющей роль TTP в Польше.

Elżbieta Andrukiewicz

TRUSTED THIRD PARTY (TTP) OFFERING SECURE COMMUNICATIONS SERVICES IN THE AGE OF INFORMATION SOCIETY - LEGAL, ORGANIZATIONAL AND TECHNICAL ISSUES

S u m m a r y

The concept of trusted third party - an organization ensuring communications security in global computer networks by means of cryptographic

tools and methods is presented in the article. Legal framework for such organizations in Europe as well as organizational and security issues are discussed. TTP services based on two cryptographic transformations: signature and verification are presented. TTP services include: cryptographic key management, certificate management, time stamping service, non-repudiation service, electronic notary. Finally, the current stage of legal framework of digital signature's services in Poland is presented. The problem of choosing the right organization which could act as TTP in our country is also discussed.

Elżbieta Andrukiewicz

UN TIERS DE CONFIDENCE (TTP) QUI OFFRE LES SERVICES DE COMMUNICATION DE SECURITE DANS LE TEMPS DE LA SOCIETE D'INFORMATION: LES CONDITIONS JURIDIQUES, D'ORGANISATION ET DE TECHNIQUE

Résumé

Une conception d'un tiers de confidence est présentée comme une institution se portent garant d'une sécurité dans les réseaux globaux d'informatique à l'aide de méthodes et des outils de cryptographie. Les résolutions juridiques de base, les problèmes d'organisation ainsi que les problèmes de la protection des institutions TTP-eux mème sont discutés. Les services de TTP basés sur la transformation de la signature numérique et sur sa verification sont présentées aussi. Il est souligné que les services de base du TTP sont suivants: gestion de cles cryptographiques, gestion des certificats, service d'indication de temps, le service d'incontestabilité, le notariat électronique. Une analyse de l'état de la legislation polonaise est faite aussi dans le sujet de services liés á la signature électronique. On a indiqué sur les problèmes dus au choix en Pologne d'une institution qui executerait un role du TTP.

Elżbieta Andrukiewicz

TRUSTED THIRD PARTY (TTP) BIETET SICHERE KOMMUNIKATIONSDIENSTE IN ÄRA DER INFORMATIONSGESELLSCHAFT AN - JURISTISCHE, ORGANISATORISCHE UND TECHNISCHE ASPEKTE

Z u s a m m e n f a s s u n g

Vorgestellt wird das Konzept von Trusted Third Party, der die Kommunikationssicherheit in globalen Computernetzen mit kryptografischen Verfahren und Mitteln gewährleisteten Organisation. Gesetzrahmen für solche Organisation in Europa wie auch organisatorische und Sicherheit betreffende Lösungen werden behandelt. Es werden TTP-Dienste präsentiert, die auf zwei kryptografischen Transformationen basieren: Signatur und ihre Verifikation. TTP-Dienste umfassen: Kryptografieschlüsselmanagement, Certyfikatemanagement, Zeitstempeldienst, Nichtabstreitbarkeitdienst und Elektronischer Notariat. Herkömlicher Gesetzrahmen von Digitalsignaturedienst in Polen rundet den Beitrag ab. Diskutiert wird auch Problem der Wahl der richtigen Organisation, die Role der TTP in Polen spielen könnte.

Marian Marciniak

621.391.63:666.189.2

BPM ANALYSIS OF A PLANAR OPTICAL WAVEGUIDE WITH GAIN AND LOSSY LAYER

Light propagation in an optical waveguide with a balance of gain and loss has been studied for the first time with beam-propagation method (BPM). In the paper the results are reported and compared with semianalytic and numerical solutions to the wave equation.

1. MOTIVATION

With the advent of semiconductor optical amplifiers a growing interest in optical waveguides composed of active (with gain) and lossy media appears. Although the theoretical background of modes in waveguides with complex refractive indices was well established almost twenty five years ago [13], the diversity of appearing structures involves a considerable and growing effort in studying optical phenomena in those devices, stimulated by availability of technology of such devices and also their potential use for optical signal processing in fiber-based telecommunication systems.

The problem of light propagation in a planar waveguide with a balance of gain and loss of a geometry as in fig. 1 has been proposed by one of the participants to COST 240 project "Techniques for Modelling and Measuring Advanced Photonic Telecommunication Components", Working Group 2, "Waveguides" [8], and formerly has been analyzed with the eigenmode formalism through the use of programs resolving numerically wave equation like Mode Solver. Then the interest of the Working Group 2 has been shifted to BPM

studies of the problem starting with the results of BPM simulation of the structure by the author of this paper [5].

In general guided modes of the structure do not cover the whole spectrum of an incident beam, and the remaining radiation part of the spectrum may be amplified in the guide, in contrast to passive waveguides where radiation field is radiated away from the guide. Therefore BPM which is a nonmodal method can serve very well for the purpose of modeling phenomena of light propagation in such waveguides. A BPM benchmark test for waveguide problem with a balance between loss and gain has been proposed [11] and its results are reported in the present paper.

2. LIGHT PROPAGATION IN A WAVEGUIDE WITH GAIN AND LOSS

The waveguide structure of interest is shown in fig. 1: two layers with mutually complex conjugate refractive indices are surrounded with a medium of a slightly lower real refractive index. The exact values of all parameters are given in fig. 1. The imaginary parts of refractive indices of guiding layers vary in a very broad range: in terms of the power absorption (gain) coefficient α, between zero and $\pm 10^4$ cm^{-1}. The wavelength $\lambda = 1.55$ μm is assumed.

Fig. 1. The geometry of a two-layer waveguide with gain and loss analysed in the paper

2.1. Theory and notation

The attenuation or amplification of light propagating in a transparent medium may be accounted for via a complex-valued refractive index:

$$n = n' - in'' \tag{1}$$

and a complex relative permettivity

$$\varepsilon = n^2 = \varepsilon' - i\varepsilon''. \tag{2}$$

The relation between the power absorption (gain) coefficient α and the imaginary part of refractive index is:

$$n'' = \frac{\alpha\lambda}{4\pi} \cdot 10^{-4}, \tag{3}$$

where α is in cm^{-1} and λ is in μm.

A time-space dependence of the form of $\exp(i\omega t - ikr)$ is assumed throughout the paper. Therefore, for a propagation in the direction of increasing r, gain is equivalent to negative value of n'', while loss is represented by its positive value.

Formally, the modal formalism of waveguides with complex refractive indices is similar to that of guides with real refractive indices. Let us assume a geometry of the waveguide as in fig. 1, where there is no change in the refractive index in the y direction. We consider optical fields that are independent of the y-coordinate.

The fields satisfy in the ith layer a scalar wave equation [7]:

$$\nabla^2\varphi_i + k_i^2\varphi_i = 0, \tag{4}$$

where $\varphi_i = E_y/H_y$ for TE/TM wave, respectively, and $k_i = k_0 n_i$ ($k_0 = 2\pi/\lambda$) is the wavenumber in the layer. The upper infinite layer will be labeled as the 1st, while the lower infinite layer as the 4th.

We consider solutions to (1) in a form of eigenmodes:

$$\varphi_i(x,z) = \phi_i(x)\exp(-ik_z z). \tag{5}$$

The eigenmodes of the form (5) differ from well-known modes of non-lossy guides in a way that the propagation constant is complex:

$$k_z = k_0[\mathrm{Re}(n_{eff}) + i\mathrm{Im}(n_{eff})]. \tag{6}$$

A substitution of (5) into (4) leads to the Helmholtz equation:

$$\frac{d^2\phi_i}{dx^2} + k_{x_i}^2\phi_i = 0, \tag{7}$$

where

$$k_z^2 + k_{x_i}^2 = k_i^2, \tag{8}$$

$$k_{x_i} = u_i - iv_i, \tag{9}$$

k_{xi} is a x - component of the wavevector in the ith layer, u_i and v_i are the transversal phase and attenuation constant, respectively. It follows from (8) that k_{xi} may have two opposite complex values, in the following we choose k_{xi} such that $v_i > 0$.

The modal fields have to satisfy boundary conditions at the interfaces between the ith and jth layers:

$$\left.\begin{aligned} \phi_i &= \phi_j \\ \phi_i' &= w_{ij}\phi_j' \end{aligned}\right\} \tag{10}$$

where the prime denotes a derivative with respect to x, and

$$w_{ij} = \begin{cases} 1 \text{ for TE wave} \\ (n_i/n_j)^2 \text{ for TM wave}. \end{cases} \tag{11}$$

The general solution to (7) is:

for $k_{xi} \neq 0$

$$\phi_i(x) = A_i \exp\left(-ik_{x_i}x\right) + B_i \exp\left(ik_{x_i}x\right), \tag{12}$$

for $k_{xi} = 0$

$$\phi_i(x) = C_i x + D_i , \tag{13}$$

where A_i, B_i, C_i, D_i are complex constants, they must ensure a fulfillment of the boundary conditions (10). For the purpose of numerical calculations it is important to include the linear solution to the wave equation (13) especially in the case of multilayer waveguides, in order to avoid numerical instabilities.

The field limitation condition (at the infinity) requires that in the outermost layers:

$$A_1 = B_4 = 0 , \tag{14}$$

provided that that $\nu_1 > 0$ and $\nu_4 < 0$ have been chosen in (9).

The fields (12)-(13) that satisfy both the limiting conditions (14) and boundary conditions (10) constitute a discrete set of bounded eigenmodes of the structure.

2.2. Numerical solution to the gain-loss waveguide for TE modes

For TE polarized modes ϕ represents the only component of electric field, $\phi = E$. It follows from (12) that the electric field distribution of a guided mode in the waveguide may be expressed in the form:

$$\begin{aligned}
x \le -d: &\quad E = A \exp\left[k\gamma_S(x+d)\right], \\
-d < x \le 0: &\quad E = B_1 \cos k\gamma_L x + B_2 \sin k\gamma_L x , \\
x > d: &\quad E = D \exp\left[-k\gamma_S(x+d)\right], \\
0 < x \le d: &\quad E = C_1 \cos k\gamma_G x + C_2 \sin k\gamma_G x ,
\end{aligned} \tag{15}$$

where

$$\gamma_S = \sqrt{\varepsilon_{eff} - \varepsilon_S}, \quad \gamma_L = \sqrt{\varepsilon_L - \varepsilon_{eff}}, \quad \gamma_G = \sqrt{\varepsilon_G - \varepsilon_{eff}},$$

$$\varepsilon_L = (n + in'')^2, \quad \varepsilon_G = \varepsilon_L^*, \quad \varepsilon_{eff} = N_{eff}^2,$$

$k = (2\pi)/\lambda$, ε_G and ε_L refer to the dielectric permettivity in the gain and lossy region, respectively, and the sign of N_{eff} is chosen so that $\mathrm{Re}\{N_{eff}\} > 0$.

The conditions of continuity of the field E and its derivative at boundaries $x = 0$ and $x = \pm d$ give a set of homogeneous linear equations for unknown amplitudes A, B_1, B_2, C_1, C_2, D. To get a non-trivial solution, the determinant of this set of equations must be equal to zero. It leads to another form of the dispersion equation:

$$\Phi(\varepsilon_{eff}, \alpha) =$$

$$= \gamma_G(\gamma_S \cos k\gamma_G d - \gamma_G \sin k\gamma_G d)(\gamma_S \sin k\gamma_L d + \gamma_L \cos k\gamma_L d) +$$

$$+ \gamma_L(\gamma_S \cos k\gamma_L d - \gamma_L \sin k\gamma_L d)(\gamma_S \sin k\gamma_G d + \gamma_G \cos k\gamma_G d) = 0 \tag{16}$$

Having this equation numerically solved, the field amplitudes A, B_1, B_2, C_1, C_2, D can be calculated, and the field distribution is then explicitly given by (15).

Dispersion equation of the type (16) was numerically solved in the complex ε_{eff} plane by the Newton method, taking into account the analyticity of the function $\Phi(\varepsilon_{eff}, \alpha)$ as a function of ε_{eff} in the region of interest. The calculated dependencies of real and imaginary parts of effective refractive indices versus the absorption coefficient α are plotted in fig. 2.

The dispersion curves from fig. 2 have a particular behavior at $\alpha_1 = 2725{,}67\ \mathrm{cm}^{-1}$, where a second order mode appears, and $\alpha_{branch} = 5226.3023\ \mathrm{cm}^{-1}$, which is a branching point for both $\mathrm{Re}\{N_{eff}\}$ and $\mathrm{Im}\{N_{eff}\}$ curves. For values of $\alpha < \alpha_1$ the waveguide is *single-*

mode, and since the imaginary part of refractive index is equal to zero, the mode propagates without loss or gain. In the interval $\alpha_1 < \alpha \leq \alpha_{branch}$, the waveguide supports two complex but *lossless*

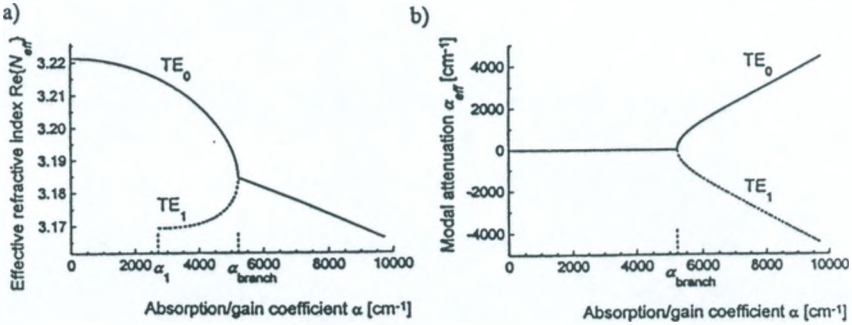


Fig. 2. Effective refractive indices versus attenuation/amplification coefficient α:
a) $\mathrm{Re}\{N_{eff}\}$; b) $\alpha_{eff} = (4\pi/\lambda)\mathrm{Im}\{N_{eff}\}$

modes with *real* effective refractive indices. The modes fulfill the condition of *complex orthogonality* (*without* complex conjugate):

$$\int_{-\infty}^{\infty} E_0(x) \cdot E_1(x)\,dx = 0\,, \tag{17}$$

which follows directly from the wave equation (7). Typical field distribution of modes in this region is shown in fig. 3a. Finally, for values of $\alpha > \alpha_{branch}$, the two modes have mutually complex-conjugate effective indices.

With increasing attenuation/gain in the waveguiding layers above α_1, the effective refractive indices and the mode fields approach to each other, and at $\alpha = \alpha_{branch}$ *both effective indices degenerate into a single real value.* For even larger α, one mode is attenuated while the other grows, but both propagate with the same phase velocity. The mode field distributions are correspondingly concentrated in the

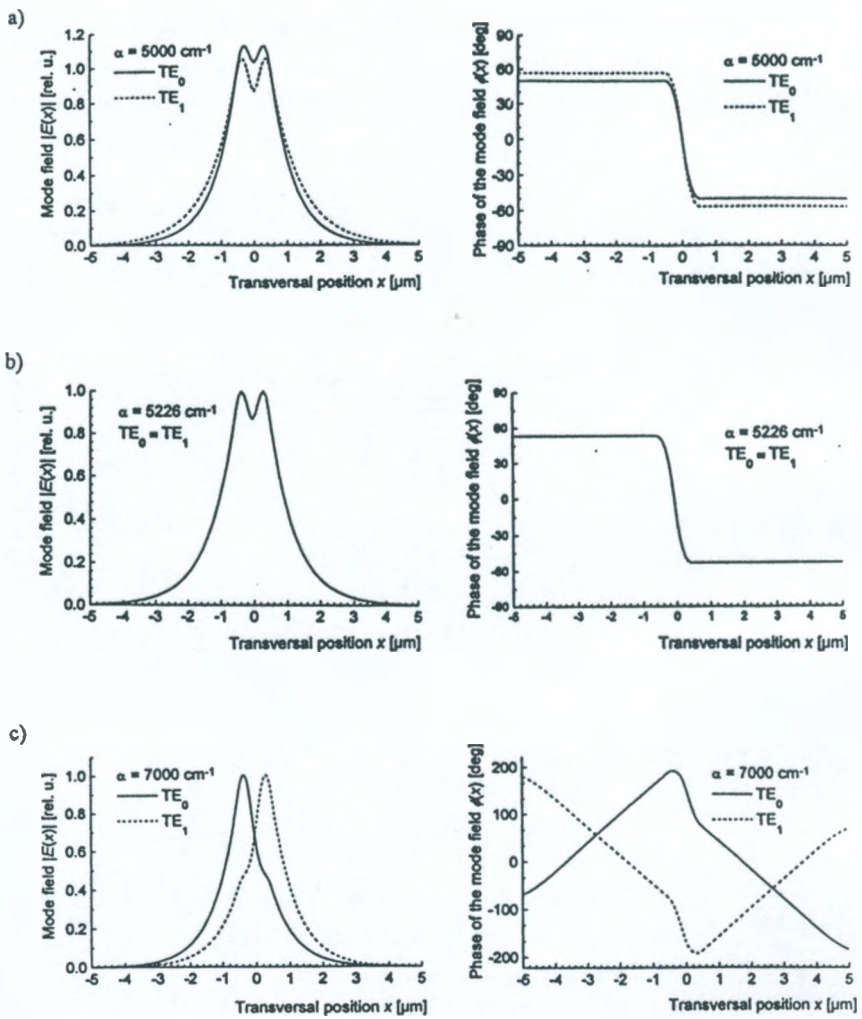


Fig. 3. Typical modal field amplitude and phase distributions: a) for $\alpha < \alpha_{branch}$: lossless modes; b) for $\alpha = \alpha_{branch}$: one degenerate lossless mode; c) for $\alpha > \alpha_{branch}$: the amplified mode is concentrated mainly in the region with gain, while the attenuated mode is concentrated mainly in the lossy region

layer with loss and gain, respectively. The mode field distributions for $\alpha = \alpha_{branch}$ and $\alpha = \alpha_{branch}$ are plotted in fig. 3b and 3c, respectively.

From the asymptotic behavior of mode fields for $\alpha \to \alpha_{branch}$ we can deduce that at α_{branch} the mode fields are degenerate, and the orthogonality condition (17) reduces to the "self-orthogonality":

$$\int_{-\infty}^{\infty} E^2(x)dx = 0\,. \tag{18}$$

It can be verified by numerical integration of the field distribution in fig. 3b. (Note that contrary to the "usual" orthogonality in which one of the functions is complex-conjugate, the complex orthogonality (17) does not require that $E(x) \equiv 0$).

As long as the modes propagate without loss, their phase front *inside* the waveguide is curved as it follows from fig. 3a,b. Since the power flow (Poynting vector) is perpendicular to the phase front, there is a constant energy flow from the layer with gain into the layer with loss. Outside the waveguide "cores", the phase front is perpendicular to the z axis so that there is no transversal power flow there. For $\alpha > \alpha_{branch}$, the phase front is curved in such a way that the mode with loss (which also has the field maximum in the lossy layer, see fig. 3c "absorbs" power from the whole space while the mode with gain "supplies" power into all the space.

2.3. Quasi-analytic solution for α_{branch}

The branching point is very interesting in theoretical point of view just because at this point we have two modes which are one mode. For $\alpha < \alpha_{branch}$ we have two *lossless* modes with similar field distributions, and we thus observe a beat length Λ, which is increasing for

increasing values of α. The branching point α_{branch} has been determined with high accuracy as $\alpha_{branch} = 5226.3023\ cm^{-1}$ by resolving numerically the wave equation for TE modes. For the purpose of the BPM benchmark test we have developed some quasi-analytical solutions for guiding phenomena near the branching point.

From fig. 2 it is seen that at the branch point α_{branch}, $d\varepsilon_{eff}/d\alpha \to \pm\infty$. Since $d\varepsilon_{eff}/d\alpha = -(\partial\Phi/\partial\alpha)/(\partial\Phi/\partial\varepsilon_{eff})$ as follows from the dispersion equation (16), it means that $\partial\Phi/\partial\varepsilon_{eff} = 0$. We get the critical value of α_{branch} by solving a set of two complex transcendental equations:

$$\Phi(\varepsilon_{eff}, \alpha) = 0, \quad \partial\Phi/\partial\varepsilon_{eff} = 0 \tag{19}$$

for ε_{eff} and α. Their (numerical) solution gives $\alpha_{branch} = 5226.3023\ cm^{-1}$, $\varepsilon_{eff} = 10.14124279$. The behavior of the dispersion curves in fig. 2 can be easily explained by the following arguments: Since $\Phi(\varepsilon_{eff}, \alpha)$ is a regular function of the complex variable ε_{eff} and a smooth function of α, it can be expanded into the Taylor (Laurent) series:

$$\begin{aligned}\Phi(\varepsilon_{eff}, \alpha) \approx{}& \Phi(\varepsilon_{eff,B}, \alpha_B) + \Phi'_{\varepsilon} \cdot (\varepsilon_{eff} - \varepsilon_{eff,B}) + \\ &+ \Phi'_{\alpha} \cdot (\alpha - \alpha_B) + \frac{1}{2}\Phi''_{\varepsilon}(\varepsilon_{eff} - \varepsilon_{eff,B})^2 + \\ &+ \Phi''_{\varepsilon\alpha}(\alpha - \alpha_B)(\varepsilon_{eff} - \varepsilon_{eff,B}) + L,\end{aligned} \tag{20}$$

where:

$$\Phi'_{\varepsilon} = \partial\Phi/\partial\varepsilon_{eff}, \quad \Phi'_{\alpha} = \partial\Phi/\partial\alpha, \quad \Phi''_{\varepsilon} = \partial^2\Phi/\partial\varepsilon_{eff}^2, \quad \Phi''_{\varepsilon\alpha} = \partial^2\Phi/\partial\alpha\partial\varepsilon_{eff}$$

are the derivatives taken at the branching point $\alpha = \alpha_B$, $\varepsilon_{eff} = \varepsilon_{eff,B}$. It follows from (19) that in the expansion in the vicinity of the branching point the first two terms vanish. The dispersion equation can thus be approximated by:

$$\Phi(\varepsilon_{eff}, \alpha) \approx \Phi'_{\alpha}(\alpha - \alpha_B) + \Phi''_{\alpha\varepsilon}(\alpha - \alpha_B)(\varepsilon_{eff} - \varepsilon_{eff,B}) + \\ + \frac{1}{2}\Phi''_{\varepsilon_{eff}}(\varepsilon_{eff} - \varepsilon_{eff,B})^2 = 0, \tag{21}$$

the solution of which is:

$$\varepsilon_{eff} \approx \varepsilon_{eff,B} - \Phi''_{\alpha\varepsilon}/\Phi''_{\varepsilon}(\alpha - \alpha_B) + \\ \pm\sqrt{\left(\Phi''_{\alpha\varepsilon}/\Phi''_{\varepsilon}\right)^2(\alpha - \alpha_B)^2 - \left(2\Phi'_{\alpha}/\Phi''_{\varepsilon_{eff}}\right)(\alpha - \alpha_B)}. \tag{22}$$

The (approximate) expression for the effective refractive index $N = \sqrt{\varepsilon_{eff}}$ can be easily obtained in the form:

$$N \approx N_B - \frac{\Phi''_{\alpha\varepsilon}}{2N_B\Phi''_{\varepsilon}}(\alpha - \alpha_B) \pm \frac{i}{2N_B}\sqrt{\frac{2\Phi'_{\alpha}}{\Phi''_{\varepsilon}}}(\alpha - \alpha_B)^{1/2} + \\ \mp \frac{i}{8N_B}\sqrt{\frac{2}{\Phi'_{\alpha}}}\frac{\Phi'^{\,2}_{\alpha\varepsilon}}{\Phi''^{\,3/2}_{\varepsilon}}(\alpha - \alpha_B)^{3/2}. \tag{23}$$

We have verified that the expression (23) represents very well the behavior of the dispersion curves in the vicinity of the branching point, even if the last term with the 3/2 power is neglected.

From the expansion (21) it is seen that the branching point really represents a doubly degenerate solution. It is known that the number of zeroes of a regular function *f(z)* inside a closed contour *C* is given by the integral:

$$M = \frac{1}{2\pi i}\oint_C \frac{df(z)/dz}{f(z)}dz, \tag{24}$$

in our case, at $\alpha = \alpha_B$,

$$M = \frac{1}{2\pi i} \oint_C \frac{2\Phi''_{\varepsilon_{eff}}(\varepsilon_{eff} - \varepsilon_{eff,B})}{\Phi''_{\varepsilon_{eff}}(\varepsilon_{eff} - \varepsilon_{eff,B})^2} d\varepsilon_{eff} = \frac{1}{\pi i} \oint_C \frac{d\varepsilon_{eff}}{\varepsilon_{eff} - \varepsilon_{eff,B}} = 2, \quad (25)$$

for any small closed contour C around $\varepsilon_{eff} = \varepsilon_{eff,B}$.

3. DESCRIPTION OF THE PROBLEM

It follows from (23) that for α approaching α_{branch} there are two different effective refractive index values, they differ in real part for $\alpha < \alpha_{branch}$ or in imaginary part for $\alpha > \alpha_{branch}$. An approximate form of (23) is valid for α close to α_{branch}:

$$N \approx N_B - \frac{\Phi''_{\alpha\alpha}}{2N_B\Phi''_\varepsilon}(\alpha - \alpha_B) \pm \frac{i}{2N_B}\sqrt{\frac{2\Phi'_\alpha}{\Phi''_\varepsilon}}(\alpha - \alpha_B)^{1/2} . \quad (26)$$

Therefore, the difference of mode effective indices scales with square root of $\alpha - \alpha_{branch}$.

Thus, if we restrict ourselves to a two-mode system only, we may expect two kinds of interference effects:

- for $\alpha < \alpha_{branch}$, as the modes differ only in phase velocity in this case, the result is a periodic beating with a spatial period Λ proportional inversely to the (real) effective index difference, which in turn is proportional to square root of $(\alpha_{branch} - \alpha)$. Thus we expect a linear dependence:

$$\frac{1}{\Lambda^2} = const\,(\alpha - \alpha_{branch}); \quad (27)$$

- for $\alpha > \alpha_{branch}$ the modes have the same phase velocity, but they differ in a way that one is attenuated while the other is amplified. At long distances of propagation, the domination of the mode with gain is obvious. Therefore, a constant growth of the field is the result of two-mode interference. Thus, the effective two-mode beam power amplification coefficient at long distances is a linear function of gain-loss coefficient α, which in turn is proportional to square root of $\alpha - \alpha_{branch}$. Thus we expect a linear dependence of the form of:

$$\alpha_{eff}^2 = const\ (\alpha - \alpha_{branch}). \tag{28}$$

The branching point has been determined with high accuracy as α_{branch} = 5226.023 cm^{-1} by resolving numerically the wave equation for TE modes. Also as the semianalytical solution gives linear expressions (27)-(28) for beat length close to the branching point, the linear dependencies have been used to define the task as finding $\alpha > \alpha_{branch}$ values from BPM studies.

The passive waveguide/gain-loss waveguide/passive waveguide structure used for definition of the task is shown in fig. 4: a gain-loss waveguide is placed between two lossless (single-mode) input and output waveguides with identical real parts of the refractive index. The outer waveguides ($z < 0$ and $z > L$) have zero imaginary parts of refractive index and are referred to as "real guides". We assume that the gain-loss waveguide is excited at $z = 0$ with the fundamental TE mode of the non-lossy waveguide on the left of fig. 4 ($z < 0$). It has to be emphasised however, that as that mode is not an eigen mode of the inner gain-loss waveguide, therefore the two (or one degenerate at the branching point) guided modes can realize the incoming beam only approximately. The approximation becomes even worse as α approaches α_{branch}, where is impossible to determine numerically the modal expansion coefficients as they diverge to infinity - see (30). This justifies the application of the beam propagation method, which

is totally non-modal method, to analyse the light propagation for α values close to the branching point α_{branch} regardless the modal structure of the beam.

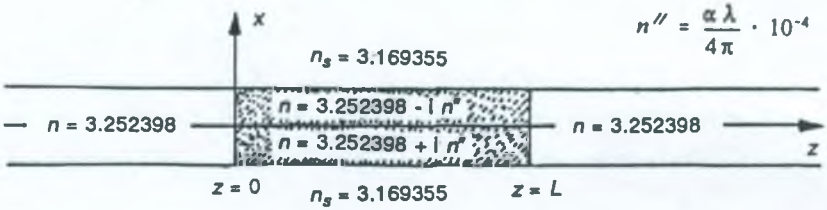


Fig. 4. Passive waveguide /gain-loss/ passive waveguide structure. The transverse dimensions of guides are the same as in fig. 1

The definition of the task is: Calculate the wave behavior for various values of the coefficient α of a gain-loss waveguide, which is placed between two lossless (single-mode) input and output waveguides with identical real parts of the refractive index, in a way as depicted in fig. 4. The task consists of three parts, all of them are to calculate branching point α_{branch} value.

The first part of the task is: determine the branching point α_{branch} from (27) by plotting $1/\Lambda^2$ over α, as is shown in fig. 5, left part. For $\alpha > \alpha_{branch}$ we have a superposition of an amplified and an attenuated modes, where only the amplified one will survive. Thus the second part of the task is to determine α_{branch} from a plot of effective gain constant α_{eff} as a linear function (28) of α as is shown in fig. 5, right part. The insert demonstrates the strong attenuation/amplification behavior of the gain-loss waveguide at $\alpha = 5306\ cm^{-1}$ from -10 dB < 0 dB (start) < 30 dB.

The calculation of the passive waveguide/gain-loss waveguide/passive waveguide structure used for the BPM test for $\alpha < \alpha_{branch}$ shows a variation of the transmitted power P propagating along the z-direction between $P_{min} < P_{start} < P_{max}$. Notice that the two eigenmodes of

the gain-loss waveguide have zero imaginary parts and that we start with 0 dB power in a real passive waveguide. How can we explain this growth behavior, shown in the insert of fig. 5, where we have $P_{min} \leq -10$ dB and $P_{max} > 30$ dB? Investigation with an eigenmode expansion method like the BEP [12] shows.

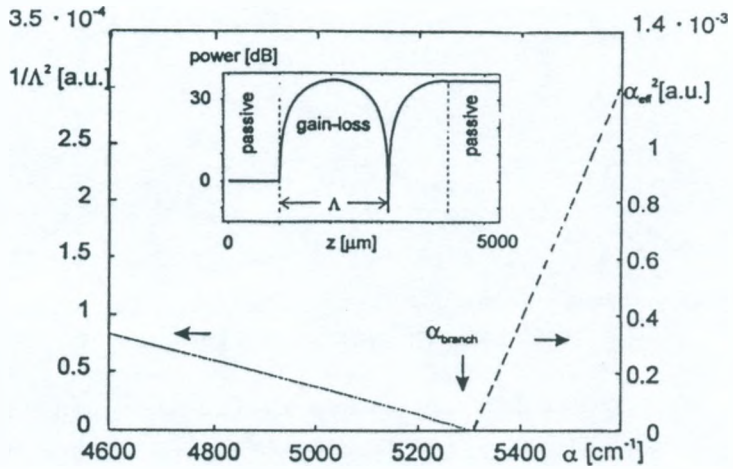


Fig. 5. BPM benchmark test with beat length Λ and α_{eff} as a function of α

Following the notation of [9] (with l = number of the section, i,k = number of modes), we can write the amplitude expansion coefficient a_{ik} at the interface of the passive/gain-loss waveguide as:

$$a_{ik}^{l+1,l} = \frac{\int_{-\infty}^{\infty} E_i^{l+1}(x) \cdot E_k^{l}(x)\,dx}{\sqrt{\int_{-\infty}^{\infty} E_i^{l+1}(x) \cdot E_i^{l+1}(x)\,dx} \cdot \sqrt{\int_{-\infty}^{\infty} E_k^{l}(x) \cdot E_k^{l}(x)\,dx}} \quad . \quad (29)$$

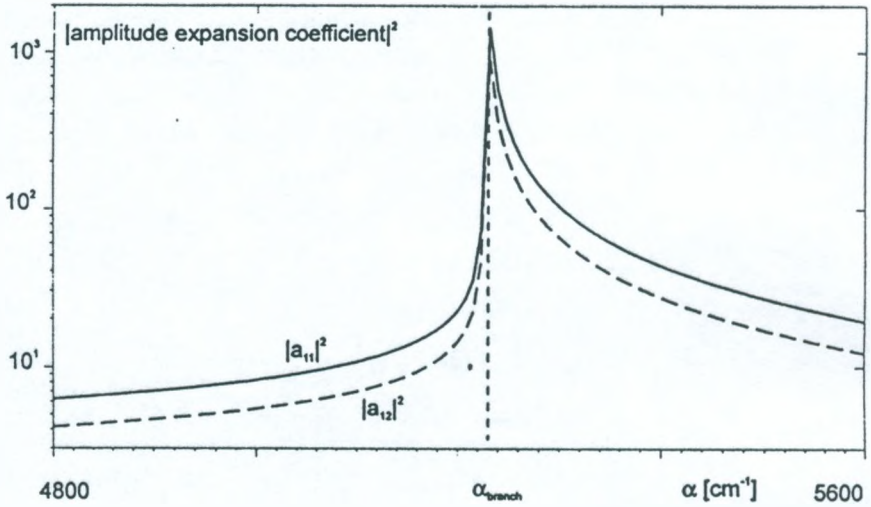


Fig. 6. Asymptotic behavior of the squared absolute value of the amplitude expansion coefficients a_{ik} as a function of α

We have calculated the squared absolute value of the amplitude expansion coefficients a_{ik} at the interface passive/gain-loss waveguide in fig. 6 and observed a strong increase for α approaching α_{branch}. As a driving force we identify that:

$$V = 1 \left(\sqrt{\int_{-\infty}^{\infty} E_l^{l+1}(x)\, E_l^{l+1}(x)\, dx} \right)^{-1} \to \infty \tag{30}$$

due to the "self-orthogonality". We can think of the two modes as of two large numbers $E_1 \cong E_2 = E_1 + \tau$ with $\tau << E_1$. By interference we get $P_{min} \cong \tau^2 << 1$ and $P_{max} \cong |E_1|^2 >> 1$. The asymptotic behavior of the modes for α approaching α_{branch} is as follows: the beat length Λ approaches to infinity, and for $z \to \infty$ the field amplitude growths to infinity, too. This has been used to define the third part of the task: calculate α_{branch} from a plot of $1/P_{max}$ over α. This also indicates the

impossibility to expand the incoming mode of the real guide, with symmetrical field distribution and constant phase accross the beam, into a set consisting of one degenerate mode with asymmetric phase distribution - see fig. 3b. This also makes the BPM an excellent tool to investigate beam propagation in a gain-loss waveguide close to and at the branching point.

4. DEFINITION OF THE BPM TASK

Beam-propagation method has been proved to be an excellent tool to study optical beam propagation in optical waveguides composed of passive media, with real refractive indices [1, 10]. Although up to now used to model light propagation in nonlossy media, the method can be easily extended to transparent media with gain or loss.

For a planar isotropic waveguide a scalar wave equation is valid. Standard beam-propagation algorithms deal with a solution to hyperbolic Helmholtz equation:

$$E(z) = E_0 \exp\left[\mathrm{i}z \sqrt{\frac{\partial^2}{\partial x^2} + k_0^2 n_r^2} + \mathrm{i}k_0 (n - n_r) z \right] \tag{31}$$

or with a solution to Fresnel parabolic equation

$$E(z) = E_0 \exp\left\{ \frac{-\mathrm{i}z}{2k_r} \left[\frac{\partial^2}{\partial x^2} + k_0^2 \left(n^2 - n_r^2 \right) \right] \right\}, \tag{32}$$

where z is the direction of propagation, E_0 is the initial field distribution at a cross section $z = 0$, $n = n(x, z)$ is the refractive index distribution in the waveguide, and n_r is the index of refraction of a reference medium in which the free-space propagation steps are to be carried out. It is assumed that the value of n_r is real and close to

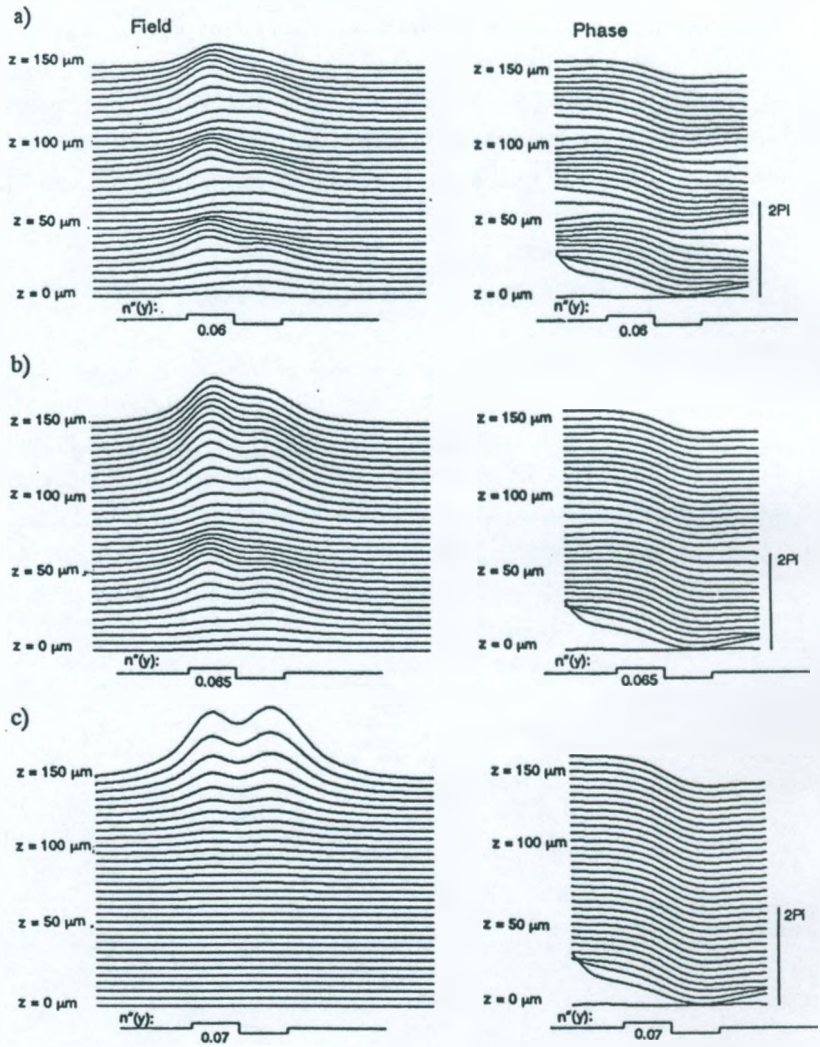


Fig. 7. Field evolution and phase distribution along the gain-loss waveguide from fig. 4 when excited at $z = 0$ with the fundamental mode of the real guide (BPM simulation):
a) $\alpha < \alpha_{branch}$; b) $\alpha = \alpha_{branch}$; c) $\alpha > \alpha_{branch}$

those of the media constituting the system. $E(x,z)$ is a slowly-varying field amplitude, and k_r is the wavenumber in the reference medium, $k_r = n_r\omega/c$.

Now the occurrence of loss or gain in a medium may be automatically accounted for in the phase compensation steps, by an appropriate exponential change (increase for gain, decrease for loss) of the field amplitude according to the imaginary part of the refractive index n [6].

Fig. 7 shows the field and phase front evolution along the gain-loss guide, for values of α below, close to and above α_{branch}.

5. BPM BENCHMARK TEST RESULTS

The analyzed waveguide structure is composed of a sequence of three waveguides, as shown in fig. 4: a gain-loss waveguide is placed between two lossless (single-mode) input and output waveguides with identical real parts of the refractive index, with dimensions and parameters as in fig. 1. This problem has been used for defining the present benchmark test for the beam propagation method (BPM), in comparison with the quasi-analytic solution (19). This test is complementary to the two tests published earlier [1, 10]. It is focused on the imaginary part of the refractive index, which was always zero in the previous tests.

In order to prove the usefulness of BPM to this kind of waveguide and to compare the results of BPM from different laboratories participating in COST 240, we have defined three particular problems to calculate, for which analytic or semi-analytic solutions may serve to some extend as a point of reference. However, the restriction is that since in the complex guide not only the guided, but also radiation field is included especially close to the branching point, therefore the two-mode theoretical model is not quite adequate to the physics of the problem. As a consequence, one can't absolutly rely on the exact-

ness of those solution in this particular problem. Also, the goal of the test was to compare the relative exactness of different programs used by the participants to the task.

- **Contributors and used methods**

The contributors and their algorithms are listed in table 1.

Heinrich Hertz Institute (Berlin) (HHI): Finite element /finite difference BPM (FE/FD) has been used [4].

University Hagen (U. Hagen): Method of lines (MoL).

University Twente (U. Twente): Finite difference BPM (FD) with third order SVEA correction Padé (3,3) and efficient interface conditions have been used [2, 3], $\Delta x = 0.002$ μm, $\Delta z = 1$ μm, number of points along x-axis: 3000.

Academy of Telecommunications/Institute of Telecommunications (Ac. Comm.): Fourier transform BPM (FT) (Helmholtz equation) with absorbing boundary conditions has been used with 4 μm observation window size, 256 equidistant sampling points in the transverse direction, and propagation step $\Delta z = 1/8$ μm.

University Roma I (U. Roma I): Method of lines with a set of lines equidistant along transverse direction has been used. An observation window 11 μm large and absorbing conditions at the boundaries have been used.

Table 1

List of contributors

Institution	Equation	Numerical method	Boundary conditions	Propagation step size
HHI		FE/FD		
U. Hagen		MoL		-
U. Twente		FD	Efficient	1 μm
Ac. Comm.	Helmholtz	FT	Absorber	1/8 μm
U. Roma I		MoL	Absorber	-

6. DISCUSSION OF THE RESULTS

The results of the task are shown in fig. 8, 9, 10 for the three consequent parts of the task. The participants have obtained points that fall quite on stright lines, as expected from the theory. The positions and the slope of the lines slightly differ. The results of Fourier transform BPM (Ac. Comm.) are quite different from the others, this should be attributed to the fact that FT BPM is not very suitable for guides with large index difference, and inherent to this method periodic boundary conditions cause reapearence of waves that have left the observation window propagation in that window, what makes the results not very reliable, especially for large distances of propagation.

The resulting values of α_{branch} with comparison to analytic value $\alpha_{branch\ anal.}$ = 5226.3/cm are reported in table 2. The differences with respect to the analytic solution do not necessarily mean errors of the method, because the propagated beam is not a combination of two

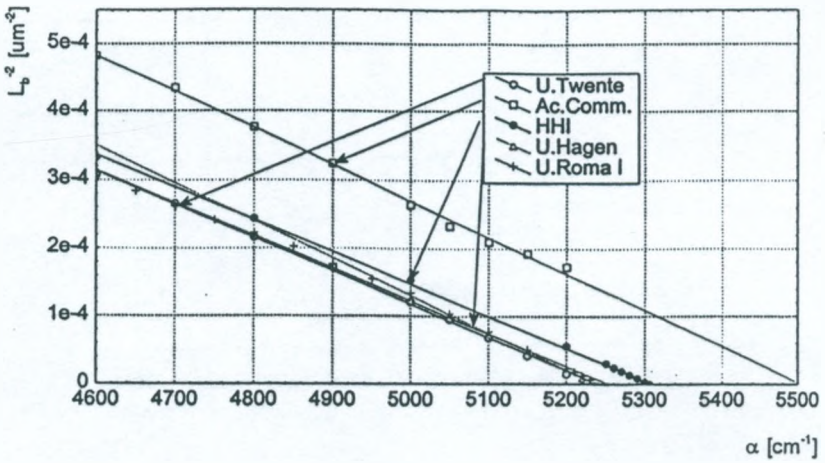


Fig. 8. Plots of results for 1/Λ beat square

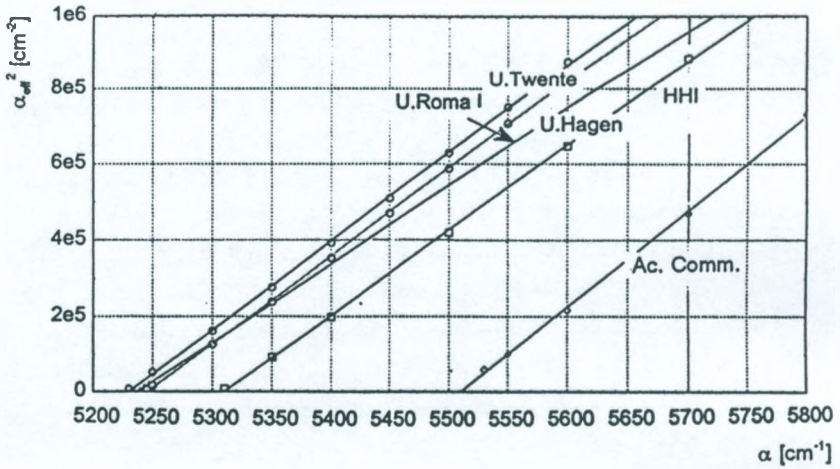


Fig. 9. Plots of results for α_{eff}^2

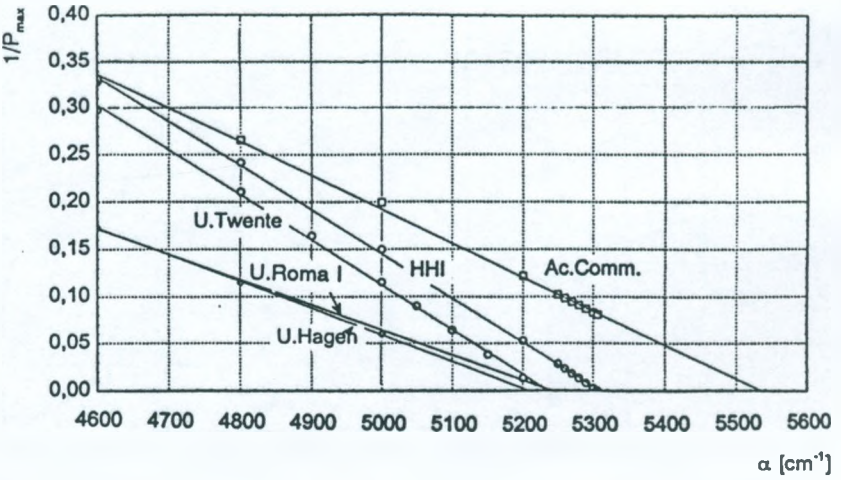


Fig. 10. Plots of results for $1/P_{max}$

guided modes of the active guide only, but also of a radiation field of this guide.

The participants to the task have done much of numerical effort to avoid inaccuracies due to numerical errors, thus the observed discrepancies should be attributed to different physical models modelled by the BPM programs used. In other words, every method used has analysed very accurately a little different situation.

Table 2

Values of α_{branch} obtained by the participants to the benchmark test

Contributor	α_{branch} [1/cm]	$\alpha_{branch} - \alpha_{branch\ anal.}$ [1/cm]
HHI	5306	79.7
U. Hagen	5236.87	10.57
U. Twente	5226.5	0.2
U. Twente	5226.9	0.6
Ac. Comm.	5500	273.7
U. Roma I	5242.5	16.2

7. CONCLUSION

Beam propagation method has been successfully applied to analyze non-modal beam propagation in a waveguide with a balance of gain and loss. We particularly have analyzed with BPM a special case of gain and loss values corresponding to degenerate solution in so called "branching point" of the dispersion curves, for which the beam expansion into the guided modes fails because of infinite values of expansion coefficients. For this particular point the BPM simulation seems to be the only reasonable way to study the optical field evolution.

We also have compared results of different BPM programs in view of their applicability to the problem and accuracy of the results.

Although different propagation schemes have led to quite consistent results, there are some systematic discrepancies that we believe are due to physical meaning of the method used.

ACKNOWLEDGMENT

The author thanks his colleagues from COST 240 Working Group 2, Waveguides: Dr H.-P. Nolting, Prof. R. Pregla, Prof. C. Sibilia, Dr J. Ctyroky and Dr H. Hoekstra, for their fruitful contributions to BPM study of the gain-loss waveguide, as well as for continuous exchange of results in this particular waveguide case analysis.

REFERENCES

1. Haes J., Baets R., Weinert C.M., Gravert M., Nolting H.-P., Adelaide Andrade M., Leite A., Bissessur H.K., Davies J.B., Ettinger R.D., Čtyroký J., Ducloux E., Ratovelomanana F., Vodjdani N., Helfert S., Pregla R., Wijnands F.H.G.M., Hoekstra H.J.W.M., Krijnen G.J.M.: A Comparison Between Different Propagative Schemes for the Simulation of Tapered Step Index Slab Waveguides. IEEE J. Lightwave Technology, Vol. 14, No. 6, 1996, pp. 1557-1569.
2. Hoekstra H.J.W.M., Krijnen G.J.M., Lambeck P.V.: Efficient interface conditions for the FD BPM. IEEE J. Lightwave Technology, Vol. 10, 1992, pp. 1352-1355.
3. Hoekstra H.J.W.M., Krijnen G.J.M., Lambeck P.V.: New formulation of the BPM based on the slowly warying envelope approximation. Optics Communications 96, 1993, pp. 301-303.
4. Koch T., Davies J.B., Wickramasinhge D.: A Finite Difference/Finite Element propagation algorithm for integrated optical device. Electronics Letters, Vol. 25, No. 8, 1989, pp. 514-516.
5. Marciniak M.: COST 240 Meeting. Porto, October 1995.
6. Marciniak M.: Light propagation in optical waveguides with complex refractive indices. Optica Applicata, Vol. XXVI, No. 4, 1996, pp. 359-368.

7. Marciniak M., Grzegorzewski J., Szustakowski M.: Analysis of lossy mode cut-off conditions in planar waveguides with semiconductor guiding layer. IEE Proceedings - J: Optoelectronics, Vol. 140, No. 4, 1993, pp. 247-252.
8. Nolting H.-P.: COST 240 Meeting. Dublin, March 1995.
9. Nolting H.-P., Grawert M.: A Comparison between Different Methods to Calculate Grating Assisted Asymmetrical Couplers. Linear and Nonlinear Integrated Optics, 11-13 April 1994, Lindau 94, Germany, Proceedings Europto Series, Vol. 2212, pp. 328-336.
10. Nolting H.P., März R.: Results of Benchmark Tests for Different Numerical BPM Algorithms. IEEE J. Lightwave Technology, Vol. 13, No. 2, 1995, pp. 216-224.
11. Nolting H.-P., Sztefka G., Grawert M., Čtyroký J.: Wave Propagation in a Waveguide with a Balance of Gain and Loss. IPR 96.
12. Sztefka G., Nolting H.-P.: Bidirectional Eigenmode Propagation for Large Refractive Index Steps. IEEE Photon. Technol. Lett., Vol. 5, No. 5, 1993, pp. 554-557.
13. Takano T., Hamasaki J.: Propagation Modes of a Metal-Clad Dielectric-Slab Waveguide for Integrated Optics. IEEE Journal of Quantum Electronics, Vol. QE-8, No. 2, 1972, pp. 206-212.

Marian Marciniak

ANALIZA PLANARNEGO FALOWODU OPTYCZNEGO Z WARSTWĄ TŁUMIĄCĄ I WZMACNIAJĄCĄ Z ZASTOSOWANIEM METODY PROPAGACJI WIĄZKI

Streszczenie

Przedstawiono rezultaty analizy propagacji światła w falowodzie optycznym o zrównoważonym tłumieniu i wzmocnieniu, z zastosowaniem metody propagacji wiązki BPM. Wyniki porównano z semianalitycznym oraz numerycznym rozwiązaniem równania falowego.

Марян Марциняк

АНАЛИЗ ПЛАНАРНОГО ОПТИЧЕСКОГО СВЕТОВОДА СО СЛОЕМ ЗАТУХАНИЯ И УСИЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДА РАСПРОСТРАНЕНИЯ ПУЧКА

Р е з ю м е

Представлено резуьтаты анализа распространения световых волн в оптическом световоде с уравновесменным затуханием и усилением с использованием метода распространения пучка BPM. Полученные результаты сравнено с семи-аналитическим и цифровым решением волнового уравнения.

Marian Marciniak

L'ANALYSE D'UN PLANAIRE GUIDE D'ONDES AUX COUCHES D'AFFAIBLISSEMENT ET D'AMPLIFICATION

R é s u m é

Les résultats de l'analyse de la propagation de lumière à l'interieur d'optique guide d'ondes aux affaiblissement et amplification équilibrés avec l'utilisation d'une méthode BPM de la propagation de faisceau lumineux sont présentés. Les résultats obtenus sont comparés dans cet article avec une solution semianalitique et numérique de l'équation d'onde.

Marian Marciniak

BPM-ANALYSE DES PLANAREN LICHTWELLENLEITERS MIT VERSTÄRKUNGS- UND DÄMPFUNGSSCHICHT

Z u s a m m e n f a s s u n g

Es sind Studien über Lichtpropagation im Lichtwellenleiter mit Ausgleichung von Verstärkung und Dämpfung durchgeführt worden, das erste Mal

mit Bündel-Propagation-Methode. Im Beitrag werden Ergebnisse vorgestellt und mit semianalytischer und numerischer Auflösung der Wellengleichung verglichen.

Marian Marciniak

621.391.631:535.37:621.371

TWO-BEAM-PROPAGATION METHOD MODELING OF SECOND-HARMONIC GENERATION IN DIELECTRIC PLANAR WAVEGUIDES

A new Two-Beam-Propagation Method algorithm for simulation of Second-Harmonic Generation (SHG) process in planar optical waveguides is presented. The model accounts for an evolution of two-beams propagating simultaneously: the fundamental and the second-harmonic one. Physically, the model consists of a separation of the propagation step and the nonlinear phase and amplitude compensation step. Mathematical formulation of the model is reported and some of its special features are discussed. The method can be easily generalized to investigate SHG processes in optical guides made from media with gain and/or loss. Also other nonlinear wave interactions such as self-phase modulation and cross-phase modulation can be dealt with using the new method.

1. INTRODUCTION

Beam-Propagation Method (BPM) is now a widely used split-step numerical technique for computer simulations of light propagation in transparent optical media including dielectric and semiconductor waveguiding structures [10], especially for fiber optic telecommunication applications [12]. The method was introduced by Fleck, Morris and Feit for modeling of laser beam propagation through nonhomogeneous atmosphere in 1976 [8]. In 1979-1980 the method was adopted by Feit and Fleck for modeling of light propagation in optical waveguides in a series of papers in "Applied Optics" [5, 6, 7]. Since then, the method has been successfully applied to analyze

various optical waveguide structures, including integrated optic waveguides made of media with gain and loss, and nonlinear waveguides as well.

This contribution reports on some recent activities in BPM modeling of light propagation in optical waveguides that have been carried out in the framework of COST 240 European Project: "Techniques for Modelling and Measuring Advanced Photonic Telecommunications Components, Working Group 2, Waveguide Devices". In particular, a new model for Beam-Propagation Method simulation of Second-Harmonic Generation (SHG) process in optical waveguides is presented. Since the model describes a simultaneous propagation of the two beams involved: the fundamental wave and second-harmonic one, we have called it Two-Beam-Propagation Method algorithm. The presented model has been developed in a framework of COST 240 Project [13], and it has been recently reported at international conferences [8, 9, 10].

2. DESCRIPTION OF THE ALGORITHM

This part is devoted to an adaptation of the BPM for modeling of SHG process in quasi-periodically corrugated planar waveguides. Those are waveguides of sequentially repeated step changes in guiding layer thickness according to self-similarity or fractal rules, especially triadic Cantor sequence is commonly reported in the literature [2, 3]. The fractal properties of the structure reflect in wavelength selectivity of transmission and reflection characteristics, thus they are often used as optical wavelength filters and reflectors.

Quasi-periodic planar waveguides are of particular interest for improving the efficiency of SHG process, as the quasi-phase matching conditions for fundamental and second-harmonic waves can be met when using them. Actually, the primary interest of this work was to model SHG in a Cantor corrugated waveguide. For that purpose,

an efficient algorithm for propagation and nonlinear interaction of fundamental and second-harmonic optical beams in a planar waveguide of a given thickness had to be invented.

In this work, a type I (eoo) of SHG has been chosen as a working example, and a model of split-step formalism of SHG has been developed. The model involves simultaneous propagation of two beams: the fundamental (pump) beam and second-harmonic beam, what justifies the name we have called it: Two-Beam-Propagation Method. We remind the reader that we consider one-dimensional optical beams propagating in a planar waveguide, and the planar waveguide is a one-dimensional free-space as there are no refractive index changes in that transversal direction which is parallel to the layers forming the waveguide. The fundamentals of the model are outlined below.

As a starting point the following coupled set of governing equations has been adopted [4]:

$$j\frac{\partial a_1}{\partial \xi} + \frac{1}{2}\frac{\partial^2 a_1}{\partial s^2} + a_1^* a_2 \exp(-j\Delta\beta\xi) = 0, \tag{1}$$

$$j\frac{\partial a_2}{\partial \xi} + \frac{\alpha}{2}\frac{\partial^2 a_2}{\partial s^2} + a_1^2 \exp(+j\Delta\beta\xi) = 0, \tag{2}$$

where a_1 is the normalized fundamental wave amplitude, a_2 is the normalized second-harmonic wave amplitude, s is the normalized transversal co-ordinate parallel to the boundaries of the layers forming the waveguide, and ξ is the normalized longitudinal co-ordinate in the waveguide. The amplitudes a_1, a_2, and the spatial co-ordinates ξ, s are normalized in the following way [15]:

$$a_1 = |K_1 K_2|^{\frac{1}{2}} |k_1| \eta^2 A_1, \qquad a_2 = |K_1|\,|k_1|\,\eta^2 A_2,$$

$$\xi = \frac{z}{\eta^2 |k_1|}, \qquad s = \frac{x}{\eta},$$

where k_i are the linear wave numbers and K_i are the overlap integrals of the modes propagating inside the guide with $i = 1$ for the fundamental wave and $i = 2$ for the second-harmonic wave, z is the propagation direction along the waveguide and x is the transverse direction. The coefficient α is given by

$$\alpha = -\frac{|k_1|}{k_2} \cong -0.5 .$$

Parameter η is an arbitrary parameter set at $\eta = 20\ \mu$m [4], and A_1 and A_2 are the field amplitudes of the fundamental and second-harmonic wave, respectively.

The phase propagation constant mismatch of the fundamental and second-harmonic wave modes $\Delta\beta$ is given by

$$\Delta\beta = \Delta k \eta^2 |k_1| ,$$

where $\Delta k = 2\ k_1 - k_2$ is the wave-vector mismatch.

Since the coupled set of equations (1), (2) cannot be solved analytically [4], semi-analytic or numerical methods have to be applied for description of the evolution of the beams. The BPM which is a semi-analytic method is especially suited for that purpose. In the next part of the paper a new algorithm of Two-Beam-Propagation Method modeling of SHG process in a waveguide is described in detail.

The developed numerical model of two-beams-propagation consists of two steps reproduced sequentially: the propagation step, and the compensation step. The model is shown schematically in fig. 1.

Fig. 1. Schematic model of Two-Beam-Propagation Method algorithm

Step 1 involves propagation of the beams only, and diffraction effects. The beams propagate independently as in the linear case so they can be treated separately. SHG process is not included in this step. This is equivalent to uncouple the governing equations by assuming the other's wave amplitude equal to zero:

$$j\frac{\partial a_1}{\partial \xi} + \frac{1}{2}\frac{\partial^2 a_1}{\partial s^2} + 0 = 0, \quad (a_2 = 0), \tag{3}$$

$$j\frac{\partial a_2}{\partial \xi} - \frac{\alpha}{2}\frac{\partial^2 a_2}{\partial s^2} + 0 = 0, \quad (a_1 = 0). \tag{4}$$

Step 2 involves nonlinear compensation of the amplitudes and phases of both beams. Simultaneously, no diffraction occurs, what follows from an assumption of vanishing transverse variation of the beams, i.e. $\partial^2/\partial s^2 = 0$. This is equivalent to plane wave propagation. Analytic description of this step is:

$$j\frac{\partial a_1}{\partial \xi} + 0 + a_1^* a_2 \exp(-j\Delta\beta\xi) = 0, \tag{5}$$

$$j\frac{\partial a_2}{\partial \xi} + 0 + a_1^2 \exp(+j\Delta\beta\xi) = 0. \tag{6}$$

The propagation step of the beams can be easily modeled via standard BPM techniques (e.g. Fourier-Transform or Finite-Difference based algorithms).

The nonlinear compensation step involves more difficulty. Under assumed conditions, the fundamental (ω) and second-harmonic (2ω) fields are subjects of the following nonlinear changes [1]:

Fundamental wave amplitude change:

$$|\tilde{A}_\omega(z)| = \left[\frac{8\pi}{n_\omega c} I_{\omega 0} - \frac{n_{2\omega}}{n_\omega} U_\omega^- sn^2\left(\frac{K(m)}{L_{\omega NL}} z|m\right)\right]^{\frac{1}{2}}. \tag{7}$$

Second-harmonic wave amplitude change:

$$|\tilde{A}_{2\omega}(z)| = \sqrt{U_{\omega}^{-}}\left|sn\left(\frac{K(m)}{\tilde{L}_{\omega NM}} z|m\right)\right|, \tag{8}$$

where the notation of [1] has been adopted. The above amplitude changes are explicitly given and do not present difficulty in calculations.

Similarly, phases of the waves change in the following way [1]:

The fundamental wave phase:

$$\Phi_{\omega}(z) = \Phi_{\omega 0} - \frac{4\pi\Delta q}{cn_{\omega}} I_{\omega 0} \int_0^z \frac{dz}{\frac{8\pi}{n_{\omega}c} I_{\omega} - \frac{n_{2\omega}}{n_{\omega}} U_{\omega}^{-} sn^2\left(\frac{K(m)}{\tilde{L}_{\omega NL}} z|m\right)}. \tag{9}$$

The second-harmonic wave phase:

$$\Phi_{2\omega}(z) = \Phi_{2\omega 0} + \pi \sum_{l=1}^{\infty} step(z - 2l\tilde{L}_{\omega NL}). \tag{10}$$

Of the above, only the first expression for fundamental wave phase change is given not explicitly, since it contains an integral. The integral has to be evaluated numerically.

As in a standard BPM, for achieving better accuracy with given propagation step, the calculation should be started with an initial half-step propagation:

Propagation ($\Delta z/2$) → Nonlinear compensation (Δz) → Propagation ($\Delta z/2$)

or, equivalently

Nonlinear compensation ($\Delta z/2$) → Propagation (Δz) → Nonlinear compensation ($\Delta z/2$)

In the above, after the first half-step calculation, the subsequent half-steps can be combined what results in performing all steps at Δz propagation grid according to the following scheme:

$$P(\Delta z/2) \rightarrow NC(\Delta z) \rightarrow P(\Delta z) \rightarrow NC(\Delta z) \rightarrow P(\Delta z) \rightarrow NC(\Delta z) \ldots$$

where **P** stands for propagation step and **NC** stands for nonlinear compensation step.

3. DISCUSSION

Some special features of the presented algorithm are pointed out below.

1. In quasi-periodical planar waveguide the phase mismatch $\Delta\beta$ varies according to the local thickness in a given section of the waveguide. Since in realistic corrugated waveguides the thickness variation is very small, this may be considered as an perturbation in a homogeneous waveguide. This issue and its impact on the amount of reflections at the boundaries is currently under study. However, it is believed that one could neglect the reflections for small changes of waveguide thickness and non-resonant optical wavelengths.
2. In the analyzed problem the beams propagate in a planar waveguide, which is a one-dimensional free space for the beams. This means that without nonlinear effects the propagation step length might be arbitrarily long. However, as the SGH process is sensitive to amplitudes and phases of the interacting beams, the propagation step should not involve significant amplitude and phase changes. Thus carry has to be taken out that propagation steps are not to long in order to properly model the SHG process.
3. For keeping the accuracy of the modeling and also to shorten the computational time needed for modeling of the device, it might be necessary to use an adaptive propagation step length. This is due

to the dependence of efficiency of SHG on amplitudes of both the waves, and their phase relations.

4. For checking the accuracy of SHG modeling in a given waveguide structure it is necessary to compare the results with an analytical solution for the geometry considered. Such solutions are available when second-harmonic beam has zero amplitude at the starting point [16].

The presented Two-Beam-Propagation Method can be easily generalized to investigate SHG processes in optical guides made from media with gain and/or loss, and also exhibiting nonlinear self-phase modulation and cross-phase modulation phenomena of different kinds. This should be included in the complex phase compensation step by a proper modification of the optical field phase and intensity. This way the presented algorithm appears as a very powerful and universal tool to model SHG process and other nonlinear wave interactions under various realistic experimental arrangements.

The Two-Beam-Propagation Method procedure is actually a subject of further development in COST 240 laboratories in University Roma I "La Sapienza", Dipartimento di Electronica, and Institute of Telecommunications, Department of Transmission and Fiber Technology, Warsaw, in order to obtain an efficient tool for SHG modeling in planar waveguides, including quasi-periodic corrugation of the guides along the propagation.

Both laboratories have agreed to further develop the Two-Beam--Propagation Method procedure in order to obtain an efficient tool for SHG modeling in planar waveguides, including quasi-periodic corrugation of the guides along the propagation. The problem of including the reflected beams in the two-beam-propagation procedure is a subject of further study. A call for a candidate to a Ph. D. thesis on that topic has been done at the Institute of Telecommunications, Department of Transmission and Fiber Technology. Also, the pertur-

bation analysis of the corrugated waveguide is currently under study in both laboratories.

ACKNOWLEDGEMENT

The author acknowledges the co-operation and fruitful discussions with his colleagues from COST 240 Project. He also wishes to express his special thanks to COST 240 Chairman, prof. George Guekos from ETH Zurich, Switzerland. The author thanks Prof. Mario Bertolotti and Prof. Concita Sibilia from Universitá di Roma I "La Sapienza", Dipartimento di Energetica, for their kind co-operation during his COST 240 Scientific Mission to their laboratory in March 1998. He also thanks several other scientists from the host laboratory for numerous discussions and fruitful comments relevant to the development of the presented model. The support of COST 240 activities by the General Directoriat DG XIII of the European Commission in Brussels is greatly appreciated.

REFERENCES

1. Aguanno G.D., Sibilia C., Fazio E., Ferrari E., Bertolotti M.: Fields phase modulation and input phase and intensity dependence in a nonlinear second order interaction. Accepted for "Journal of Modern Optics", 1998.
2. Bertolotti M., Masciulli P., Ranieri R., Sibilia C.: Optical bistability in a nonlinear Cantor corrugated waveguide. Journal of the Optical Society of America B, Vol. 13, No. 7, 1996, pp. 1517÷1525.
3. Bertolotti M., Masciulli P., Sibilia C., Wijnands F., Hoekstra H.: Transmission properties of a Cantor corrugated waveguide. Journal of the Optical Society of America B, Vol. 13, No. 3, 1996, pp. 628÷634.
4. Cerioni R., Sibilia C., Bertolotti M., Dekker J.: Spatial control of pulses in quadratic nonlinear materials. Optical and Quantum Electronics, Special Issue on Optical Waveguide Theory and Numerical Modelling, 1998.

5. Feit M.D., Fleck J.A. Jr.: Calculation of dispersion in graded-index multimode fibers by a propagating-beam method. Applied Optics, Vol. 18, No. 16, 1979, pp. 2843÷2851.
6. Feit M.D., Fleck J.A. Jr.: Computation of mode properties in optical fiber waveguides by a propagating-beam method. Applied Optics, Vol. 19, No. 7, 1980, pp. 1154÷1164.
7. Feit M.D., Fleck J.A. Jr.: Light Propagation in graded-index optical fibers. Applied Optics, Vol. 17, 1978, pp. 3990÷3998.
8. Fleck J.A. Jr., Morris J.R., Feit M.D.: Time-Dependent Propagation of High Energy Laser Beams through the Atmosphere. Applied Physics, Vol. 10, No. 2, 1976, pp. 129÷160.
9. Marciniak M.: Beam-Propagation Method modelling of light propagation in optical waveguides. International Conference on Mathematical Methods in Electromagnetic Theory MMET'98, Invited Paper Inv 09, 2-5 June, 1998, Kharkov (Ukraine).
10. Marciniak M.: Beam-Propagation Method modelling of optical waveguides. Telecommunication and Transport Publishers (WKL), Warsaw 1995.
11. Marciniak M.: Beam-Propagation Method Modelling of Second-Harmonic Generation in Dielectric Planar Waveguides. International Workshop on Optical Waveguide Theory and Numerical Modelling, 18-19 September 1998, Hagen (Germany).
12. Marciniak M.: Optical Fibre Telecommunications. Telecommunication and Transport Publishers (WKL), Warsaw 1998.
13. Marciniak M.: Report on COST 240 Short-Term Visit. University Roma I "La Sapienza", Dipartimento di Energetica, 10-28 March, 1998, Roma (Italy).
14. Marciniak M.: Two-Beam-Propagation Method algorithm of second--harmonic generation in dielectric planar waveguides. International Workshop and Fall School for Young Scientists and Students "Light Scattering Technologies in Mechanics, Biomedicine and Material Science", 6-9 October, 1998, Saratov (Russia).
15. Menyuk C.R., Schiek R., Torner L.: Solitary waves due to cascading. Journal of the Optical Society of America B, Vol. 11, 1994, pp. 2434÷2443.

16. Re A., Sibilia C., Fazio E., Bertolotti M.: Field dependent effects in a quadratic nonlinear medium. Journal of Modern Optics, Vol. 42, No. 4, 1995, pp. 823÷839.

Marian Marciniak

MODELOWANIE GENERACJI DRUGIEJ HARMONICZNEJ W FALOWODACH OPTYCZNYCH METODĄ PROPAGACJI DWU WIĄZEK

Streszczenie

Zaprezentowano algorytm nowej metody modelowania generacji drugiej harmonicznej w planarnych falowodach optycznych metodą propagacji dwu wiązek 2-BPM (*Two-Beam-Propagation Method*). Model uwzględnia równolegle równoczesną ewolucję wiązki o częstotliwości podstawowej oraz generowanej drugiej harmonicznej. Algorytm numeryczny polega na oddzieleniu zachodzących jednocześnie zjawisk propagacji oraz nieliniowej kompensacji fazy i amplitudy, są one modelowane jako zachodzące naprzemiennie. Przedstawiono podstawy matematyczne nowej metody. Metoda może być łatwo uogólniona do przypadku generacji drugiej harmonicznej w falowodach wykonanych z ośrodków tłumiących lub wzmacniających światło. Również inne nieliniowe procesy optyczne w falowodach, jak samomodulacja fazy oraz skrośna modulacja fazy, mogą być analizowane opisaną metodą.

Марян Марциняк

МОДЕЛИРОВАНИЕ ГЕНЕРИРОВАНИЯ ВТОРОЙ ГАРМОНИКИ В ОПТОВОДАХ МЕТОДОМ РАСПРОСТРАНЕНИЯ ДВУХ ПУЧКОВ

Резюме

Приводится алгоритм нового метода моделирования генерирования второй гармоники в планарных оптоводах мето-

дом генерации двух пучков 2-BPM (Two-Beam-Propagation Method). Модель учитывает паралельно одновременную эволюцию пучка с основной частотой и генерированной второй гармоникой. Нумерический алгоритм основан на разделении одновременно проходящих явлений распространения волн и нелинейной компенсации фазы и амплитуды. Эти два явления моделируются как проходящие на перемену. Представлено математические основы нового метода. Метод можно легко обобщит для случая генерации второй гармоники в оптоводах выполненных на материалах поглощающих или усиливающих свет. Этим методом можно проводить анализ других нелинейных процессов в оптоводах как самомодуляция фазы и перекрестная модуляция фазы.

Marian Marciniak

MODELAGE D'UNE GENERATION DE LA DEUXIEME HARMONIQUE EN GUIDES D'ONDE OPTIQUES AVEC LA METHODE DE LA PROPAGATION DE DEUX FAISCEAU

R é s u m é

Un algorithme d'une nouvelle méthode de modelage d'une génération de la deuxième harmonique dans les guides d'ondes optiques planaires avec la méthode de la propagation de deux faisceau 2-BPM (Two-Beam-Propagation Method). Le modèle prends à la fois en considération l'evolution du faisceau de la fréquence de base ainsi que celle de deuxième harmonique. L'algorithme numérique consiste sur la séparation des effets qui ont lieu simultanement voir la propagation ainsi que la compensation nonlinéaire de la phase et de l'amplitude qui sont modelés comme ayant lieu altérnativement. Les bases de mathématique de cette méthode nouvelle sont présentées. La méthode peut être facilement généralisée pour le cas de la génération de la deuxième harmonique dans les guides d'ondes réalisés de milieu d'affaiblissant ou

amplifiant la lumière. Avec la méthode décrite on peut analyser aussi les processus optiques nonlineaires dans guides d'ondes par exemple automodulation de phase ainsi que la modulation croisée de phase.

Marian Marciniak

ERZEUGUNGSMODELLIERUNG DER ZWEITEN HARMONISCHEN IN LICHTWELLENLEITER ANHAND ZWEIBÜNDELSPROPAGATIONSMETHODE

Z u s a m m e n f a s s u n g

Ein neuer Zweibündelspropagationsmethode-Algorithmus für Simulation der Erzeugung der zweiten Harmonischen in Planarlichtwellenleiter wird vorgestellt. Im Modell wird es simultane Bündelevolution der ersten und der zweiten Harmonischen in Betracht gezogen. Physisch besteht der Modell in Separation der zwei Schrittes: der Propagationsseparation und der nichtlinearen Phase- und Amplitudekompenstionsseparation. Mathematische Grundlagen der neuen Methode werden behandelt und einige der Spezialeigenschaften diskutiert. Verallgemeinert werden kann die vorgestellte Methode leicht auf Untersuchung der Generationssprozesse der zweiten Harmonischen in Lichtwellenleiter, die aus dem Licht verstärkende oder dämpfende Medium gemacht werden. Auch auf andere nonlineare Welleninteraktionen wie Self- und Kreuzphasenmodulation kann es mit dieser Methode eingegangen werden.

Lech Smoczyński
Marian Marciniak

621.391.631.2

ŚWIATŁOWODOWE LINIE DO TRANSMISJI FAL MILIMETROWYCH

Omówiono obecne tendencje w rozwoju światłowodowych linii do transmisji sygnałów radiowych, polegające na stosowaniu coraz wyższych częstotliwości mikrofalowych. Przedstawiono specyficzne problemy światłowodowej transmisji fal milimetrowych oraz podano przykłady najnowszych osiągnięć w dziedzinie optycznych metod ich generacji i transmisji.

1. WSTĘP

Udoskonalone szybkie techniki modulacji bezpośredniej źródeł światła oraz modulacji zewnętrznej umożliwiają wykorzystanie znakomitych parametrów transmisyjnych światłowodów, takich jak: niskie tłumienie, szerokie pasmo transmisyjne, brak przesłuchów oraz niewrażliwość na zakłócenia elektromagnetyczne w transmisji mikrofal i fal milimetrowych. Transmisja sygnału mikrofalowego za pośrednictwem zmodulowanej fali optycznej w światłowodzie umożliwia znaczne oddalenie źródeł lub detektorów promieniowania mikrofalowego od miejsc generacji lub obróbki sygnału mikrofalowego. Umożliwia to koncentrację urządzeń elektronicznych w jednym miejscu (pomieszczeniu), pożądaną w środowisku nieprzyjaznym lub w warunkach wielkomiejskich.

Światłowodowa transmisja fal mikrofalowych i milimetrowych znajduje zastosowanie w dynamicznie rozwijającej się telefonii komórkowej, wymagającej gęstej sieci anten nadawczo-odbiorczych

sygnału radiowego, oraz w łączach naziemnych systemów łączności satelitarnej. Postęp w technologii laserów półprzewodnikowych umożliwił rozpowszechnienie się światłowodowych systemów ze zwielokrotnieniem na podnośnych (*subcarrier multiplexing - SCM*). W systemach SCM są przesyłane sygnały cyfrowe i analogowe w kanałach o różnych częstotliwościach podnośnych, modulujących amplitudowo optyczną falę nośną. Transmisja jest zwykle realizowana za pomocą laserów DFB w zakresie długości fali 1310 nm lub 1550 nm. Łącza takie znajdują zastosowanie w magistralach sieci telewizji kablowej CATV i w systemach HFC (*hybrid fiber - coaxial*), które umożliwiają przesyłanie sygnałów kanałów CATV razem z dodatkowymi usługami multimedialnymi [2, 9]. Częstotliwości podnośnych w systemach HFC sięgają prawie do 1 GHz, co wiąże się z pasmem przenoszenia kabli współosiowych.

W światłowodowych liniach, służących do przesyłania sygnałów z anten satelitarnych są stosowane częstotliwości podnośnych z zakresu wyższych częstotliwości mikrofalowych [1]. Ostatnio obserwuje się znaczny wzrost zainteresowania światłowodową transmisją mikrofal, związany z rozwojem telekomunikacji ruchomej [8, 11]. Stały wzrost liczby użytkowników sieci telefonii komórkowej wymaga przejścia do tzw. sieci mikrokomórkowych, które zapewniają efektywne wykorzystanie pasma częstotliwości.

W systemie mikrokomórkowym centralna stacja bazowa (C-BS) obsługuje znaczną liczbę mikrokomórek, z których każda jest wyposażona w port antenowy, zainstalowany w stacji mikrobazowej (M-BS). Ze względu na koszty dużej liczby M-BS ich wyposażenie musi być możliwie proste. Linie światłowodowe mogą być wykorzystywane do transmisji sygnałów mikrofalowych ze stacji centralnej C-BS do M-BS. Optyczna sieć rozprowadzająca zapewnia szerokie pasmo, małe straty oraz odporność na zakłócenia elektromagnetyczne. Generacja sygnałów w. cz. odbywa się w stacji centralnej C-BS;

koszty jej wyposażenia rozkładają się na wiele portów antenowych, a wyposażenie stacji M-BS znacznie się upraszcza.

Przyszły rozwój telekomunikacji ruchomej będzie prowadził do bezprzewodowego dostarczania użytkownikom sieci komórkowej, również usług multimedialnych, radiowy dostęp będzie zaś wykorzystywany do dostarczania usług wideo abonentom stacjonarnym. Jednakże pasma częstotliwości w zakresie od UHF do dolnych częstotliwości mikrofalowych są obecnie bardzo eksploatowane. Znacznie więcej wolnych kanałów jest jeszcze w zakresie fal milimetrowych, co stwarza realne możliwości wykorzystania tego zakresu do bezprzewodowego przesyłania usług szerokopasmowych. Światłowodowe linie, służące do rozprowadzania fal milimetrowych przenoszących usługi szerokopasmowe znajdą zastosowanie w tych przyszłych sieciach [10].

2. ZAKRESY CZĘSTOTLIWOŚCI MIKROFALOWYCH, PRZEZNACZONE DLA BEZPRZEWODOWEJ SIECI SZEROKOPASMOWEJ

Bezprzewodowy, o dużej przepływności dostęp do Internetu oraz usługi multimedialne dostarczane odbiorcom ruchomym będą głównymi stymulatorami przyszłego rozwoju sieci bezprzewodowych. Obecnie nie ma jeszcze ostatecznie zaaprobowanych standardów sieci bezprzewodowej do efektywnego przesyłania usług szerokopasmowych [5]. Oczekuje się jednak, że w bezprzewodowej sieci szerokopasmowej będą stosowane nowe systemy działające w pasmach częstotliwości powyżej 3 GHz.

W krajach Unii Europejskiej (w obrębie programu ACTS) prowadzi się badania nad bezprzewodowymi systemami szerokopasmowymi w pasmach: 5, 17, 40 i 60 GHz. W Stanach Zjednoczonych realizuje się projekty badawcze dotyczące wykorzystania w sieci szeroko-

pasmowej zakresów częstotliwości 5 GHz i 60 GHz, a w Japonii prowadzi się badania nad systemami w pasmach: 10÷16 GHz, 19 GHz i 60 GHz. W tej sytuacji światłowodowe linie wykorzystywane do transmisji sygnałów mikrofalowych w wymienionych zakresach częstotliwości stały się przedmiotem znacznego zainteresowania laboratoriów i producentów urządzeń. Światłowodowe linie do transmisji mikrofal mogą również znaleźć zastosowanie w systemach monitorowania i sterowania ruchem na autostradach. Unia Europejska zaleciła swoim członkom wykorzystanie do tego celu pasm: 63÷64 GHz oraz 76÷77 GHz [10]. Do rozprowadzania fal milimetrowych mogą być wykorzystane w tym przypadku jednokierunkowe linie światłowodowe.

3. SPECYFICZNE PROBLEMY ŚWIATŁOWODOWEJ TRANSMISJI FAL MILIMETROWYCH

Światłowodowa transmisja w zakresie niższych częstotliwości mikrofalowych (rzędu kilku GHz) obecnie nie przedstawia większych trudności. Odpowiednie wymagania spełniają systemy dostępne na rynku.

W zakresie wyższych częstotliwości mikrofalowych, a zwłaszcza w zakresie fal milimetrowych ($f > 30$ GHz) pojawia się wiele trudności, które muszą być przezwyciężone. Wynikają one z funkcjonowania różnych bloków kanału optycznego.

Głównym problemem jest zaprojektowanie i wykonanie odpowiednich nadajników. Można z pewnością stwierdzić, że rozpowszechnienie się światłowodowych linii do transmisji fal milimetrowych w przyszłych bezprzewodowych sieciach szerokopasmowych będzie uwarunkowane dostępnością tanich nadajników optycznych. Wprawdzie, za pomocą bezpośredniej modulacji lasera MQW (*multi quantum well*) można zrealizować nadajnik działający w pasmie do 30 GHz, jednak perspektywy zwiększenia częstotliwości modulacji bezpośredniej są mierne. Zastosowanie zewnętrznej modulacji sygnału

optycznego z lasera umożliwia rozszerzenie pasma modulacji nawet do 75 GHz. Zewnętrzne modulatory szerokopasmowe są jednak drogie, wnoszą duże straty optyczne i wymagają dużego napięcia sterującego, co stwarza znaczną trudność w odniesieniu do źródeł sygnałów milimetrowych. W związku z tym można zaobserwować duże zainteresowanie nowymi metodami generacji sygnału optycznego modulowanego falami milimetrowymi [3]. Szczególnie są interesujące optyczne metody generacji i dystrybucji fal milimetrowych, które polegają, np. na mieszaniu dwóch sygnałów laserowych o odpowiednim odstępie częstotliwości. Metody takie będą głównym tematem rozważań dalszej części artykułu.

Dodatkowe trudności wiążą się z wpływem dyspersji chromatycznej i dyspersji polaryzacyjnej światłowodu na transmisję sygnałów optycznych modulowanych falami milimetrowymi. Istotnym problemem jest również detekcja sygnału optycznego zmodulowanego sygnałem bardzo wysokiej częstotliwości. Wprawdzie fotodetektory o pasmie przenoszenia do 100 GHz były demonstrowane, jednakże dostępność odpowiednio tanich detektorów szerokopasmowych będzie miała istotny wpływ na rozpowszechnianie się zastosowań światłowodowych linii do transmisji fal milimetrowych.

4. OPTYCZNE METODY GENERACJI FAL MILIMETROWYCH

Optyczne metody generacji fal milimetrowych można podzielić na dwie grupy:

- metody wykorzystujące dwa źródła laserowe, których sygnały wyjściowe są koherentnie mieszane; różnica częstotliwości dwóch sygnałów laserowych odpowiada pożądanej częstotliwości fal milimetrowych;
- metody wykorzystujące jedno źródło optyczne do generacji fal milimetrowych.

Najprostsza realizacja nadajnika pierwszej grupy wykorzystuje zdudnianie sygnałów uzyskanych z dwóch laserów na fotodiodzie p-i-n. Pole elektryczne zdudnianych sygnałów optycznych w funkcji czasu można zapisać jako:

$$E_1(t) = E_{01} \cos\left(2\pi f_1 t\right), \tag{1}$$

$$E_2(t) = E_{02} \cos\left(2\pi f_2 t\right). \tag{2}$$

Jeżeli sygnały te zostaną zsumowane na powierzchni czynnej fotodiody p-i-n, wówczas prąd fotodiody będzie zawierał między innymi składową:

$$I_f(t) \approx E_{01} E_{02} \cos\left[2\pi\left(f_1 - f_2\right)t\right]. \tag{3}$$

Przez odpowiedni dobór różnicy częstotliwości f_1 i f_2 można więc uzyskać generację sygnału milimetrowego o pożądanej częstotliwości. Modulację sygnału milimetrowego sygnałem użytecznym otrzymuje się przez uprzednie zmodulowanie jednego z sygnałów optycznych sygnałem przenoszącym informację, na przykład:

$$E_1(t) = m(t)\, E_{01} \cos\left(2\pi f_1 t\right). \tag{4}$$

W tej sytuacji prąd fotodiody będzie zawierał składową:

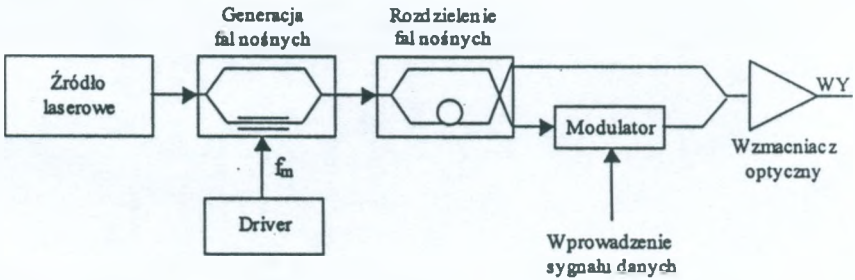
$$I_f \approx E_{01} E_{02} m(t) \cos\left[2\pi\left(f_1 - f_2\right)t\right]. \tag{5}$$

Sygnał użyteczny $m(t)$ może stanowić zbiór różnych częstotliwości podnośnych i wówczas prąd fotodiody będzie zawierał składową nośną o częstotliwości $(f_1\text{-}f_2)$ oraz symetryczne wstęgi boczne złożone z podnośnych.

W praktyce jednak sygnał fal milimetrowych otrzymany opisaną metodą zdudniania dwóch sygnałów optycznych cechuje duża zawar-

tość szumów, spowodowana znacznymi szumami fazowymi laserów. Do uzyskania sygnału fal milimetrowych o wymaganych do transmisji parametrach jest niezbędne zastosowanie synchronizacji obydwu laserów. Do tego celu służą pętle automatycznej regulacji częstotliwości, optoelektroniczne pętle fazowe itp.

Inne sposoby poprawy koherencji fazowej zdudnianych sygnałów optycznych polegają na otrzymywaniu tych sygnałów z jednego źródła optycznego. Przykładem takiego rozwiązania jest metoda samozdudniania (*self-heterodyning*). Na rys. 1 przedstawiono schemat dwuprążkowego źródła optycznego działającego na zasadzie samozdudniania [4].



Rys. 1. Schemat ilustrujący działanie optycznego źródła dwuprążkowego

Sygnał fali ciągłej z lasera jednomodowego jest modulowany za pomocą modulatora Macha-Zehndera sygnałem mikrofalowym o częstotliwości f_m. Sygnał optyczny w funkcji czasu na wyjściu modulatora można zapisać następująco:

$$E(t) = E_o \cos\left[\beta \frac{\pi}{2} + \alpha \frac{\pi}{2} \cos(\omega_m t)\right] \cos(\omega_0 t), \qquad (6)$$

gdzie: ω_0 - częstotliwość kołowa sygnału optycznego z lasera,

$$\omega_m = 2\pi f_m$$

$\alpha = \frac{d_m}{V\pi}$ - znormalizowana amplituda sygnału drivera,

$\beta = \frac{U_b}{V\pi}$ - znormalizowany punkt pracy modulatora spolaryzowanego napięciem stałym U_b.

$E(t)$ może być wyrażone za pomocą funkcji Bessela:

$$\begin{aligned} E(t) = E_0 \Bigg\{ & J_0\left(\alpha\frac{\pi}{2}\right)\cos\left(\beta\frac{\pi}{2}\right)\cos(\omega_0 t) + \\ & - J_1\left(\alpha\frac{\pi}{2}\right)\sin\left(\beta\frac{\pi}{2}\right)\cdot \\ & \cdot\left[\cos(\omega_0 - \omega_m)t + \cos(\omega_0 + \omega_m)t\right] + \\ & - J_2\left(\alpha\frac{\pi}{2}\right)\cos\left(\beta\frac{\pi}{2}\right)\cdot \\ & \cdot\left[\cos(\omega_0 - 2\omega_m)t + \cos(\omega_0 + 2\omega_m)t\right] + \ldots \Bigg\} . \end{aligned} \tag{7}$$

Dobierając odpowiednio napięcie polaryzacji modulatora Macha-Zendera można uzyskać $\beta = 1$ i wówczas znikają wszystkie wyrazy parzyste. W rezultacie na wyjściu modulatora otrzymuje się dwa prążki boczne oddalone o $\pm\omega_m$ od środkowej częstotliwości optycznej ω_0, przy całkowitym stłumieniu nośnej optycznej ω_0. Uzyskuje się w ten sposób źródło dwóch koherentnych sygnałów optycznych o częstotliwościach różniących się o $2f_m$. Otrzymane na wyjściu modulatora Macha-Zendera sygnały optyczne zostają następnie rozdzielone za pomocą filtru - również w postaci interferometru Macha-Zendera - dzięki temu jeden z nich może być zmodulowany sygnałem użytecznym. Dobierając odpowiednio częstotliwość f_m otrzymuje się optyczne źródło dwuprążkowe z odstępem równym pożądanej często-

tliwości z pasma fal milimetrowych. Obydwa sygnały optyczne mogą być przesłane światłowodem do oddalonej stacji bazowej, w której zostaną zdudnione w szerokopasmowym fotodetektorze, a otrzymany sygnał fali milimetrowej będzie niósł wysłaną informację użyteczną. Istotną zaletą tej metody jest modulowanie sygnału optycznego przez driver na częstotliwości równej połowie częstotliwości sygnału emitowanego przez antenę stacji bazowej.

Do grupy metod wykorzystujących jedno źródło optyczne do generacji fal milimetrowych należy również metoda zdudniania sygnałów z lasera dwumodowego [7]. Stosuje się w niej filtr optyczny do selekcji tylko dwóch modów lasera impulsowego, których częstotliwości różnią się o wartość częstotliwości fal milimetrowych. Inna modyfikacja tej metody polega na wykorzystaniu specjalnie skonstruowanych laserów dwumodowych. Mody lasera dwumodowego są synchronizowane w elektronicznej pętli fazowej [12]. Laser dwumodowy jest wielosekcyjnym laserem DFB, w którym uzyskuje się generację dwóch modów o częstotliwościach położonych symetrycznie po obu stronach częstotliwości Bragga.

5. WPŁYW DYSPERSJI CHROMATYCZNEJ I POLARYZACYJNEJ NA PRACĘ ŚWIATŁOWODOWYCH LINII DO TRANSMISJI FAL MILIMETROWYCH

Ponieważ obydwa sygnały optyczne o częstotliwościach różniących się o $2f_m$ pochodzą z jednego źródła o szerokości linii $\Delta\nu$, szumy fazowe tych sygnałów są całkowicie skorelowane i sygnał milimetrowy, otrzymany z fotodetektora p-i-n bezpośrednio na wyjściu źródła dwuprążkowego, ma małą szerokość linii. W praktycznych zastosowaniach sygnały te są przesyłane razem, jednym światłowodem do fotodetektora w oddalonej stacji bazowej i dopiero tam

zdudniane. Względne opóźnienie sygnałów optycznych spowodowane dyspersją chromatyczną może pogorszyć korelacje odbieranych przez fotodetektor bazowej stacji sygnałów, co wywołuje poszerzenie linii sygnału elektrycznego fali milimetrowej i pogorszenie bilansu mocy.

Szkodliwy wpływ na transmisję fal milimetrowych światłowodową linią, działającą na zasadzie zdudniania dwóch sygnałów optycznych, ma także dyspersja polaryzacyjna (*polarization mode dispersion - PMD*). Moc sygnału milimetrowego otrzymanego po zdudnieniu zależy od względnego stanu polaryzacji sygnałów optycznych. Niedopasowanie polaryzacji powoduje pogorszenie bilansu mocy sygnału fal milimetrowych.

W praktycznej realizacji światłowodowej linii dyspersja polaryzacyjna PMD zmienia się przypadkowo w czasie i w zależności od długości fali, np. na skutek wpływu temperatury na dwójłomność światłowodu. W związku z tym w dokładnej analizie wpływu PMD na transmisję muszą być uwzględnione zmiany rozkładów statystycznych PMD.

Badania szkodliwego wpływu dyspersji chromatycznej i dyspersji polaryzacyjnej na transmisję sygnałów fal milimetrowych w systemach wykorzystujących samozdudnianie były prowadzone w trakcie realizacji europejskiego projektu RACE 2005 MODAL (*microwave optical duplex antenna link*) [4]. Z badań tych wynika, że na transmisję fal milimetrowych w pasmie 30÷60 GHz dominujący wpływ ma dyspersja polaryzacyjna PMD. Wpływ dyspersji chromatycznej w światłowodzie standardowym (D = 17 ps/nm · km) na transmisję sygnału 30 GHz przenoszonego na długości fali λ = 1,55 μm powoduje pogorszenie bilansu mocy < 0,25 dB przy długości linii 100 km. W przypadku dyspersji polaryzacyjnej pogorszenie bilansu mocy dla transmisji fal milimetrowych o częstotliwości 60 GHz wynosiło ~ 2 dB dla linii długości 20 km.

6. PRZYKŁADY EKSPERYMENTALNYCH ŚWIATŁOWODOWYCH SYSTEMÓW TRANSMISJI FAL MILIMETROWYCH

Opisane nowe optyczne metody generacji i transmisji fal milimetrowych zastosowano w doświadczalnych systemach światłowodowej transmisji sygnałów radiowych (*radio over fibre*). Metoda samozdudniania została wykorzystana do generacji i transmisji sygnału 36 GHz zmodulowanego w formacie DPSK (*differential phase shift keying*) z przepływnością 140 Mbit/s, za pomocą światłowodowych linii długości 25 km, do 1600 stacji bazowych [4]. Po transmisji w światłowodowej linii, a następnie w wolnej przestrzeni, detekcji i demodulacji stopa błędów nie przekraczała 10^{-9}.

W celu zademonstrowania (w czasie projektu RACE 2005 Modal) przydatności metody samozdudniania do transmisji dwukierunkowej przeprowadzono eksperyment w pełni dupleksowej transmisji fal milimetrowych. W optycznej linii przenoszącej sygnał 30 GHz na długości fali 1550 nm w dół, zrealizowano również kanał zwrotny do przesyłania sygnału 1,8 GHz na długości fali 1300 nm. W stacji centralnej jeden z dwóch sygnałów optycznych ze źródła dwuprążkowego (z odstępem między prążkami 30 GHz) był modulowany amplitudowo sygnałem podnośnej 1,5 GHz, który z kolei został zmodulowany cyfrowo w formacie ASK z przepływnością 2 Mbit/s.

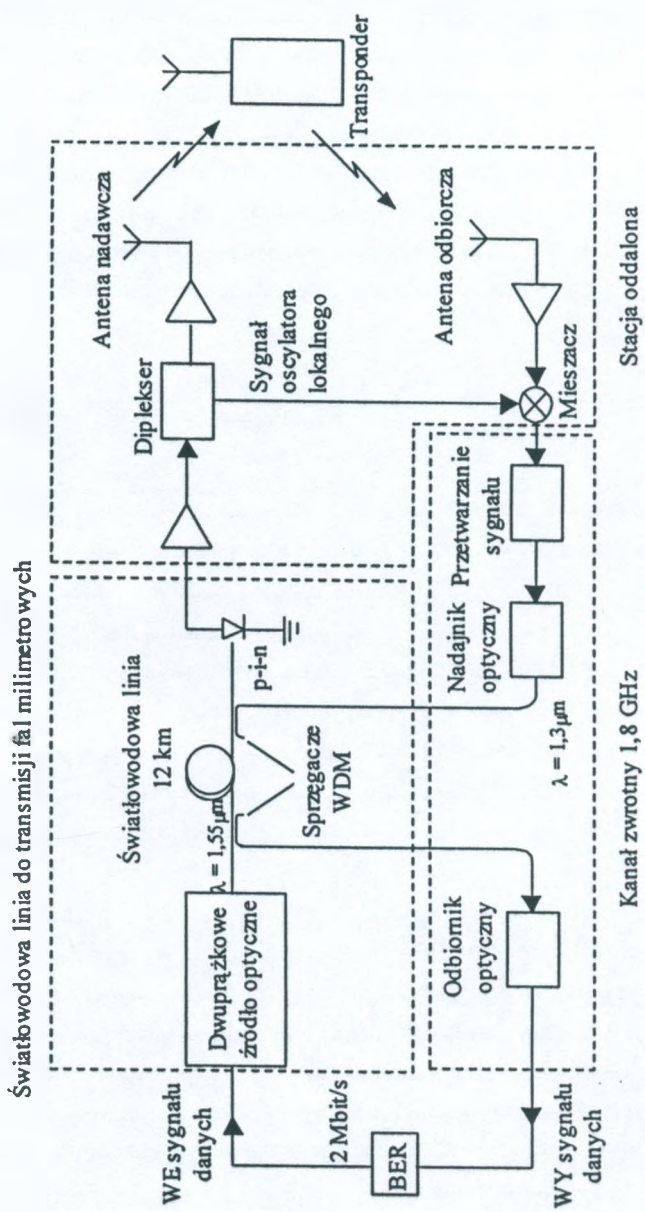
Po transmisji na odległość 12 km standardowym światłowodem jednomodowym sygnały optyczne były zdudniane za pomocą fotodiody p-i-n. Z fotodiodą był zintegrowany wzmacniacz wyposażony w diplekser, który służył do wydzielenia jednej ze wstęg bocznych. Sygnał o częstotliwości 31,5 GHz otrzymany na wyjściu dipleksera był emitowany za pomocą anteny stożkowej. Sygnał milimetrowy, odebrany przez transponder po transmisji w wolnej przestrzeni, był przemieniany w dół na częstotliwość 1,8 GHz, z wykorzystaniem

odtworzonego sygnału 30 GHz jako oscylatora lokalnego. Sygnał o częstotliwości pośredniej 1,8 GHz modulował następnie laser 1300 nm, pełniący rolę nadajnika w kanale zwrotnym. Transmisja na jednym światłowodzie w obydwu kierunkach była możliwa dzięki zastosowaniu sprzęgacza WDM 1,3/1,55 μm. Na rys. 2 przedstawiono schemat ideowy eksperymentu [4].

Eksperymentalną dystrybucję sygnałów wideo i danych zademonstrowano za pomocą światłowodowego systemu transmisji fal milimetrowych, wyposażonego w nadajnik z laserem półprzewodnikowym synchronizowanym hybrydowo [6]. Zastosowany laser zbudowano z pięciu sekcji: dwu sekcji wzmacniania, nasycalnego absorbera, sekcji DBR i sekcji sterowania fazy (PC). Sekcje wzmocnienia zasilano prądem stałym, odpowiednio 43 mA i 94 mA, natomiast sekcje DBR i PC nie były obciążone.

Gdy również sekcja absorbera nie była zasilana napięciem stałym, laser pracował w trybie pasywnej synchronizacji modów, generując ciąg impulsów o częstotliwości powtarzania 37 GHz. Sygnał wyjściowy zawierał wówczas duże szumy amplitudowe i fazowe. Doprowadzenie do sekcji absorbera sygnału zewnętrznego o częstotliwości 37 GHz i amplitudzie +4 dBm powodowało synchronizację lasera tym sygnałem, dzięki czemu szumy fazowe zostały zredukowane do poziomu -85 dBc/Hz przy częstotliwości offsetu 10 kHz. Taki tryb pracy lasera impulsowego, nazywany hybrydową synchronizacją modów, jest obecnie coraz częściej wykorzystywany w optycznych generatorach fal milimetrowych.

Do równoczesnej transmisji analogowych sygnałów wideo i cyfrowych sygnałów danych wykorzystano zwielokrotnienie SCM. Trzy kanały wideo przesyłano na częstotliwości podnośnej 1 GHz, a strumień danych cyfrowych 200 Mbit/s NRZ na podnośnej 2,5 GHz. Zsumowany sygnał obydwu podnośnych był wzmacniany, a następnie modulował sygnał lasera z hybrydową synchronizacją modów za



Rys. 2. Topologia doświadczalnej instalacji do dwukierunkowej światłowodowej transmisji fal milimetrowych

pośrednictwem elektrooptycznego modulatora Macha-Zendera. Zmodulowany sygnał optyczny przesyłano za pomocą standardowego światłowodu jednomodowego na odległość 10 km. Na końcu światłowodowej linii sygnał optyczny odbierano przez fotodetektor szerokopasmowy o szerokości pasma 45 GHz. Otrzymany z fotodetektora sygnał SCM wzmacniano oraz rozdzielano na składowe wideo i składową danych. Stopa błędów sygnału cyfrowego nie przekraczała 10^{-9}, a ważony stosunek sygnału do szumów dla kanałów wideo wynosił 43,4 dB.

7. PODSUMOWANIE

W związku z przewidywanym rozwojem telefonii komórkowej oraz sieci bezprzewodowych dostarczających szerokopasmowe usługi multimedialne będą potrzebne światłowodowe linie *„radio over fibre"* do rozprowadzania sygnałów do mikrokomórkowych stacji bazowych. Szczególnie będą pożądane światłowodowe linie do transmisji wyższych częstotliwości mikrofalowych i fal milimetrowych. W przypadku transmisji fal milimetrowych występuje jeszcze wiele problemów technicznych, które muszą być rozwiązane, zanim systemy optyczne dla tych zakresów częstotliwości osiągną pełną dojrzałość.

Obecnie prowadzi się intensywne badania nad optycznymi metodami generacji i transmisji sygnałów milimetrowych. W eksperymentalnych systemach wykorzystujących optyczne metody generacji fal milimetrowych uzyskano już parametry odpowiadające wymaganiom przyszłych sieci szerokopasmowych.

W najbliższej przyszłości należy oczekiwać szybkiego doskonalenia źródeł optycznych, które zapewnią powszechną dostępność ekonomicznych nadajników.

WYKAZ LITERATURY

1. Bowers J.E., Chipaloski A.C., Boodaghians S.: Long distance fiber-optic transmission of C-band microwave signals to and from a satellite antenna. J. Lightwave Technol., Vol. 5, 1987, pp. 1733-1741.
2. Chiddix J.A., David H.L., Pangrac M., Williamson L.D., Wolfe R.W.: AM video on fiber in CATV systems: need and implementations. IEEE J. Select. Areas Commun., Vol. 8, 1990, pp. 1229-1239.
3. Georges J.B., Cutrer D.M., Solgaard O., Lau K.Y.: Optical transmission of narrowband millimeter-wave signals. IEEE Trans. Microwave Theory and Techn., Vol. 43, No. 9, 1995, pp. 2229-2240.
4. Hofsteter R., Schmuck H., Heidemann R.: Dispersion effects in optical millimeter-wave systems using self-heterodyne method for transport and generation. IEEE Trans. Microwave Theory and Techn., Vol. 43, No. 9, 1995, pp. 2263-2269.
5. Mikkonen J., Corrado C., Evici C., Progler M.: Emerging wireless broadband networks. IEEE Commun. Magazine, February 1998, pp. 112-117.
6. Novak D., Ahmed Z., Liu H.F.: SCM millimeter-wave optical transport system for data and video signal distribution. W: Trends in Optic and Photonic, Vol. 12, pp. 468-471, edited by Wikers A.E. and Menyuk C.R., Optical Society of America, 1997.
7. Novak D., Ahmed Z., Waterhouse B., Tucker R.S.: Signal generation using pulsed semiconductor lasers for application in millimeter-wave wireless links. IEEE Trans. Microwave Theory and Techn., Vol. 43, No. 9, 1995, pp. 2257-2276.
8. Ohamoto R., Othuska H., Idukawa H.: Fiber-optic microcell systems with a spectrum delivery scheme. IEEE J. Select. Areas Commun., Vol. 11, 1993, pp. 1108-1117.
9. Olshansky R., Lanzisera V.A., Hill P.M.: Subcarrier multiplexed lightwave systems for broadband distribution. IEEE J. Lightwave Technol., Vol. 7, 1989, pp. 1329-1342.
10. O'Reilly J., Lane P.: Remote delivery of video services using mm-waves and optics, IEEE J. Lightwave Technol., Vol. 12, 1994, pp. 369-375.
11. Shibutami M., Kanai T., Domou W., Esmura K.: Optical fiber feeder for microcellular mobile communications systems (H-015). IEEE J. Select. Areas Commun., Vol. 11, 1993, pp. 1118-1126.

12. Wake D., Lima C.R., Davies A.: Optical generation of millimeter-wave signals for fiber-radio systems using dual-mode DFB semiconductor lasers. IEEE Trans. Microwave Theory and Techn., Vol. 43, No. 9, 1995, pp. 2270-2276.

Лех Смочиньски
Марян Марциняк

ЛИНИИ ПЕРЕДАЧИ МИЛЛИМЕТРОВЫХ ВОЛН НА СВЕТОВОДАХ

Резюме

Рассмотрено актуальные тренды развития линий передачи радиоволн, состоящие в применении все более высоких частот СВЧ диапазона. Приводятся специфические проблеммы передачи миллиметровых волн по светово дам а также описание новых достижений в области оптических методов их генерации и передачи.

Lech Smoczyński
Marian Marciniak

FIBRE OPTIC LINKS FOR MILLIMETER-WAVE SIGNAL TRANSMISSION

Summary

There is recent increase of interest in regard of radio over fibre transmission. Actual trends of moving of the microwave carriers to the higher frequences are discussed. Specific problems of the millimeter-wave transmission over fibre and recent examples of optical methods of millimeter-wave generation and transmission are presented.

Lech Smoczyński
Marian Marciniak

LES LIGNES DE FIBRES OPTIQUES POUR UNE TRANSMISSION DES ONDES MILLIMETRIQUES

Résumé

Les tendences actuelles en développement des lignes optiques pour la transmission des signaux de radio qui consiste en utilisation des plus en plus houtes fréquences de microondes sont décrits dans cet article. On a présenté les problèmes spécifiques de la transmission optique des ondes millimétriques ainsi que les exemples des réalisations les plus recents dans le domaine de méthodes optiques utilisées pour les générer et pour les transmettre.

Lech Smoczyński
Marian Marciniak

GLASFASERLEITUNGEN FÜR ÜBERTRAGUNG DER MILIMMETER-WELLEN

Zusammenfassung

Rasante technologische Entwicklung der Glasfaser-Anwendungen für Übertragung in immer höheren Frequenzen wird vermittelt. Die Autoren geben einen Einblick in spezifische Probleme der Milimeterwellenübertragung über Glasfaser und stellen letzte Beispiele der optischen Milimeterwellenerzeugung-Methoden dar.

KOMUNIKAT

Tomasz Kossek
Anna Warzec

681.2.089.002.56:
:621.39:621.317.004.5

SYSTEM EWIDENCJI I NADZORU METROLOGICZNEGO NAD WZORCAMI ORAZ APARATURĄ KONTROLNO-POMIAROWĄ INSTYTUTU ŁĄCZNOŚCI

W komunikacie przedstawiono propozycję zarządzania przyrządami pomiarowymi, zgodną z wymaganiami systemu jakości wprowadzonego w Instytucie Łączności. Opisano sposób nadzoru, ewidencji i propozycję podziału przyrządów pomiarowych. Omówiono też konkretną realizację komputerowej bazy danych, utworzoną w środowisku Microsoft Access.

1. WPROWADZENIE

W Instytucie Łączności utworzono dwa laboratoria: Laboratorium Metrologii Elektrycznej, Elektronicznej i Optoelektronicznej (LMEEiO) oraz Laboratorium Badań i Homologacji Urządzeń Telekomunikacyjnych (LBHUT).

Laboratorium Metrologii Elektrycznej, Elektronicznej i Optoelektronicznej dokonuje wzorcowania aparatury kontrolno-pomiarowej Instytutu i klientów z zewnątrz oraz wystawia świadectwa wzorcowania tego sprzętu. Natomiast Laboratorium Badań i Homologacji Urządzeń Telekomunikacyjnych zajmuje się badaniem urządzeń telekomunikacyjnych oraz sprawdzaniem zgodności ich parametrów z wymaganiami krajowymi [7,8]. W LMEEiO oraz LBHUT znajduje się ok. 500 przyrządów pomiarowych i innych urządzeń, które są wykorzystywane w procesie homologacji oraz wzorcowania.

W celu zdobycia i utrzymania zaufania odbiorców wprowadzono w laboratoriach system jakości oraz ustanowiono Księgi Jakości i Procedury Systemowe, jako dokumenty opisujące system jakości. Zarządzanie przyrządami pomiarowymi jest elementem systemu zapewnienia jakości i obejmuje dobór przyrządów pomiarowych oraz nadzór nad nimi.

Zgodnie z przewodnikiem ISO/IEC 25 pt. "Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i pomiarowych" [5, pkt 5.5]:

- laboratorium powinno być wyposażone we wszystkie elementy niezbędne do realizacji pomiarów wymaganych do prawidłowego przeprowadzania badań lub wzorcowań (pkt 5.5.1);
- wyposażenie powinno zapewniać wymaganą dokładność oraz spełniać odnośne specyfikacje dotyczące badań lub wzorcowań (pkt 5.5.2);
- wyposażenie powinno być obsługiwane przez kompetentny i upoważniony personel (pkt 5.5.4);
- dla każdego obiektu wyposażenia, istotnego do wykonywanych badań lub wzorcowań, należy prowadzić i utrzymywać zapisy (pkt 5.5.6);
- wyposażenie powinno być regularnie konserwowane (pkt 5.5.7).

Zaistniała więc konieczność prowadzenia kartotek wyposażenia pomiarowego. Prowadzenie kartotek "papierowych" jest bardzo pracochłonne i niewygodne, chociażby ze względu na brak możliwości całościowej oceny systemu nadzoru nad wyposażeniem, a wyszukiwanie danych jest szczególnie kłopotliwe, gdy kartoteki znajdują się w wielu zespołach. Wprowadzenie komputerowego systemu ewidencji i nadzoru metrologicznego nad wzorcami oraz aparaturą kontrolno-pomiarową Instytutu Łączności umożliwiło ujednolicenie i unowocześnienie sposobu gromadzenia, przechowywania, aktualizacji, przeszukiwania i przetwarzania danych o aparaturze

kontrolno-pomiarowej, a także nadzór nad nią według obowiązujących wymagań.

2. WYMAGANIA STAWIANE SYSTEMOWI ZARZĄDZANIA WYPOSAŻENIEM POMIAROWYM

Zgodnie z obowiązującymi normami i wymaganiami systemu jakości, musi być ustanowiony oraz utrzymywany skuteczny system zarządzania, potwierdzania i użytkowania wyposażenia pomiarowego. Konieczne jest też prowadzenie oraz utrzymywanie danych o wyposażeniu pomiarowym, czyli kartotek i rejestrów wyposażenia.

Zapisy te muszą zawierać co najmniej:

- identyfikację obiektu;
- nazwę producenta, oznaczenie typu oraz numer seryjny lub inne indywidualne oznaczenie;
- datę przyjęcia i datę włączenia do eksploatacji;
- aktualną lokalizację, gdy jest to potrzebne;
- stan w chwili przyjęcia;
- tytuły instrukcji producenta, jeżeli są dostępne;
- daty wykonanych wzorcowań oraz datę kolejnego wzorcowania;
- daty wykonanych konserwacji oraz datę kolejnej konserwacji;
- nazwiska osób odpowiedzialnych za stan techniczny wyposażenia;
- nazwiska osób upoważnionych do obsługi.

Komputerowy system zarządzania wyposażeniem pomiarowym powinien spełniać takie warunki, jak:

- łatwość obsługi;
- niezawodność pracy;
- wyświetlanie komunikatów w języku polskim;

- elastyczność, tj. możliwość łatwej rozbudowy i zmiany kryteriów wyszukiwania w zależności od potrzeb;
- możliwość szybkiego oraz niezawodnego dostępu do danych (tworzenie różnych form prezentacji danych według zadanych kryteriów, zestawień i raportów);
- możliwość uaktualniania danych;
- ograniczenie dostępu do komputera osobom nieupoważnionym, ustalenie poziomu zabezpieczenia danych przez identyfikację operatorów, sprawdzanie hasła, kontrolę uprawnień;
- możliwość archiwizacji danych (zapisy na dyskietkach);
- nadzór nad terminowością wzorcowań i konserwacji;
- kontrola niezawodności sprzętu;
- możliwość pracy w lokalnej sieci komputerowej laboratorium.

3. OPIS SYSTEMU

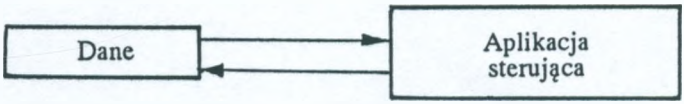
Komputerowy system ewidencji i zarządzania aparaturą kontrolno-pomiarową (ENWAK) utworzono wykorzystując program Microsoft Access, pracujący w systemie operacyjnym Windows 95. Taki program wybrano ponieważ, zarówno program jak i system operacyjny są znane i stosowane przez wielu użytkowników, co miałoby znaczenie przy udostępnianiu systemu ENWAK. Program Access umożliwia tworzenie relacyjnych baz danych, podobnie jak np. program dBase, daje on jednak dużo większe możliwości budowy interfejsu użytkownika, wykorzystując środowisko Windows 95. Ma także wiele narzędzi, które ułatwiają bardziej efektywne zarządzanie danymi.

Podstawowym sposobem uzyskania informacji z tabel, w których są gromadzone dane, jest kwerenda (zapytanie). Program Access umożliwia proste tworzenie kwerend za pomocą narzędzia QBE (*Query By Example*) oraz języka SQL (*Structure Query Language*).

Przy budowie interfejsu użytkownika nieodzownymi obiektami są formularze i raporty, które można zaprojektować według potrzeb wykorzystując dostępne obiekty, takie jak: pola wyboru, pola listy itp. Projektant bazy danych może modyfikować właściwości obiektów, a także dokonywać pewnych operacji dzięki zdefiniowanym dla nich metodom. Zarządzanie danymi i obiektami może odbywać się za pomocą makr lub procedur i funkcji napisanych w języku Access Basic, który okazuje się często niezastąpiony. Program Access umożliwia utworzenie systemu ochrony danych oraz dostępu do bazy w celu uniknięcia jej modyfikacji przez osoby do tego niepowołane.

3.1. Rozwiązanie techniczne systemu ENWAK

Komputerowy system ENWAK ma dwie bazy danych (rys. 1). Jedna zawiera jedynie tabele z danymi, a druga - aplikację sterującą, która pracuje na danych pochodzących z tabel. Takie rozwiązanie ma wiele zalet; przede wszystkim można tworzyć nowe wersje aplikacji sterującej i dołączać ją do istniejących danych.



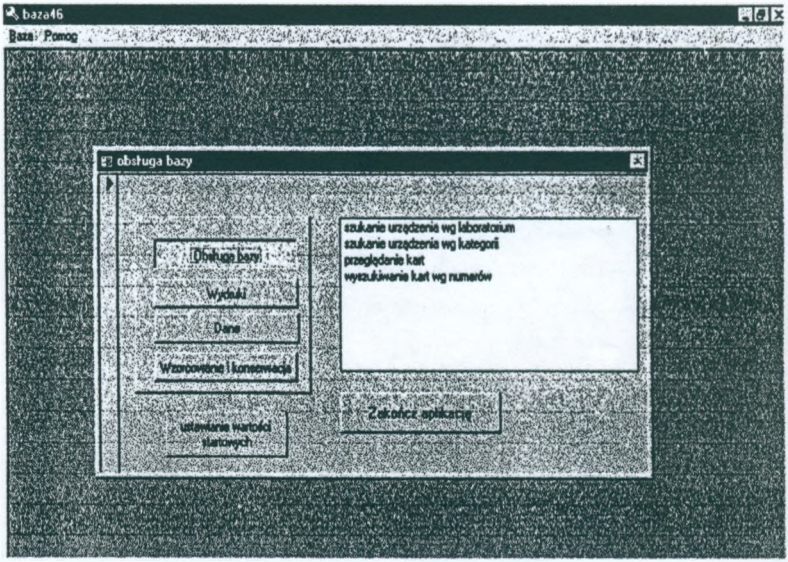
Rys. 1. Schematyczne przedstawienie struktury systemu ENWAK

Aby spełnić wymagania opisane w Księgach Jakości LMEEiO LBHUT, w zaprojektowanej bazie danych ENWAK utworzono tabele, mające przechowywać takie dane, jak:

- karta techniczna (dane identyfikacyjne i techniczne urządzeń);
- karta wzorcowania (dane dotyczące terminów wzorcowań);

- karta konserwacji (dane dotyczące terminów konserwacji);
- karta napraw (dane o naprawach).

Tabele są tak połączone, aby zawarte w nich dane były spójne - takie powiązanie w programie Access nazywa się relacją. Polem wiążącym jest numer "identyfikacyjny laboratorium", który dla tabeli "karta techniczna" stanowi klucz główny. Dla innych tabel klucz główny jest utworzony sztucznie. Aby ograniczyć liczbę danych oraz zminimalizować prawdopodobieństwo powstania błędów, zaprojektowano jeszcze tabele "lista producentów", "lista laboratoriów" oraz "kategoria urządzenia".



Rys. 2. Formularz sterujący "obsługa bazy"

Wpisywanie danych i zarządzanie nimi odbywa się za pośrednictwem formularzy. Rolę formularza głównego - sterującego pełni formularz "obsługa bazy" (rys. 2). Zawiera on pełną listę poleceń możliwych do zrealizowania w bazie.

Aplikacja ta umożliwia:
- wpisywanie i aktualizację wszystkich danych;
- wyszukiwanie urządzenia o danym numerze identyfikacyjnym laboratorium, numerze fabrycznym, numerze inwentarzowym;
- wyszukanie urządzenia według laboratorium;
- wyszukanie urządzenia według kategorii;
- wyszukanie urządzeń bez ważnego świadectwa wzorcowania;
- wyszukanie urządzeń bez ważnego terminu konserwacji;
- wyszukanie urządzeń, których ważność świadectwa kończy się w ciągu trzech miesięcy lub roku kalendarzowego;
- przeglądanie kart urządzeń.

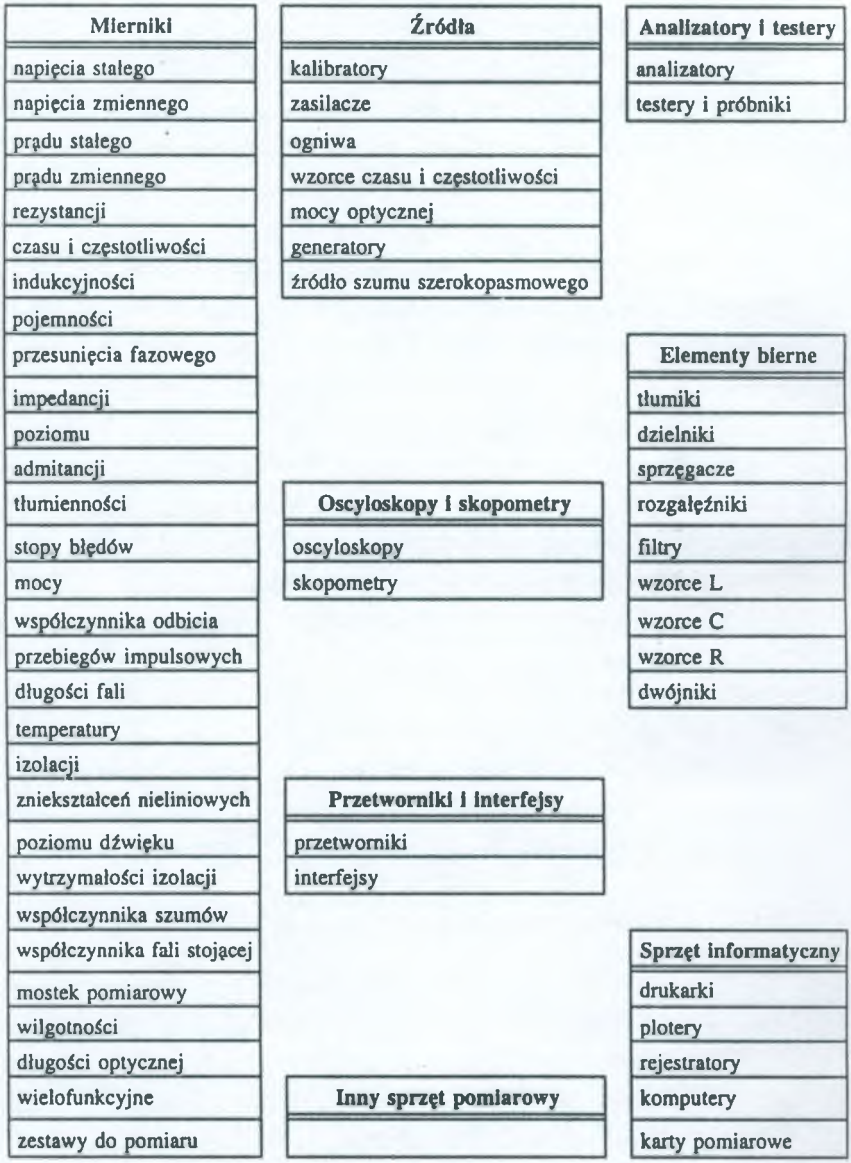
Formularze są tak zaprojektowane, aby zminimalizować prawdopodobieństwo wpisania błędnych danych w poszczególnych polach formularza (np. w polu daty ciągu znaków nie będących nią). Wprowadzono też elementy ułatwiające wpisywanie danych w postaci pól wyboru. Wyświetla się również komunikaty w przypadku wpisania błędnych danych.

Kolejnym elementem aplikacji są raporty, dzięki którym użytkownik systemu może uzyskać wydruki żądanych informacji. Raporty uruchamia się zarówno z poziomu poszczególnych formularzy, jak i z formularza głównego. Wykonuje się je na drukarce zainstalowanej w systemie operacyjnym.

- **Podział urządzeń pomiarowych według przeznaczenia**

W celu umożliwienia osobom korzystającym z systemu ENWAK znalezienia właściwego urządzenia dokonano ich klasyfikacji według przeznaczenia (rys. 3).

Podział ten nie jest zupełny i nie uwzględnia wszystkich, często bardzo specyficznych, przyrządów pomiarowych stosowanych w telekomunikacji. W miarę jednak aktualizowania danych można tworzyć nowe kryteria podziału, co powoduje, że ten system jest otwarty.



Rys. 3. Podział urządzeń pomiarowych według przeznaczenia

3.2. Zabezpieczenie systemu ENWAK

Program Access umożliwia tworzenie systemu ograniczonego dostępu do bazy danych. Możliwość tę wykorzystano. Użytkowników podzielono na trzy grupy:

- administratorów,
- obsługujących,
- użytkowników.

Administratorzy mają pełny dostęp do systemu ENWAK. Mogą nadawać prawa innym użytkownikom, modyfikować wszystkie obiekty, a także dopisywać, aktualizować i przeglądać dane.

Obsługujący są to osoby upoważnione do dopisywania i aktualizowania danych.

Użytkownicy mogą jedynie przeglądać dane.

Wszyscy korzystający z systemu ENWAK muszą podać grupę użytkowników, do których należą, oraz hasło. Ograniczenia te dotyczą zarówno aplikacji sterującej, jak i bazy danych. Można zaszyfrować system, jednak nie skorzystano z tego, gdyż spowalnia to jego pracę o ok. 15%.

4. PODSUMOWANIE

Komputerowy system ewidencji i zarządzania aparaturą kontrolno-pomiarową ENWAK spełnia wymagania systemu jakości i zarządzania systemem komputerowym. Umożliwia on szczegółową ewidencję i nadzór metrologiczny nad wzorcami oraz aparaturą kontrolno-pomiarową Instytutu Łączności. Istnieje możliwość rozbudowy istniejącej bazy (jeżeli będzie taka potrzeba), jak również włączenia jej do pracy w lokalnej sieci komputerowej Instytutu.

WYKAZ LITERATURY

1. Boratyn D.: MS Access 2.0 system, oblicze, ku aplikacjom. Croma, Wrocław 1995.
2. Budowa systemu zarządzania przyrządami pomiarowymi, zgodnie z normami ISO 9000. Materiały szkoleniowe firmy POLGAT.
3. Hrycyk W.: MS Access 2.0 leksykon języka Access Basic. Croma, Wrocław 1996.
4. PN EN 45001: Ogólne kryteria działalności laboratoriów badawczych.
5. Projekt nowelizacji przewodnika ISO/IEC25 - Ogólne wymagania dotyczące kompetencji laboratoriów pomiarowych i badawczych.
6. Tworzenie aplikacji Microsoft Access dla Windows 95. Microsoft Corporation, 1995.
7. Wymagania techniczne dotyczące elementów składowych telewizji kablowej. Załącznik nr 21 do rozporządzenia Ministra Łączności z dnia 4 września 1997 r. Instytut Łączności, Warszawa 1997.
8. Wymagania techniczne i eksploatacyjne dla systemu SDH. Załącznik nr 24 do rozporządzenia Ministra Łączności z dnia 4 września 1997 r. Instytut Łączności, Warszawa 1997.

Томаш Коссек
Анна Важец

СИСТЕМА УЧЕТА И МЕТРОЛОГИЧЕСКОГО КОНТРОЛЯ ЭТАЛОНАМИ И КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНОЙ АППАРАТУРОЙ ИНСТИТУТА СВЯЗИ

Резюме

Предложен способ учета и контроля измерительной аппаратуры соответствующий требованиям системы качества внедряемой в Институте Связи. Дается описание этого спо-

соба и предложение классификации измерительной аппаратуры.Рассматривается конкретная реализация компютерной базы данных, работающей в среде Microsoft Access.

Tomasz Kossek
Anna Warzec

METRIC SYSTEM OF REGISTRATION AND SURVEILLANCE OF GAUGES AND CONTROL AND MEASUREMENT SET OF APPARATUS IN INSTITUTE OF TELECOMMUNICATIONS

Summary

In this communication a proposition how to menage all the set of measurement apparatus according to system of quality recently introduced Institute of Telecommunications is presented. The mode of surveillance and registration is described as well as a proposition of measurement apparatus qualification. A real realisation of computer data base created for Microsoft Access environment is presented, too.

Tomasz Kossek
Anna Warzec

SYSTEME METROLOGIQUE D'ENREGISTREMENT ET SUROCILLANCE SUR LES ETALONS ET L'APPAREILLAGE DE CONTROLE ET MESURE A L'INSTITUTE DE TELECOMMUNICATION

Résumé

On a présenté dans ce communiqué une proposition de management des appareillages de mesure conformement aux cahier de charges du systéme de

la qualité qui a été introduit à l'Institute de Télécommunication. Le moyen de surveillance et d'enregistrement ainsi que la proposition de classification des appareils de mesurey sont aussi présentés. Une réalisation concrète de la base de données sur l'ordinateur crée à l'Institute de Télécommunication est decrite aussi.

Tomasz Kossek
Anna Warzec

REGISTRIERUNGS- UND METROLOGISCHES ÜBERWACHUNGSSYSTEM ÜBER MEßSTANDARDE UND PRÜF- UND UNTERSUCHUNGSEINRICHTUNGEN IM INSTITUT FÜR FERNMELDEWESEN

Zusammenfassung

Im Bericht wird Management über Meßgeräte vorgeschlagen, das Forderungen hinsichtlich des im Institut für Femmeldewesen eingeleiteten Qualitätssystems entspricht. Es wird Überwachungs- und Kontrollverfahren beschrieben wie auch Meßgeräteeinordnung vorgeschlagen. Verwirklichung von Rechner-Datenbasis in Microsoft Access Medium wird dargestellt.

AUTORZY

Mgr inż. Tomasz Kossek urodził się 5 kwietnia 1970 r. w Gdyni. W 1996 r. ukończył studia na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej (specjalność optoelektronika i telekomunikacja). Od 1995 r. pracuje w Instytucie Łączności w Centralnej Izbie Pomiarów Telekomunikacyjnych (w Zespole Metrologii Optoelektronicznej). Od 1996 r. jest studentem Studium Doktoranckiego na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Zajmuje się metrologią optoelektroniczną i automatyzacją procesów pomiarowych.

Inż. Anna Warzec urodziła się 5.02.1950 r. w Warszawie. W 1978 r. ukończyła studia na Wydziale Elektrycznym Politechniki Warszawskiej (specjalność automatyka i metrologia elektryczna). Od 1972 r. pracuje w Instytucie Łączności w Centralnej Izbie Pomiarów Telekomunikacyjnych (CIPT), pełniąc obowiązki kierownika CIPT i kierownika Laboratorium Metrologii Elektrycznej, Elektronicznej i Optoelektronicznej oraz sprawując nadzór nad utrzymaniem systemu jakości w Laboratorium. Zajmuje się zagadnieniami automatyzacji procesów pomiarowych oraz metrologią wielkości podstawowych, takich jak: napięcie, prąd stały i przemienny, rezystancja, pojemność i indukcyjność.

Dr inż. Elżbieta Andrukiewicz - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 108, 1997.

Doc. dr hab. Marian Marciniak - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 109, 1997.

Dr inż. Lech Smoczyński - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 103, 1994.