William Stallings

Poznaj najskuteczniejsze techniki ochrony systemów oraz informacji — zostań ekspertem w dziedzinie bezpieczeństwa w Internecie!

# KRYPTOGRAFIA *i* BEZPIECZEŃSTWO *sieci komputerowych*

## *Koncepcje i metody bezpiecznej komunikacji*

Wydanie V

- Opanuj techniki bezpiecznego uwierzytelniania użytkowników
- Wykorzystaj potencjał drzemiący w protokołach SSH, HTTPS i SSL
- Poznaj metody wykrywania ataków hakerskich i wirusów oraz skutecznej obrony przed nimi

Helion

Tytuł oryginału: Cryptography and Network Security: Principles and Practice, Fifth Edition

Tłumaczenie: Andrzej Grażyński
Projekt okładki: Urszula Banaszewska

ISBN: 978-83-246-2987-9

Authorized translation from the English language edition, entitled: Cryptography and Network Security: Principles and Practice, Fifth Edition; ISBN 0136097049, by William Stallings, published by Pearson Education, Inc, publishing as Prentice Hall, Copyright © 2011, 2006 by Pearson Education, Inc.



Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/krybek
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:
http://helion.pl/krybek

Printed in Poland.

# SPIS TREŚCI

ROZDZIAŁ 4

# BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH

*Liczne raporty dokumentujące obserwowane zachowanie się ptaków dowodzą istnienia ciekawego fenomenu, który nazwać by można kulturą konwersacji: otóż gdy wypowiada się jeden, pozostałe poświęcają mu całą swą uwagę, kontemplując w milczeniu jego świergot.*

*Badacze analizujący komunikację głosową ptaków zebrali wiele danych świadczących o tym, iż (a) ptasi monolog nigdy nie jest w żaden sposób przerywany, (b) ptasi słownik jest prawdopodobnie znacznie bogatszy, niż się powszechnie sądzi, oraz (c) w naturze ptasiej komunikacji odkrywa się w miarę postępu badań coraz większą głębię i złożoność.*

— *The Human Nature of Birds*, Theodore Barber

## KLUCZOWE POJĘCIA

- IEEE 802.11 to standard bezprzewodowych sieci lokalnych (*Wireless LAN*). Implementacje zgodne z tym standardem określane są mianem *Wi-Fi*.
- IEEE 802.11i to specyfikacja standardów bezpieczeństwa dla sieci IEEE 802.11 — uwierzytelniania, poufności, ochrony integralności danych i zarządzania kluczami. Zgodne z tym standardem implementacje zabezpieczeń określane są akronimem WPA, od *Wi-Fi Protected Access*.
- Protokół WAP (*Wireless Application Protocol* — protokół aplikacji bezprzewodowych) jest standardowym środkiem zapewniającym urządzeniom mobilnym dostęp do telefonii i usług informacyjnych, między innymi sieci WWW.
- Zabezpieczenia specyfikowane protokołu WAP realizowane są głównie za pomocą protokołu WTLS (*Wireless Transport Layer Security* — bezpieczeństwo bezprzewodowej warstwy transportowej), dostarczającego usług bezpieczeństwa dla komunikacji urządzenia mobilnego z bramką internetową WAP.
- Istnieje wiele podejść do całościowego zabezpieczenia komunikacji WAP; jedno z nich opiera się na założeniu, że w urządzeniu mobilnym zaimplementowany jest protokół TLS na bazie TCP/IP, a sieć bezprzewodowa zapewnia transport pakietów IP.

Ten rozdział poświęcony jest dwóm ważnym schematom bezpieczeństwa sieci bezprzewodowych. Pierwszym z nich jest IEEE 802.11i — standard zabezpieczania bezprzewodowych sieci LAN. Jest on częścią większej całości — standardu IEEE 802.11, określanego popularnie mianem *Wi-Fi*, od którego rozpoczniemy naszą analizę, by następnie zająć się szczegółami samego IEEE 802.11i.

W dalszym ciągu rozdziału zajmiemy się problemem bezpiecznego dostępu do internetu z poziomu urządzeń mobilnych — telefonów komórkowych, PDA i innych rodzajów terminali, po czym omówimy protokół WTLS, zapewniający bezpieczeństwo na odcinku komunikacji między urządzeniem mobilnym a bramką

łączącą sieć bezprzewodową (komórkową) z internetem. Rozdział zakończymy omówieniem problematyki całościowego zabezpieczania komunikacji między urządzeniami mobilnymi a serwerami WWW.

## 4.1. SIECI BEZPRZEWODOWE IEEE 802.11

IEEE 802 to nazwa komitetu, który stworzył wiele standardów dotyczących sieci lokalnych (LAN — *Local Area Network*). W 1990 roku komitet ten utworzył nową grupę roboczą — IEEE 802.11 — której zadaniem było opracowanie protokółów i specyfikacji transmisji dla bezprzewodowych sieci LAN (oznaczanych powszechnie akronimem WLAN, od *Wireless Local Area Network*). Od tego czasu lawinowo wręcz rozwijają się zastosowania tych sieci pracujących na różnych częstotliwościach i z różnymi prędkościami przesyłu danych, a wspomniana grupa robocza wypracowała wiele standardów, których lista wciąż się powiększa. Wyjaśnienie ważniejszych terminów związanych ze standardami kategorii IEEE 802.11 znajduje się w tabeli 4.1.

**Tabela 4.1.** Podstawowa terminologia standardów IEEE 802.11

| | | |
|---|---|---|
| Punkt dostępowy | *Access Point* (AP) | Dowolna encja posiadająca funkcjonalność stacji i zapewniająca skojarzonym stacjom dostęp do systemu dystrybucyjnego za pośrednictwem medium bezprzewodowego. |
| Podstawowy zbiór usług | *Basic Service Set* (BSS) | Zbiór stacji sterowanych przez wspólną funkcję koordynującą. |
| Funkcja koordynująca | *Coordination Function* | Funkcja określająca, kiedy stacja funkcjonująca w ramach BSS ma prawo wysyłać dane oraz kiedy gotowa jest na ich przyjęcie. |
| System dystrybucyjny | *Distribution System* (DS) | System wykorzystywany do połączenia BSS-ów i zintegrowanych sieci LAN w ESS. |
| Rozszerzony zestaw usług | *Extended Service Set* (ESS) | Zbiór połączonych BSS-ów i zintegrowanych sieci LAN, który jawi się jako pojedynczy dla warstwy LLC dowolnej stacji skojarzonej z jednym ze wspomnianych BSS-ów. |
| Jednostka danych protokołu MAC | *MAC Protocol Data Unit* (MPDU) | Jednostka danych wymienianych między dwiema połączonymi encjami MAC za pomocą usług warstwy fizycznej. |
| Jednostka danych usługi MAC | *MAC Service Data Unit* (MSDU) | Jednostka informacji wymienianych między użytkownikami MAC. |
| Stacja | *Station* | Dowolne urządzenie, w którym zaimplementowano warstwę fizyczną oraz warstwę MAC zgodnie ze standardem IEEE 802.11. |

### Wi-Fi Alliance

Pierwszym powszechnie zaakceptowanym standardem kategorii 802.11 był standard 802.11b. Wiele produktów, mimo iż zaprojektowanych i wykonanych zgodnie z nim, stwarzało jednak problemy we współdziałaniu; w celu ich rozwiązywania powołano w 1999 roku konsorcjum przemysłowe o nazwie *Wireless Ethernet Compatibility Alliance* (WECA), przemianowanej później na *Wi-Fi Alliance* (*Wireless Fidelity Alliance*). Konsorcjum to opracowało zestaw testowy, weryfikujący poprawność współdziałania produktów grupy 802.11b; produkty, które otrzymały stosowny certyfikat, określane więc były mianem produktów *Wi-Fi*. Opracowało ono także analogiczny zestaw testowy dla produktów standardu 802.11a — certyfikowane produkty określane były mianem *Wi-Fi5*. Obecnie prace Wi-Fi Alliance koncentrują się na wielu aspektach projektowania i funkcjonowania sieci bezprzewodowych — domowych, firmowych i hot-spotów.

Wi-Fi Alliance jest także autorem procedur certyfikacyjnych związanych ze standardami bezpieczeństwa IEEE 802.11i, określanych akronimem WPA (od *Wi-Fi Protected Access*). Nowsza wersja WPA, oznaczana akronimem WPA2, obejmuje wszelkie elementy bezpieczeństwa bezprzewodowych sieci wspomnianego standardu.

### Architektura protokołów rodziny IEEE 802

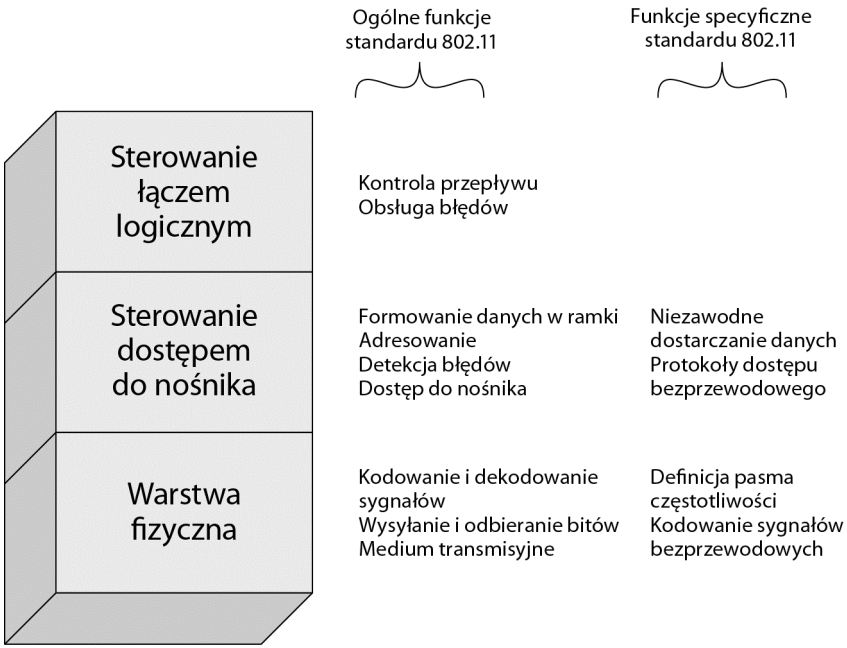
Rozpoczniemy od bliższego przyjrzenia się architekturze protokołów kategorii IEEE 802. Architektura ta, o strukturze warstwowej, przedstawiona jest na rysunku 4.1.

#### *WARSTWA FIZYCZNA*

Najniższe miejsce w hierarchii warstw modelu referencyjnego IEEE 802 zajmuje **warstwa fizyczna**, odpowiedzialna między innymi za kodowanie i dekodowanie sygnałów oraz wysyłanie i odbieranie poszczególnych bitów. Do warstwy fizycznej należy także specyfikacja medium transmisyjnego. W standardzie IEEE 802.11 specyfikacja warstwy fizycznej obejmuje także pasmo transmisyjne i charakterystykę anteny.

#### *STEROWANIE DOSTĘPEM DO NOŚNIKA*

Każda sieć LAN stanowi kolekcję urządzeń wykorzystujących jej możliwości transmisyjne. Dla poprawnej i efektywnej współpracy tych urządzeń konieczne jest istnienie pewnego mechanizmu, szeregującego ich dostęp do owych możliwości. Rolę tę spełnia sterowanie dostępem do nośnika (*Media Access Control*, w skrócie *MAC*). Warstwa MAC wymienia informację z warstwą wyższą — którą zazwyczaj jest sterowanie połączeniem logicznym (*Logical Link Control*, w skrócie *LLC*) — w postaci bloków danych określanych mianem **jednostki danych usługi MAC** (*MAC Service Data Unit*, w skrócie *MSDU*). Ogólnie rzecz biorąc, warstwa MC spełnia następujące funkcje:

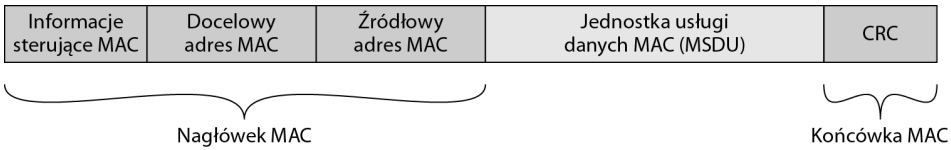



**Rysunek 4.1.** Stos protokołów IEE 802.11

- formowanie wysyłanych danych w ramki, określane jako **jednostki danych protokołu MAC** (*MAC Protocol Data Unit*, w skrócie *MPDU*) i zawierające pola związane z adresami oraz detekcją błędów;
- rozformowywanie otrzymywanych ramek, połączone z weryfikacją ich poprawności i rozpoznawaniem zawartych w nich adresów;
- zarządzanie dostępem do medium transmisyjnego sieci LAN.

Szczegółowy format MPDU różni się nieco pomiędzy używanymi protokołami MAC, generalnie jednak da się przedstawić w postaci widocznej na rysunku 4.2 i obejmującej następujące pola:

- **informacje sterujące MAC** — na przykład wartość priorytetu transmisji ramki;
- **docelowy adres MAC** — czyli fizyczny adres urządzenia docelowego w sieci;
- **źródłowy adres MAC** — czyli fizyczny adres urządzenia będącego nadawcą ramki;
- **MSDU** — czyli dane związane z wyższą warstwą;
- **CRC** — suma kontrolna, znana także pod akronimem FCS (*Frame Check Sequence* — ciąg weryfikacji ramki), obliczana dla całego pola MSDU. Odbiorca ramki porównuje zawartość tego pola z sumą kontrolną obliczoną dla otrzymanego MSDU — różnica między tymi wartościami świadczy o zniekształceniu jednego lub kilku bitów podczas transmisji.




**Rysunek 4.2.** Ogólny format MPDU IEEE 802

Ciąg pól poprzedzających pole MSDU nazywany jest **nagłówkiem MAC**, podobnie pola występujące po polu MSDU tworzą **końcówkę MAC**. Oba te obszary zawierają informacje pomocnicze, wykorzystywane wewnętrznie przez protokół MAC.

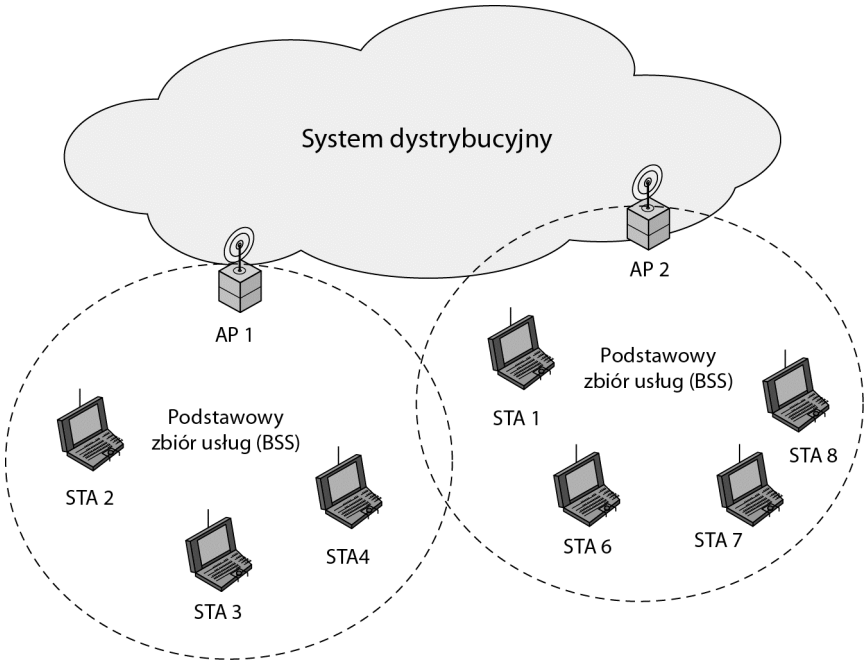
*STEROWANIE POŁĄCZENIEM LOGICZNYM*

W przypadku większości protokołów sterowania łączem danych warstwa ta odpowiedzialna jest nie tylko za detekcję błędów (za pomocą sum kontrolnych CRC), lecz także za korygowanie owych błędów poprzez ponowną transmisję ramek, które uległy uszkodzeniu. W architekturze protokołów sieci LAN te dwie funkcje zostały rozdzielone — i tak odpowiedzialność warstwy MAC ogranicza się do wykrywania błędów transmisji i odrzucania uszkodzonych ramek, natomiast za retransmisję brakujących ramek odpowiedzialna jest (opcjonalnie) warstwa LLC.

### Komponenty i model architektoniczny sieci IEEE 802.11

Na rysunku 4.3 widoczny jest model opracowany przez grupę roboczą 802.11. W modelu tym najmniejszym blokiem składowym bezprzewodowej sieci LAN jest **podstawowy zbiór usług** (*Basic Service Set — BSS*), składający się ze stacji bezprzewodowych wykonujących ten sam protokół MAC i ubiegających się o dostęp do tego samego, współdzielonego medium bezprzewodowego. BSS może być obiektem izolowanym albo przyłączonym do magistrali zwanej **systemem dystrybucyjnym** (*Distribution System — DS*) za pośrednictwem **punktu dostępowego** (*Access Point — AP*). W ramach BSS stacje komunikują się ze sobą nie bezpośrednio, lecz właśnie za pośrednictwem punktu dostępowego: stacja nadawcza wysyła odpowiednią ramkę do punktu dostępowego, ten zaś przesyła ją do stacji docelowej. Podobnie rzecz się ma w przypadku komunikacji dwóch stacji należących do różnych BSS-ów: stacja nadawcza wysyła odpowiednią ramkę do „swego" punktu dostępowego, który — za pośrednictwem systemu dystrybucyjnego — dostarcza ją do punktu dostępowego w docelowym BSS-ie, który to punkt dostępowy ostatecznie przesyła wspomnianą ramkę do stacji docelowej. Punkt dostępowy spełnia rolę przekaźnika w ramach swego BSS-u oraz rolę pomostu między połączonymi BSS-ami.

BSS stanowi bliski odpowiednik tego, co w literaturze określane jest mianem „komórki" (*cell*). Jeśli chodzi o naturę systemu dystrybucyjnego, to może on mieć formę przełącznika (*switch*), sieci przewodowej lub sieci bezprzewodowej.




**Rysunek 4.3.** Rozszerzony zestaw usług IEE 802.11

Wyjątkiem od opisanej zasady pośrednictwa punktu dostępowego jest tzw. **niezależny BSS** (*independent BSS — IBSS*), w ramach którego poszczególne stacje mobilne komunikują się ze sobą w sposób bezpośredni. Zazwyczaj istnieje on w formie tymczasowej, jako sieć ustanowiona ad hoc.

W prostej konfiguracji przedstawionej na rysunku 4.3 każda stacja przynależy do jednego BSS-u, czyli znajduje się w zasięgu innych stacji tegoż BSS-u. BSS-y nie muszą być jednak rozłączne: mogą „nakładać się" geograficznie, czyli posiadać wspólny obszar. Każda ze stacji znajdujących się na takim wspólnym obszarze przynależy do dwóch (lub więcej) BSS-ów. Ponadto związek danej stacji z konkretnym BSS-em nie musi mieć charakteru permanentnego: stacja może zmieniać swe położenie, przemieszczając się między BSS-ami, może także po prostu zostać wyłączona.

Zbiór dwóch lub więcej BSS-ów połączonych za pomocą systemu dystrybucyjnego nazywany jest **rozszerzonym zestawem usług** (*Extended Service Set — ESS*). Z perspektywy warstwy LLC cały ESS jawi się jako (logicznie) pojedyncza sieć LAN.

### Usługi IEEE 802.11

W standardzie IEEE 802.11 zdefiniowano dziewięć usług, których dostarczać musi sieć bezprzewodowa w celu zapewnienia funkcjonalności charakterystycznych dla przewodowych sieci LAN. Wymieniono je w tabeli 4.2, sugerując przy okazji dwojakie kryterium ich podziału:

- **Ze względu na dostawcę usługi**, którym może być stacja albo system dystrybucyjny. Usługi stacji zaimplementowane są w każdej stacji zgodnej z IEEE 802.11, czyli także w punktach dostępowych. Usługi dystrybucyjne mają związek z łącznością między BSS-ami i mogą być implementowane w punktach dostępowych albo specjalnych urządzeniach przyłączonych do systemu dystrybucyjnego.
- **Ze względu na cel**, którym może być kontrola dostępu i zapewnienie bezpieczeństwa (do tej grupy należą trzy usługi) albo transmisja MSDU między stacjami. W tym drugim przypadku, jeśli dana MSDU jest zbyt duża, by mogła być przesłana jako całość, podlega podziałowi na mniejsze kawałki (fragmentacji) i ponownemu złożeniu w całość w miejscu przeznaczenia.

**Tabela 4.2.** Usługi zdefiniowane w standardzie IEEE 802.11

| Usługa | Dostawca | Cel |
|---|---|---|
| Skojarzenie (*association*) | System dystrybucyjny | Transmisja MSDU |
| Uwierzytelnienie (*authentication*) | Stacja | Dostęp do sieci i bezpieczeństwo |
| Anulowanie uwierzytelnienia (*deauthentication*) | Stacja | Dostęp do sieci i bezpieczeństwo |
| Zakończenie skojarzenia (*disassociation*) | System dystrybucyjny | Transmisja MSDU |
| Dystrybucja (*distribution*) | System dystrybucyjny | Transmisja MSDU |
| Integracja (*integration*) | System dystrybucyjny | Transmisja MSDU |
| Dostarczanie MSDU (*MSDU delivery*) | Stacja | Transmisja MSDU |
| Ochrona prywatności (*privacy*) | Stacja | Dostęp do sieci i bezpieczeństwo |
| Zmiana skojarzenia (*reassociation*) | System dystrybucyjny | Transmisja MSDU |

Wzorując się na dokumencie definiującym standard IEEE 802.11, opiszemy poszczególne usługi istniejące w sieciach tego standardu. Wcześniej omówiliśmy już podstawową usługę dostarczania MSDU, w sekcji 4.2 zajmiemy się natomiast usługami związanymi z bezpieczeństwem sieci.

*PRZESYŁANIE KOMUNIKATÓW WEWNĄTRZ DS*

Z przesyłaniem komunikatów w ramach DS związane są dwie usługi: dystrybucja i integracja. **Dystrybucja** jest podstawową usługą wykorzystywaną przez stacje do wymiany MPDU w sytuacji, gdy stacje te skojarzone są z różnymi BSS-ami — wymiana MPDU odbywa się wówczas z wykorzystaniem systemu dystrybucyjnego. Powracając do rysunku 4.3: załóżmy, że stacja STA 2 zamierza wysłać ramkę do stacji STA 7. Stacja STA 2 wysyła wspomnianą ramkę do własnego punktu dostępowego AP 1, który przekazuje ramkę do systemu dystrybucyjnego z zadaniem dostarczenia jej do punktu dostępowego AP 2, który ostatecznie przekaże ją do stacji STA 7. Warto w tym momencie wspomnieć, że standard IEEE 802.11 nie określa szczegółów transmisji ramki poprzez system dystrybucyjny.

Gdy dwie komunikujące się stacje skojarzone są z tym samym BSS-em, opisana sytuacja upraszcza się znacznie, ponieważ w wymianie ramki między nimi uczestniczy tylko jeden punkt dostępowy.

Usługa **integracji** umożliwia transfer danych między stacją zlokalizowaną w sieci bezprzewodowej standardu IEEE 802.11 a stacją w zintegrowanej sieci LAN standardu IEEE 802.x. Określenie „zintegrowana" odnosi się do przewodowej sieci LAN fizycznie przyłączonej do systemu dystrybucyjnego, a wspomniane dwie stacje połączone są ze sobą w sensie logicznym. Usługa integracji odpowiedzialna jest przy tym za kwestie związane z translacją adresów i konwersją danych, wynikające z tegoż połączenia.

*USŁUGI ZWIĄZANE ZE SKOJARZENIEM*

Podstawowym zadaniem warstwy MAC jest transfer MSDU między encjami MAC; zadanie to realizowane jest przez usługę dystrybucji. Warunkiem funkcjonowania tej usługi jest dostępność informacji dotyczących poszczególnych stacji w ramach ESS-u — informację tę zapewniają usługi związane ze skojarzeniem. Zanim usługa dystrybucji będzie w stanie dostarczać lub odbierać dane do (ze) stacji, stacja ta musi najpierw zostać *skojarzona*. Koncepcja skojarzenia powiązana jest nieodłącznie z koncepcją *mobilności* urządzenia. W standardzie definiowane są trzy typy *przejść*, bazujące na mobilności:

- **Bez przejścia** (*no transition*) — stacja wykazująca zachowanie tego typu jest bądź to urządzeniem stacjonarnym, bądź też w swej mobilności nie opuszcza konkretnego BSS-u.
- **Przejście wewnętrzne** (*BSS transition*) — oznacza przemieszczanie stacji między BSS-ami należącymi do tego samego ESS-u. Warunkiem dostarczenia danych do stacji jest rozpoznawalność nowej lokalizacji urządzenia w ramach istniejących mechanizmów adresowania.
- **Przejście zewnętrzne** (*ESS transition*) — oznacza przemieszczenie stacji między BSS-ami należącymi do różnych ESS-ów. W tej sytuacji nie można gwarantować zachowania połączenia między wyższymi warstwami modelu 802.11, wskutek czego możliwe jest zakłócenie bieżąco realizowanej usługi.

Aby system dystrybucyjny mógł realizować usługę dystrybucji, musi dysponować informacją na temat lokalizacji stacji docelowej, a dokładniej — identyfikacji punktu dostępowego, do którego należy dostarczyć komunikat przeznaczony dla tej stacji. W tym celu stacja musi zostać skojarzona z konkretnym punktem dostępowym (AP), z czym związane są trzy następujące usługi:

- **Skojarzenie** — ustanawia początkowe skojarzenie między stacją a AP w konkretnym BSS-ie, dzięki czemu znany staje się adres i lokalizacja wspomnianej stacji. Z kolei rzeczony AP, komunikując się z innymi AP w tym samym ESS-ie, zapewnia transmisję ramek między ową stacją a innymi stacjami w tymże ESS-ie.

- **Zmiana skojarzenia** — realizuje przełączenie skojarzenia między dwoma AP w związku z przemieszczeniem się stacji między BSS-ami.
- **Zakończenie skojarzenia** — realizuje powiadomienie (wysłane przez stację lub AP), że istniejące skojarzenie zostaje zakończone. Stacja powinna wysłać takie powiadomienie przed wyłączeniem albo opuszczeniem ESS-u, w którym aktualnie się znajduje. Mechanizmy warstwy MAC przygotowane są jednak na ochronę przed urządzeniami „znikającymi" bez powiadomienia.

## 4.2. BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH IEEE 802.11I

Sieci bezprzewodowe pozbawione są z natury dwóch następujących cech organicznie związanych z przewodowymi sieciami LAN:

1. Aby urządzenie mogło transmitować dane poprzez sieć przewodową, należy je wpierw do tej sieci fizycznie przyłączyć. Przyłączenie to stanowi więc formę uwierzytelnienia urządzenia w sieci i jest aktem spektakularnym. Dla odmiany urządzenie mobilne, gdy tylko znajdzie się w zasięgu sieci bezprzewodowej, ma fizyczną możliwość realizowania transmisji bez żadnych dodatkowych, wyraźnych zabiegów.
2. Podobnie ma się rzecz z odbieraniem danych przez urządzenie: w przypadku przewodowej sieci LAN musi zostać ono wpierw do tej sieci fizycznie przyłączone. Jawne przyłączanie urządzeń do sieci przewodowej nosi więc znamiona realizacji ochrony prywatności. Dla odmiany urządzenie mobilne może fizycznie odbierać dane ze wszystkich sieci bezprzewodowych, w których zasięgu się znajduje.

Wobec powyższych różnic zrozumiałą staje się konieczność zapewnienia usług niwelujących ich konsekwencje. Zestaw mechanizmów ochrony prywatności i uwierzytelniania, zdefiniowanych w oryginalnej specyfikacji 802.11, pozostawia wiele do życzenia. Ochronę prywatności zapewniać miał algorytm WEP (*Wired Equivalent Privacy* — prywatność równoważna [osiągalnej w sieci] przewodowej), który okazał się być dotknięty poważnymi brakami. W standardzie 802.11i pojawiły się w związku z tym definicje solidniejszych mechanizmów bezpieczeństwa, między innymi ogłoszony przez Wi-Fi Alliance standard **Wi-Fi Protected Access** (WPA). Finalna postać standardu 802.11i określana jest akronimem **RSN**, od *Robust Security Network* (sieć z solidnym zabezpieczeniem), często też spotyka się synonim WPA2, wskazujący ów standard jako następcę WPA. Przez WPA2 oznacza się też program, w ramach którego Wi-Fi Alliance prowadzi certyfikowanie zgodności urządzeń z tym standardem.

### Usługi IEEE 802.11i

W standardzie IEEE 802.11i zdefiniowane są następujące usługi bezpieczeństwa:

- **Uwierzytelnianie**. Zdefiniowany został protokół komunikacji użytkownika z serwerem uwierzytelniania (*Authentication Server — AS*) zapewniający wzajemne uwierzytelnienie klienta i AP oraz generowanie tymczasowych kluczy na potrzeby ochrony bezprzewodowej komunikacji między nimi.
- **Kontrola dostępu**[1]. Usługa ta odpowiedzialna jest za wymuszenie uwierzytelniania, właściwe trasowanie komunikatów i wymianę kluczy. Współpracuje z wieloma protokołami uwierzytelniania.
- **Ochrona prywatności i integralności komunikatów**. Dane poziomu MAC (czyli na przykład jednostki protokołu LLC) są szyfrowane i uwierzytelniane za pomocą kodu integralności komunikatu (*MIC*), co zapewnia poufność i zabezpiecza przed skutecznymi modyfikacjami.

W części (a) rysunku 4.4 uwidocznione są protokoły wspierające powyższe usługi, zaś w części (b) pokazane są grupy algorytmów kryptograficznych, z których wspomniane usługi korzystają.

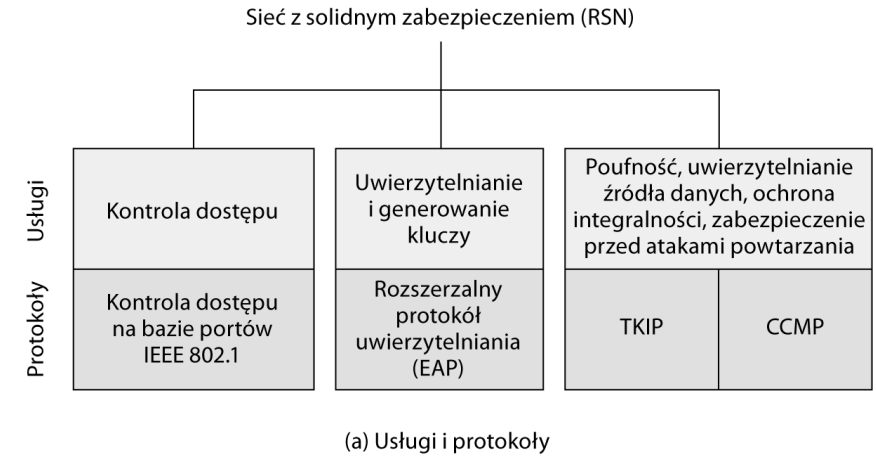
### Operacje IEEE 802.11i

Każda operacja IEEE 802.11i RSN może być rozpatrywana w podziale na pięć faz. Dokładna postać każdej fazy zależna jest od konfiguracji sieci, jak również od komunikujących się punktów — zgodnie z rysunkiem 4.3 mamy w tym względzie następujące możliwości:

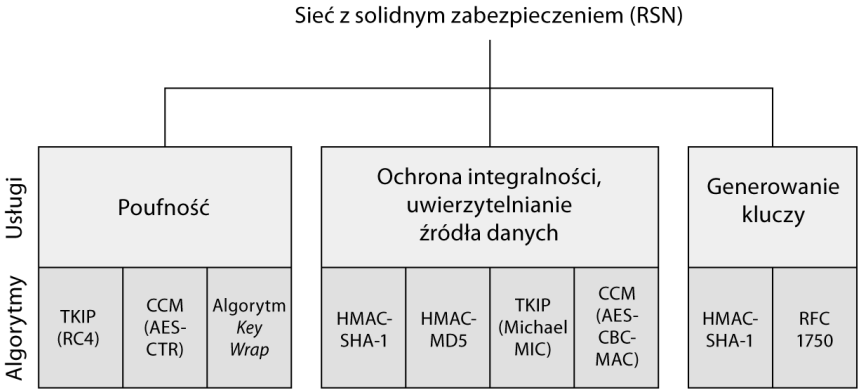
1. Dwie stacje należące do tego samego BSS-u komunikują się za pośrednictwem punktu dostępowego.
2. Dwie stacje należące do tego samego BSS-u komunikują się ze sobą w sposób bezpośredni.
3. Dwie stacje należące do różnych BSS-ów komunikują się za pośrednictwem odpowiednich punktów dostępowych (AP) i systemu dystrybucyjnego (DS).
4. Stacja bezprzewodowa komunikuje się za pośrednictwem swego AP i DS z urządzeniem w sieci przewodowej.

W gestii standardu IEEE 802.11i leży wyłącznie zabezpieczanie komunikacji stacji z jej punktem dostępowym. W przypadku nr 1 każda ze stacji nawiązuje bezpieczne połączenie ze wspólnym punktem dostępowym. Przypadek nr 2 jest podobny, bo funkcjonalność punktu dostępowego wbudowana jest przynajmniej w jedną ze stacji. W przypadku nr 3 bezpieczeństwo gwarantowane jest jedynie na skrajnych odcinkach — zabezpieczenie połączenia między punktami dostępowymi i systemem dystrybucyjnym nie wchodzi w kompetencje standardu

[1] W tym miejscu używamy określenia „kontrola dostępu" w kontekście mechanizmów bezpieczeństwa — nie należy go mylić z kontrolą dostępu do nośnika (MAC) opisywaną w sekcji 4.1. Niestety, w wielu publikacjach, również w dokumentach definiujących standard, pojęcie *access control* używane jest w obu znaczeniach.




(a) Usługi i protokoły



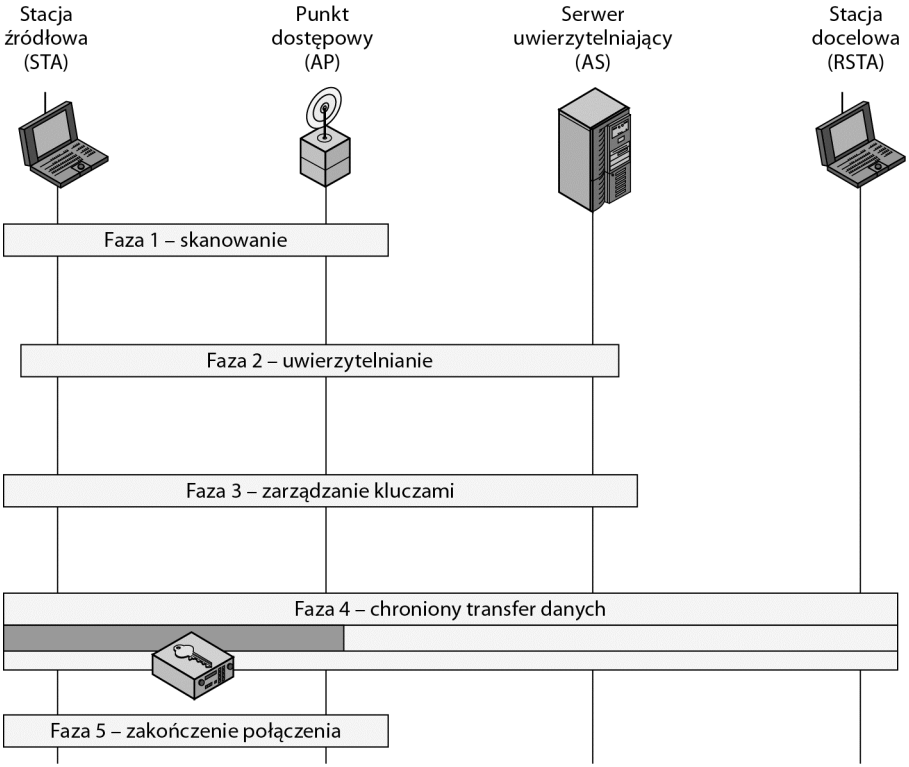

(b) Algorytmy kryptograficzne

CBC-MAC = Cipher Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

**Rysunek 4.4.** Elementy standardu IEEE 802.11i

IEEE 802.11i; jeżeli wymagane jest całościowe (*end-to-end*) zabezpieczenie połączenia, musi zostać zrealizowane w wyższej warstwie protokołu. Podobnie w przypadku nr 4 bezpieczeństwo gwarantowane jest jedynie na odcinku między stacją bezprzewodową a jej punktem dostępowym.

Przy powyższych zastrzeżeniach pięć wspomnianych faz operacji RSN przedstawić można w sposób pokazany na rysunku 4.5, gdzie uwidoczniono także komponenty sieciowe wchodzące w skład danej fazy; nowym komponentem jest tu serwer uwierzytelnienia (AS). Poziome prostokąty symbolizują wymianę ciągów MPDU.




**Rysunek 4.5.** Fazy operacji protokołu IEEE 802.11i RSN

- **Skanowanie**. Stacja bezprzewodowa wyszukuje dostępne sieci bezprzewodowe, w zasięgu których się znajduje. Wyszukiwanie to może być prowadzone na dwa sposoby. W wariancie *biernym* stacja przegląda wszystkie kanały, nasłuchując wysyłanych okresowo przez punkty dostępowe komunikatów zwanych w oryginale *beacons*[2] i realizujących rozgłaszanie prezentowanej przez te punkty polityki bezpieczeństwa (i parametrów konfiguracyjnych). Skanowanie *czynne* polega na wysyłaniu przez stację komunikatów rozgłoszeniowych *probe request*[3], na które punkt dostępowy powinien odpowiadać komunikatami *probe response*[4]. Rezultatem opisanego skanowania jest skojarzenie stacji z punktem dostępowym, powiązane z uzgodnieniem systemu szyfrowania i mechanizmu uwierzytelniania.
- **Uwierzytelnianie**. Stacja (STA) i AS prezentują sobie nawzajem swe tożsamości. Rola punktu dostępowego (AP) w tej konwersacji ogranicza się do blokowania wszelkiego ruchu między STA i AS nie związanego z uwierzytelnianiem.

[2] Dosł. rozbłyski — analogia do sygnałów świetlnych wysyłanych przez latarnię morską — *przyp. tłum.*
[3] Dosł. zapytanie sondujące — *przyp. tłum.*
[4] Dosł. odpowiedź na sondowanie — *przyp. tłum.*

- **Generowanie i dystrybucja kluczy**. AP i STA wykonują szereg operacji zmierzających do tego, by uzgodnić wspólne klucze kryptograficzne. Ramki wymieniane są wyłącznie między AP i STA.
- **Chroniony transfer danych**. Stacja źródłowa (STA) i docelowa (RSTA) wymieniają ze sobą ramki za pośrednictwem punktu dostępowego (AP). Ochrona transferu ogranicza się jednak do odcinka między STA a AP (co na rysunku 4.5 zaznaczono częściowym zacieniowaniem prostokąta) — protokół IEEE 802.11i nie gwarantuje całościowej (od STA do RSTA) ochrony transferu.
- **Zakończenie połączenia**. AP i STA wymieniają odpowiednie ramki związane z zakończeniem ochrony połączenia — połączenie między nimi powraca do poprzedniego stanu.

### Faza skanowania

Przeanalizujmy dokładniej poszczególne fazy protokołu RSN, poczynając od fazy skanowania, zilustrowanej w górnej części rysunku 4.6. Zadaniem tej fazy jest wzajemne rozpoznanie się STA i AP, uzgodnienie między nimi parametrów bezpieczeństwa i zbudowanie ich skojarzenia na bazie tychże parametrów na potrzeby przyszłej komunikacji.

#### *PARAMETRY BEZPIECZEŃSTWA*

Negocjowane między STA i AP parametry bezpieczeństwa obejmują następujące obszary:

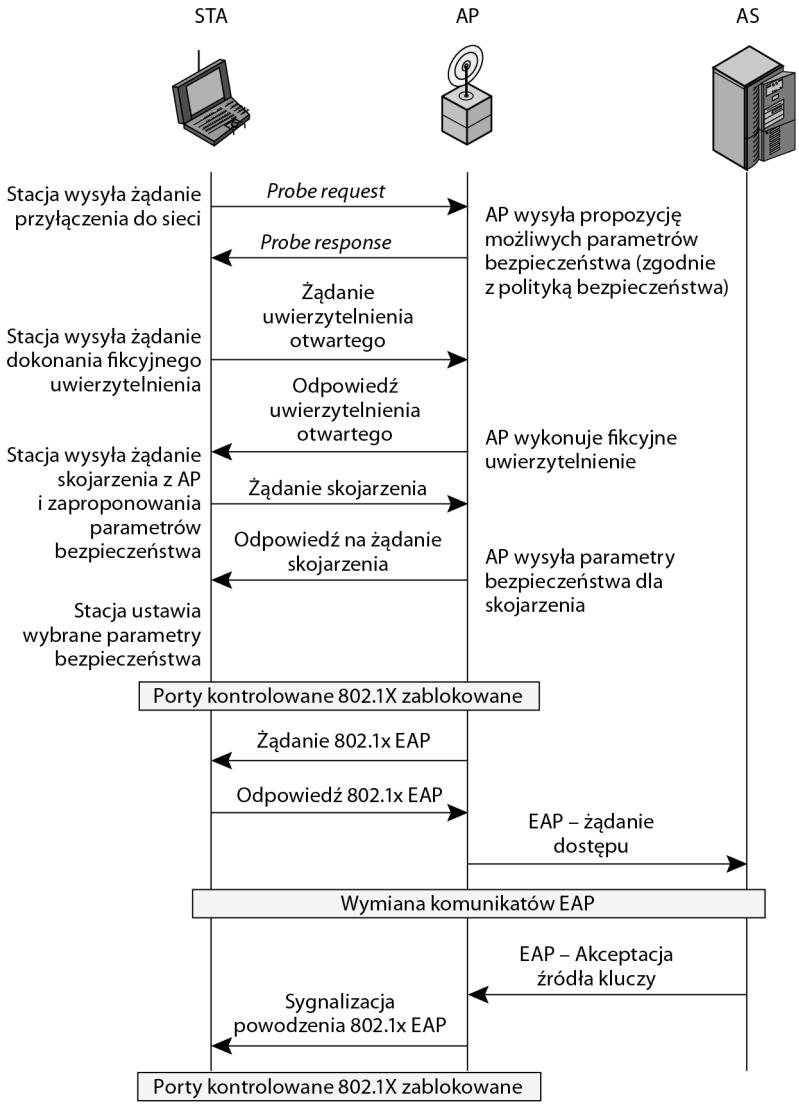
- protokoły zapewniające poufność i integralność MPDU wymienianych w trybie *unicast*[5], czyli wyłącznie między STA i AP;
- metody uwierzytelniania;
- zarządzanie kluczami kryptograficznymi.

Protokoły zapewniające poufność i ochronę integralności dla transmisji w trybie *multicast*[6] i *broadcast* (rozgłoszeniowym)[7] narzucane są przez AP, skutkiem czego wszystkie STA należące do grupy *multicast* używać muszą takich samych szyfrów i protokołów — specyfikacja tychże, nazywana *zestawem szyfrowym* (*cipher suite*), obejmuje wskazanie konkretnego algorytmu i (ewentualnie) długości klucza (gdy dla danego algorytmu istnieje kilka długości do wyboru). Aktualnie dostępne są w tym względzie następujące opcje:

[5] Tryb transmisji z dokładnie jednym nadawcą i dokładnie jednym odbiorcą — *przyp. tłum.*

[6] Tryb transmisji z jednym nadawcą i wieloma odbiorcami, logicznie postrzeganymi przez nadawcę jako jeden odbiorca grupowy — *przyp. tłum.*

[7] Tryb transmisji, w którym pakiety wysyłane w jeden kanał przeznaczone są do odbierania przez wszystkie pozostałe kanały w podsieci — *przyp. tłum.*




**Rysunek 4.6.** Fazy operacji IEEE 802.11i: skanowanie, uwierzytelnienie i skojarzenie

- WEP z kluczem zarówno 40-bitowym, jak i 104-bitowym, co zapewnia kompatybilność ze starszymi implementacjami IEEE 802.11;
- TKIP;
- CCMP;
- metody specyficzne dla dostawcy.

Dwa pozostałe obszary negocjacyjne, określane wspólnym mianem *zestawu uwierzytelniania i zarządzania* kluczami, w skrócie *AKM* (*Authentication and Key Management*), obejmują ustalenie (1) środków, za pomocą których STA i AP

realizować będą wzajemne uwierzytelnienie, oraz (2) sposób ustalenia klucza głównego (*root key*), na bazie którego generowane będą wszystkie inne klucze. Do dyspozycji są następujące opcje:

- IEEE 802.1X;
- ustalony tajny klucz współdzielony przez STA i AP — jego istnienie eliminuje potrzebę jawnego uwierzytelniania;
- metody specyficzne dla dostawcy.

*WYMIANA MPDU*

W fazie skanowania dokonują się trzy następujące akty wymiany ramek:

- **Wykrywanie sieci i usług**. Wymiana ta ma na celu wykrycie przez STA istnienia sieci bezprzewodowej, co — jak wcześniej wyjaśnialiśmy — może się dokonywać poprzez nasłuchiwanie rozgłaszanych przez AP komunikatów *beacon* (w postaci ramek RSN IE — *Robust Security Network Information Element*) bądź przez jawną wymianę komunikatów *probe request* i *probe response* między STA i AP.
- **Uwierzytelnianie otwarte**. Ten akt wymiany ramek istnieje ze względu na zapewnienie kompatybilności wstecz z maszyną stanu IEEE 802.11, implementowaną w wielu istniejących rozwiązaniach sprzętowych. Fizycznie sprowadza się do wymiany identyfikatorów między STA i AP, co nazywane jest **fikcyjnym uwierzytelnieniem** (*null authentication*).
- **Skojarzenie**. Na tym etapie następuje uzgodnienie parametrów bezpieczeństwa przyszłych połączeń. STA wysyła do AP ramkę *association request* (żądanie skojarzenia), zawierającą określenie wyboru spośród możliwości oferowanych przez AP (czyli konkretny zestaw AKM, jeden zestaw szyfru dla klucza selektywnego i jeden dla klucza grupowego). Jeśli AP nie akceptuje wyboru dokonanego przez STA (bo wybór ten na przykład wykracza poza opcje proponowane przez AP), odrzuca żądanie skojarzenia. STA również rezygnuje (ze względów bezpieczeństwa) z dalszego dialogu z AP — niepowodzenie skojarzenia mogło przecież być wynikiem komunikacji z niewłaściwym AP bądź też skutkiem otrzymania ramki spreparowanej przez intruza. Jak to pokazano na rysunku 4.6, zablokowane zostają porty kontrolowane IEEE 802.1X (za chwilę wyjaśnimy ten mechanizm).

### Faza uwierzytelniania

Jak już wspominaliśmy, w tej fazie następuje wzajemne uwierzytelnienie STA i serwera AS zlokalizowanego w systemie dystrybucyjnym (DS). Uwierzytelnianie to ma dwojakie cele: po pierwsze, ogranicza możliwości kontaktu z siecią wyłącznie do autoryzowanych stacji, po drugie — daje stacji zapewnienie, że komunikacja odbywa się z właściwą siecią.

*KONTROLA DOSTĘPU WEDŁUG IEEE 802.1X*

IEEE 802.11i wykorzystuje specyficzną, opartą na portach metodę dostępu do sieci (*Port-Based Network Access Control*) znaną jako standard IEEE 802.1X. W standardzie tym definiowany jest specyficzny protokół uwierzytelniania, oznaczany akronimem EAP (*Extensible Authentication Protocol* — rozszerzalny protokół uwierzytelniania). Protokół ten definiuje trzy role podmiotów uwierzytelniania: **suplikanta** (*suplicant*), **autentyfikator** (*authenticator*) oraz **serwer uwierzytelniający** (AS — *authentication server*). W kontekście sieci bezprzewodowych 802.11 dwa pierwsze terminy odnoszą się do (odpowiednio) stacji bezprzewodowej i punktu dostępowego. Serwer uwierzytelniający jest zwykle oddzielnym urządzeniem, zlokalizowanym w sieci przewodowej, dostępnej za pośrednictwem systemu dystrybucyjnego, chociaż może być także zaimplementowany jako część autentyfikatora.

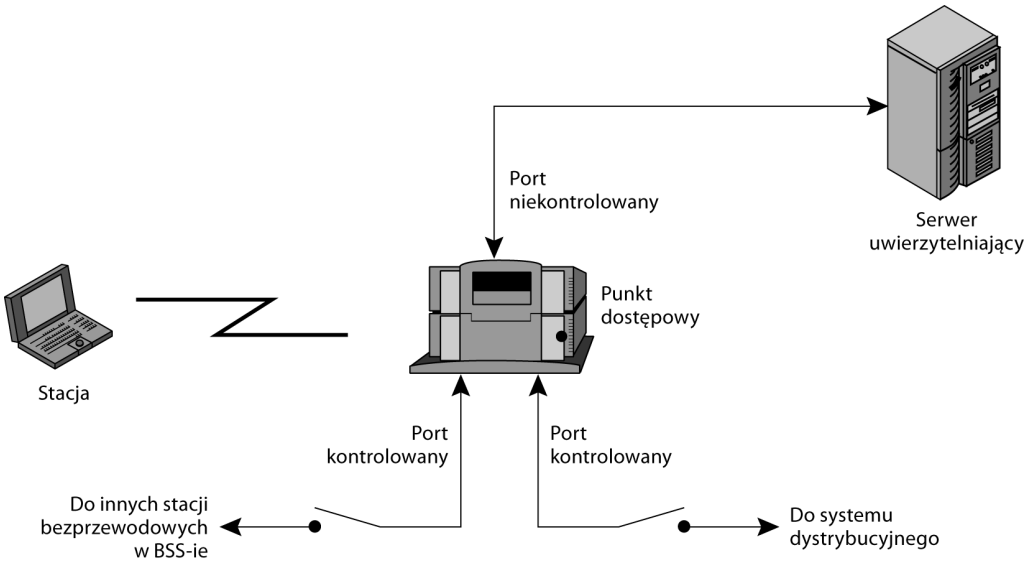
Dopóki suplikant nie zostanie uwierzytelniony przez AS za pomocą odpowiedniego protokołu, autentyfikator nie zezwala na przepływ między suplikantem a AS komunikatów innych niż sterujące i służące uwierzytelnianiu; kanał sterujący 802.1X jest otwarty, natomiast zablokowany jest kanał danych 802.11. Gdy jednak suplikant zostanie uwierzytelniony i uzgodnione zostaną klucze szyfrowania, autentyfikator dopuszcza przesyłanie danych do (od) suplikanta z zachowaniem predefiniowanych reguł kontroli jego dostępu do sieci. Innymi słowy, kanał danych zostaje odblokowany na określonych warunkach.

Na rysunku 4.7 zilustrowano podstawową dla 802.1X koncepcję portu kontrolowanego i portu niekontrolowanego. Porty są logicznymi encjami definiowanymi w kontekście autentyfikatora i reprezentują fizyczne połączenia sieciowe. W sieci bezprzewodowej autentyfikator (którym jest punkt dostępowy) może dysponować jedynie dwoma kontrolowanymi portami fizycznymi, łączącymi go (odpowiednio) z systemem dystrybucyjnym oraz stacjami w jego własnym BSS-ie. Każdy port logiczny musi zostać odwzorowany w jeden z tych dwóch portów fizycznych. Niekontrolowany port umożliwia wymianę PDU między suplikantem a serwerem AS niezależnie od stanu uwierzytelnienia suplikanta. Dla odmiany port kontrolowany umożliwia wymianę PDU między suplikantem z innymi systemami w sieci tylko wtedy, gdy suplikant taką wymianę autoryzuje.

Opisany framework, z protokołem uwierzytelniania w warstwie wyższej, funkcjonuje doskonale w konfiguracji BSS-u ze stacjami bezprzewodowymi i punktem dostępowym. W IBSS-ie nie ma jednak punktu dostępowego — stacje komunikują się ze sobą bezpośrednio; na tę okazję standard 802.11i przewiduje inny, bardziej skomplikowany schemat, realizujący wzajemne uwierzytelnianie pomiędzy komunikującymi się stacjami.

*WYMIANA MPDU*

W dolnej części rysunku 4.6 widoczna jest wymiana MPDU w fazie uwierzytelniania IEEE 802.11i. Fazę tę możemy rozpatrywać w rozbiciu na trzy następujące etapy:




**Rysunek 4.7.** Kontrola dostępu według IEEE 802.1X

- **Łączenie z AS**. STA wysyła do skojarzonego z nią AP żądanie połączenia z AS. AP akceptuje to żądanie i wysyła do AS żądanie dostępu.
- **Wymiana komunikatów EAP**. STA i AS uwierzytelniają się nawzajem, wymieniając odpowiednie ramki; jak za chwilę pokażemy, etap ten może przebiegać według różnych szczegółowych scenariuszy.
- **Bezpieczne dostarczenie klucza**. Gdy tylko uwierzytelnianie zostanie pomyślnie przeprowadzone, AS generuje główny klucz sesji (*master session key*, w skrócie *MSK*), określany także mianem „klucza AAA" (od *Authentication, Authorization, and Accounting*) i przesyła ów klucz do STA. Jak zobaczymy w dalszym ciągu rozdziału, wszystkie klucze wykorzystywane przez STA do ochrony komunikacji z AP generowane są na bazie MSK. Standard IEEE 802.11i nie precyzuje sposobu bezpiecznego dostarczenia MSK z AS do STA, zakładając rozwiązanie tego problemu w ramach EAP; niezależnie jednak od konkretnej metody ramki zawierające zaszyfrowany MSK wędrują z AS, poprzez AP, do STA.

*WYMIANA KOMUNIKATÓW PROTOKOŁU EAP*

Jak wspomnieliśmy, wymiana ramek w ramach protokołu EAP może odbywać się na różne sposoby. Zazwyczaj jednak na odcinku między STA a AP realizowany jest protokół o nazwie EAPOL (*EAP over LAN*), zaś na odcinku między AP a AS — protokół RADIUS (*Remote Authentication Dial In User Service*). Autorzy publikacji [FRAN07] przedstawiają następujące streszczenie tego scenariusza:

1. Wymianę EAP rozpoczyna AP, wysyłając do STA ramkę *EAP-Request/Identity*.

2. STA odpowiada ramką *EAP-Response/Identity*, którą AP otrzymuje za pośrednictwem niekontrolowanego portu; ramkę tę AP pakuje do postaci pakietu RADIUS i wysyła do AS.
3. AS odpowiada wysłaniem pakietu *RADIUS-Access-Challenge packet*, który zostaje przez AP przekształcony do postaci pakietu *EAP-Request*, zawierającego informacje niezbędne do uwierzytelnienia, m.in. dane o charakterze „wyzwania". Pakiet ten wysłany zostaje do STA.
4. STA odpowiada komunikatem *EAP-Response*, zawierającym m.in. odpowiedź na „wyzwanie" z punktu 3. AP przekształca ten pakiet do postaci komunikatu *Radius-Access-Request* i wysyła do AS.

   Zależnie od konkretnej metody realizacji EAP kroki 3. i 4. mogą tworzyć wielokrotnie powtarzany cykl. Przykładowo: dla metody opartej na tunelowaniu TLS następuje zazwyczaj 10 – 20 powtórzeń.
5. AS wysyła do AP pakiet *Radius-Access-Accept*, sygnalizując w ten sposób zezwolenie na dostęp STA do sieci. AP informuje STA o tym fakcie, wysyłając do niej ramkę *EAP-Success* (niektóre protokoły mogą wymagać dodatkowego potwierdzenia ze strony STA, na przykład poprzez tunel TLS). Kontrolowany port jest autoryzowany i użytkownik uzyskuje dostęp do sieci.

Zauważmy jednak (patrz rysunek 4.6), że kontrolowany port AP nadal jest zablokowany dla ogólnego ruchu danych. Jakkolwiek uwierzytelnianie zakończyło się pomyślnie, transmisja danych nie może się rozpocząć, dopóki w STA i AP nie zostaną zainstalowane odpowiednie klucze tymczasowe, co nastąpi w ramach czterostronnego uwierzytelniania.

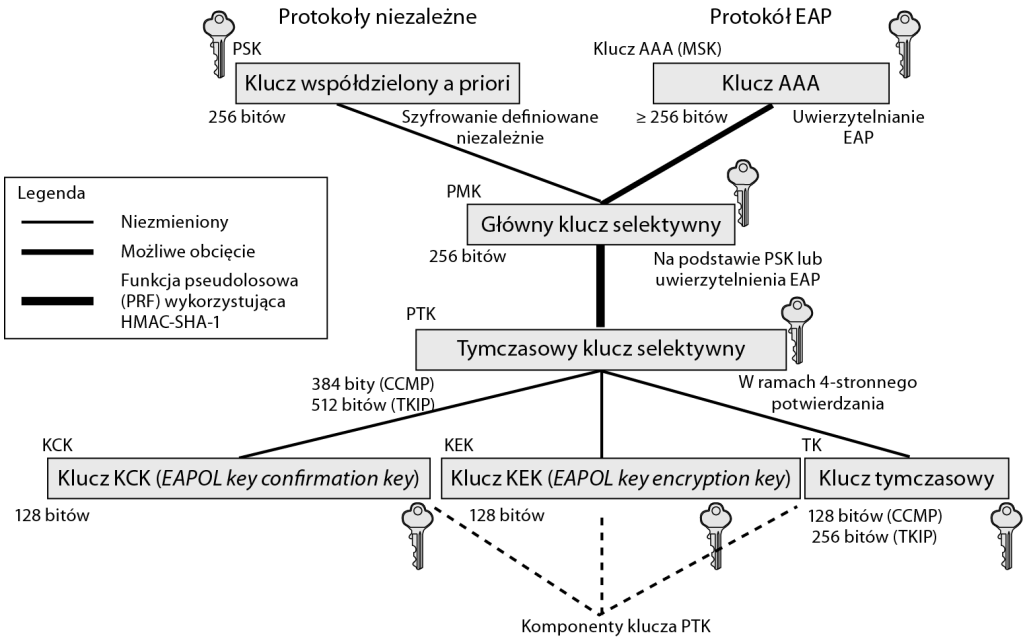
### Faza zarządzania kluczami

W tej fazie odbywa się generowanie rozmaitych kluczy kryptograficznych i ich rozprowadzanie do STA. Klucze te podzielić można na dwie grupy: **klucze selektywne** (*pairwise keys*) wykorzystywane są w komunikacji między poszczególnymi STA i AP, natomiast **klucze grupowe** (*group keys*) używane są w transmisjach w trybie *multicast*. Na rysunku 4.8, zaczerpniętym z publikacji [FRAN07], uwidocznione są hierarchie kluczy w ramach obu grup, natomiast w tabeli 4.3 znajduje się opis przeznaczenia poszczególnych kluczy.

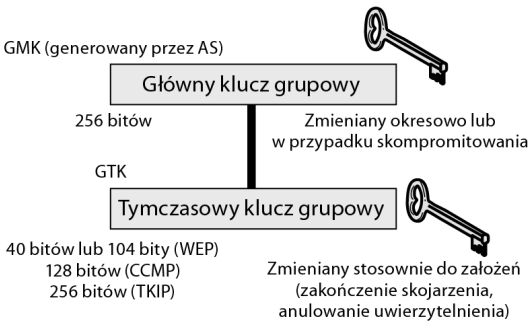
#### *KLUCZE SELEKTYWNE*

Klucze selektywne wykorzystywane są w komunikacji między dwoma urządzeniami, zazwyczaj STA i AP. Klucze te tworzą hierarchię, z kluczem głównym na szczycie i generowanymi dynamicznie na jego podstawie innymi kluczami, używanymi w ograniczonych przedziałach czasu.

Jeśli chodzi o wspomniany klucz główny na szczycie hierarchii, to istnieją dwie możliwości. Po pierwsze, między AP a konkretną STA może istnieć tajny klucz, ustanowiony za pomocą mechanizmów nie mających związku z IEEE 802.11i; klucz taki nazywamy **kluczem współdzielonym a priori** i oznaczamy




(a) Hierarchia kluczy selektywnych




(b) Hierarchia kluczy grupowych

**Rysunek 4.8.** Hierarchie kluczy IEEE 802.11i

skrótem **PSK** (od *pre-shared key*). Po drugie, klucz główny może być generowany w oparciu o protokół 802.1X w fazie uwierzytelniania (co wcześniej opisywaliśmy) i wówczas nazywany jest **kluczem głównym sesji** i oznaczany skrótem **MSK** (od *master session key*) lub skrótem **AAAK** (od *authentication, authorization, and accounting key*). Konkretna metoda generowania kluczy zależna jest od szczegółów używanego protokołu uwierzytelniania, jednak w obu przypadkach (PSK i MSK) AP współdzieli unikatowy klucz z każdą STA z osobna w swym BSS-ie; na bazie tego klucza generowane są wszystkie inne klucze unikatowe dla tej pary

**Tabela 4.3.** Klucze IEEE 802.11i używane przez protokoły zapewniające poufność i integralność danych

| Oznaczenie | Nazwa (oryginalna) | Przeznaczenie | Rozmiar (w bitach) | Typ |
|---|---|---|---|---|
| AAA | *Authentication, Accounting and Authorization Key* | Wykorzystywany do generowania PMK, uwierzytelniania IEEE 802.1x i zarządzania kluczami | ≥ 256 | Klucz generowania kluczy, klucz nadrzędny |
| MSK | *Master Session Key*, synonim AAA | | | |
| PSK | *Pre-shared Key* | Pełni rolę PMK, ustanawiany poza kompetencją IEEE 802.11 | 256 | Klucz generowania kluczy, klucz nadrzędny |
| PMK | *Pairwise Master Key* | Wykorzystywany przez partnerów do generowania PTK | 256 | Klucz generowania kluczy |
| GMK | *Group Master Key* | Wykorzystywany do generowania GTK | 128 | Klucz generowania kluczy |
| PTK | *Pair-wise Transient Key* | Generowany na podstawie PMK, obejmuje trzy podklucze: EAPOL-KCK, EAPOL-KEK i TK, a w przypadku TKIP także klucz MIC | 512 (TKIP)<br>384 (CCMP) | Klucz złożony |
| TK | *Temporal Key* | Klucz tymczasowy, wykorzystywany przez TKIP lub CCMP do zapewniania poufności i ochrony integralności w transmisjach w trybie *unicast* | 256 (TKIP)<br>128 (CCMP) | Klucz zabezpieczenia transmisji |
| GTK | *Group Temporal Key* | Tymczasowy klucz grupowy, generowany na podstawie GMK. Wykorzystywany do zapewniania poufności i ochrony integralności w transmisjach w trybach multicast i rozgłoszeniowym | 256 (TKIP)<br>128 (CCMP)<br>40, 104 (WEP) | Klucz zabezpieczenia transmisji |
| MIC Key | *Message Integrity Code Key* | Wykorzystywany przez TKIP w algorytmie Michael MIC do ochrony integralności komunikatów | 64 | Klucz ochrony integralności komunikatu |
| EAPOL-KCK | *EAPOL-Key Confirmation Key* | Używany do ochrony integralności źródła kluczy przesyłanego w ramach 4-stronnego potwierdzania | 128 | Klucz ochrony integralności komunikatu |

**Tabela 4.3.** Klucze IEEE 802.11i używane przez protokoły zapewniające poufność i integralność danych — *ciąg dalszy*

| Oznaczenie | Nazwa (oryginalna) | Przeznaczenie | Rozmiar (w bitach) | Typ |
|---|---|---|---|---|
| EAPOL-KEK | *EAPOL-Key Encryption Key* | Używany do zapewnienia poufności GTK i źródła kluczy, przesyłanych w ramach 4-stronnego potwierdzania | 128 | Klucz ochrony transmisji, w tym przesyłanych kluczy szyfrowania |
| WEP Key | *Wired Equivalent Privacy Key* | Wykorzystywany przez protokół WEP | 40 lub 104 | Klucz ochrony transmisji |

AP i STA. Zatem w dowolnej chwili każda STA utrzymuje zestaw kluczy przeznaczonych dla komunikacji z AP (jak przedstawiono to w części (a) rysunku 4.8), natomiast AP utrzymuje zbiór takich zestawów dla każdej ze „swoich" STA.

**Główny klucz selektywny** (*Pairwise master key* — **PMK**) wyprowadzany jest z klucza głównego jako jego kopia — jeśli tym kluczem głównym jest MSK dłuższy niż 256 bitów, PMK powstaje jako wynik jego obcięcia to tejże długości. Po zakończeniu uwierzytelniania (co kwitowane jest komunikatem *EAP Success* protokołu IEEE 802.1X — por. rysunek 4.6) AP i STA posiadają kopie wspólnego klucza MSK.

PMK wykorzystywany jest z kolei do wygenerowania **tymczasowego klucza selektywnego** (*pairwise transient key* — **PTK**), który w rzeczywistości składa się z trzech podkluczy wykorzystywanych w komunikacji między STA i AP po ich wzajemnym uwierzytelnieniu. Dokładniej: PTK powstaje jako wynik zastosowania funkcji HMAC-SHA-1 do konkatenacji PMK, adresów MAC STA i AP oraz (opcjonalnie) wartości *nonce* generowanych osobno przez STA i przez AP. Użycie adresów MAC udaremnia próby ataków „z człowiekiem pośrodku" i podszywanie się intruzów pod legalnych użytkowników, natomiast wartości *nonce* wprowadzają do generowanego klucza dodatkowy element losowości.

Trzy wspomniane podklucze klucza PTK to:

- **Klucz potwierdzający EAPOL** (*EAP Over LAN (EAPOL) Key Confirmation Key* — **EAPOL-KCK**) — zapewnia integralność danych i autentyczność ich źródła dla ramek wymienianych między STA i AP na etapie uzgadniania parametrów RSN, jest także świadectwem posiadania klucza PMK przez nadawcę, uzyskującego tym samym autoryzację dostępu do łącza.
- **Klucz szyfrowania EAPOL** (*EAPOL Key Encryption Key* — **EAPOL-KEK**) — zadaniem tego podklucza jest ochrona poufności kluczy i innych danych wymienianych na etapie kojarzenia STA z AP.
- **Klucz tymczasowy** (*Temporal Key* — **TK**) — jest bieżącym, tymczasowym kluczem wykorzystywanym do ochrony przesyłanych danych.

*KLUCZE GRUPOWE*

Klucze grupowe wykorzystywane są do komunikacji w trybie *multicast*, zgodnie z którym jedna STA (lub AP) wysyła MPDU jednocześnie do wielu innych STA. Na szczycie hierarchii kluczy grupowych znajduje się **główny klucz grupowy** (*group master key* — **GMK**). W przeciwieństwie do PTK, uwzględniającego cechy zarówno AP, jak i STA, GMK generowany jest całkowicie w obrębie AP (lub nadawczej STA) i transmitowany do skojarzonych z nim STA. Sposób generowania GTK nie jest zdefiniowany w standardzie 802.11i, wymaga się jedynie, by klucze GTK były nieodróżnialne w sensie obliczeniowym od wartości losowych. Przesyłanie GTK do docelowych STA chronione jest za pomocą kluczy selektywnych (których kopie znajdują się już w docelowych STA). GTK zmieniany jest każdorazowo, gdy któreś ze skojarzonych urządzeń opuszcza zasięg sieci.

*DYSTRYBUCJA KLUCZY SELEKTYWNYCH*

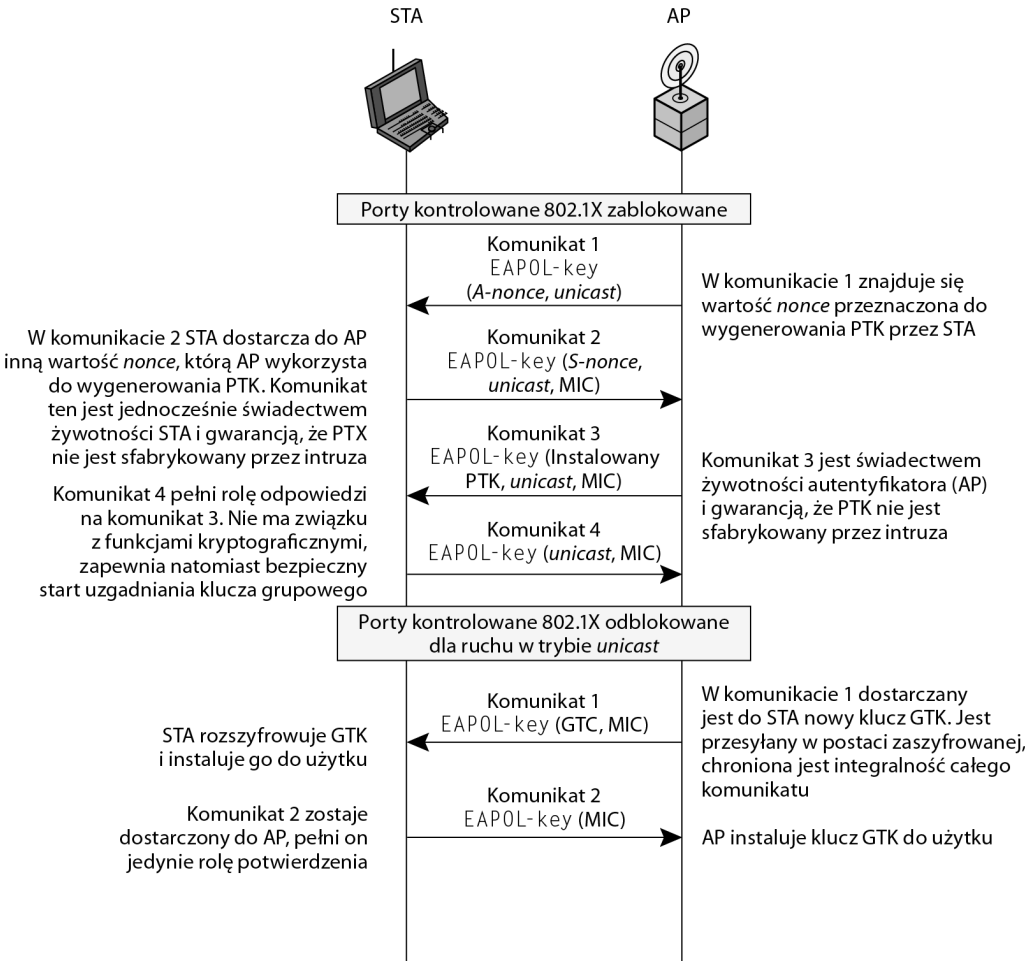
W górnej części rysunku 4.9 widoczna jest wymiana MPDU związanych z dystrybucją kluczy selektywnych. Wymiana ta, określana powszechnie jako **4-stronne potwierdzanie** (*4-way handshake*), ma na celu potwierdzenie istnienia PMK, weryfikację wyboru zestawu szyfrowego i wygenerowanie PTK na potrzeby przyszłej sesji. Obejmuje ona cztery następujące komunikaty:

- **AP → STA**: przesyłany komunikat zawiera adres MAC AP i wybraną przez AP wartość *nonce* (*A-nonce*).
- **STA → AP**: STA wybiera własną wartość *nonce* (*S-nonce*) i generuje PTK na podstawie obu *nonce*, obu adresów MAC (AP i własnego) i PMK. Wysyła także do AP swój adres MAC i wartość *S-nonce*, umożliwiając AP wygenerowanie identycznego PTK. Komunikat ten uwierzytelniony jest za pomocą kodu MIC[8], obliczanego przy użyciu klucza KCK i funkcji haszującej HMAC-MD5 lub HMAC-SHA-1-128.
- **AP → STA**: AP generuje PTK i wysyła do STA tę samą informację co w pierwszym komunikacie, tym razem jednak uwierzytelnioną za pomocą kodu MIC.
- **STA → AP**: ten komunikat jest zasadniczo potwierdzeniem otrzymania trzeciego komunikatu przez STA, również uwierzytelnionym za pomocą kodu MIC.

*DYSTRYBUCJA KLUCZA GRUPOWEGO*

Klucz GTK jest generowany przez AP i rozsyłany do wszystkich STA wchodzących w skład grupy *multicast*. Z każdą z nich AP wymienia dwa następujące komunikaty:

[8] Czytelnicy zauważyli już zapewne, że akronim MAC, używany w poprzednich rozdziałach na oznaczenie kodu uwierzytelniania komunikatu (*Message Authentication Code*), w tym rozdziale (i ogólnie w kontekście standardu 802.11) oznacza zupełnie co innego — sterowanie dostępem do nośnika (*Media Access Control*). Kod uwierzytelniania komunikatu nazywany jest natomiast **kodem integralności komunikatu** i oznaczany akronimem **MIC** (*Message Integrity Code*).




**Rysunek 4.9.** Fazy operacji IEEE 802.11i: 4-stronne potwierdzanie i uzgadnianie klucza grupowego

- **AP → STA**: w komunikacie zawarty jest GTK zaszyfrowany algorytmem RC4 lub AES przy użyciu klucza KEK. Do szyfrogramu dołączony jest kod MIC (obliczony przed szyfrowaniem).
- **STA → AP**: tym komunikatem (także uwierzytelnionym za pomocą MIC) STA potwierdza otrzymanie GTK.

### Faza chronionego transferu danych

IEEE 802.11i definiuje dwa schematy ochrony danych transmitowanych w MPDU: *Temporal Key Integrity Protocol* (TKIP) oraz *Counter Mode-CBC MAC Protocol* (CCMP).

*TKIP*

TKIP zaprojektowany został pod kątem starszych urządzeń, z zaimplementowanym protokołem WEP (*Wired Equivalent Privacy*); jego implementacja sprowadza się do wymiany firmware'u w tych urządzeniach. Oferuje on dwie następujące usługi:

- **ochronę integralności komunikatu** — do danych zawartych w ramce MAC dołączany jest kod MIC, obliczony za pomocą algorytmu haszującego o nazwie Michael, produkującego 64-bitową wartość jako funkcję adresów MAC (źródłowego i docelowego), źródła kluczy oraz wspomnianych danych;
- **poufność danych** — poufność tę uzyskuje się przez zaszyfrowanie algorytmem RC4 konkatenacji MPDU i jej kodu MIC.

256-bitowy klucz TK dzielony jest na trzy części (podklucze). Dwie z nich, o rozmiarze 64 bitów każda, wykorzystywane są przez algorytm Michael do obliczania kodów MIC dla komunikatów przepływających (odpowiednio) od STA do AP i od AP do STA. Z pozostałej 128-bitowej części wycinany jest klucz dla algorytmu RC4, szyfrującego transmitowane dane.

Dodatkowo, dla większego bezpieczeństwa, z każdą ramką związany zostaje konsekwentnie zwiększany licznik (*TKIP sequence counter*, w skrócie *TSC*). Spełnia on dwojakie zadanie: po pierwsze, jako składnik informacji wejściowej dla kodu MIC zapobiega skutecznym atakom powtarzania komunikatów; po drugie, w połączeniu z TK tworzy on dynamiczny klucz szyfrowania, inny dla każdej MPDU, co wydatnie utrudnia potencjalne zabiegi kryptoanalityczne.

*CCMP*

Ten schemat przeznaczony jest dla nowszych urządzeń IEEE 802.11, wyposażonych w odpowiednie wsparcie sprzętowe. Oferuje on — oczywiście w odmienny sposób — te same usługi, co TKIP, mianowicie:

- **ochronę integralności komunikatu** — kod integralności komunikatu obliczany jest przy użyciu trybu CBC (CBC-MAC) w sposób opisany w rozdziale 12. (tom I);
- **poufność danych** — do szyfrowania danych wykorzystywany jest algorytm AES w trybie licznikowym (CTR) opisanym w rozdziale 6. (tom I).

Dla obu usług wykorzystywany jest ten sam 128-bitowy klucz AES. Dodatkowo wykorzystywany jest 48-bitowy numer pakietu, służący do generowania wartości *nonce* w celu zapobieżenia skutecznym atakom powtarzania komunikatów.

### Funkcja pseudolosowa IEEE 802.11i

W wielu miejscach definicji standardu IEEE 802.11i przywoływana jest funkcja pseudolosowa (*pseudo-random function*, w skrócie *PRF*). Wykorzystuje się ją m.in. do generowania wartości *nonce*, kluczy selektywnych i klucza GTK. Względy bezpieczeństwa przemawiają za tym, by do każdego z tych celów używać innej

funkcji pseudolosowej; względy ekonomiczne — głównie efektywność implementacji — są jednak silną przesłanką na rzecz jej ujednolicenia we wszystkich tych zastosowaniach.

Mamy zatem w standardzie IEEE 802.11i jedną funkcję pseudolosową, opartą na generowaniu losowego strumienia bitów za pomocą algorytmu HMAC-SHA-1. Jak pamiętamy, wynikiem tego algorytmu jest 160-bitowy hasz stanowiący funkcję dwóch argumentów: danych źródłowych i klucza o długości co najmniej 160 bitów. Algorytm SHA-1 cechuje się silną właściwością rozpraszania (patrz sekcja 3.1 (tom I)) — zmiana pojedynczego bitu w argumencie wejściowym skutkuje drastyczną zmianą wartości wynikowego hasza, co w kontekście generatorów liczb pseudolosowych stanowi cechę jak najbardziej pożądaną.

Funkcja PRF standardu IEEE 802.11i posiada cztery argumenty wejściowe, a jej wynikiem jest hasz o żądanym rozmiarze. Dokładniej: wywołanie tej funkcji ma postać `PRF`(*K*, *A*, *B*, *Len*), gdzie

*K* jest tajnym kluczem,

*A* jest ciągiem znaków (łańcuchem) precyzującym konkretne zastosowanie (na przykład generowanie wartości *nonce* i kluczy selektywnych),

*B* reprezentuje pewne dane specyficzne w konkretnym zastosowaniu,

*Len* jest żądaną długością (w bitach) wynikowego hasza.

Przykładowo: obliczanie za pomocą PRF klucza PTK w schemacie CCMP odbywa się poprzez wywołanie[9]

```
PTK = PRF(PMK, "Pairwise key expansion", min(AP—Addr,
↪STA—Addr) || max(AP—Addr, STA—Addr) || min(Anonce, Snonce) ||
↪max(Anonce, Snonce), 384)
```

którego (łatwo rozpoznawalnymi) parametrami są

*K* `PMK`

*A* `"Pairwise key expansion"`

*B* konkatenacja obu adresów MAC i obu wartości *nonce*

*Len* `384`

Podobnie ma się rzecz w przypadku generowania wartości *nonce*:

```
Nonce = PRF(Random Number, "Init Counter", MAC || Time, 256)
```

W tym wywołaniu `Time` jest wskazaniem czasu sieci dostępnym dla urządzenia (komputera) implementującego generator.

Z kolei generowanie grupowego klucza tymczasowego realizowane jest przez wywołanie

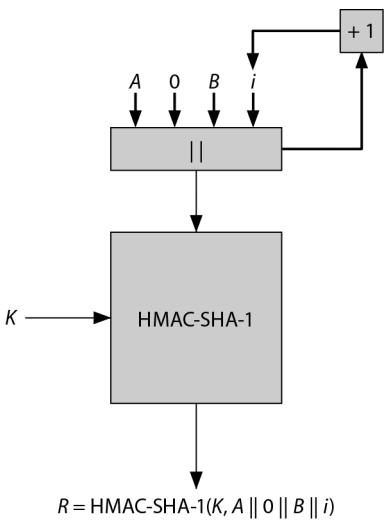
```
GTK = PRF(GMK, "Group key expansion", MAC || Gnonce, 256)
```

[9] Użycie funkcji `min` i `max` ma za zadanie uniewrażliwić wynikową wartość na *kolejność* użycia adresów i wartości *nonce*: w konkatenacji jako pierwsza zawsze występuje mniejsza z dwóch wartości — *przyp. tłum.*

Zasada działania funkcji PRF (a dokładniej: zasada wykorzystywania funkcji HMAC na potrzeby funkcji PRF) zilustrowana została na rysunku 4.10. Ponieważ od funkcji PRF zażądać można wyniku o dowolnej długości, funkcja HMAC (dająca zawsze hasz 160-bitowy) wywoływana jest być może wielokrotnie, a wyniki tych wywołań cząstkowych konkatenowane są w ostateczny wynik. Kluczem dla funkcji HMAC jest zawsze parametr *K* wywołania funkcji PRF, natomiast argumentem wejściowym funkcji HMAC jest konkatenacja czterech wartości: parametru *A*, liczby 0, parametru *B* i licznika *i* — licznik ten ma wartość 0 przy pierwszym wywołaniu funkcji HMAC i jest zwiększany o 1 przy każdym następnym wywołaniu. Symbolicznie można to zapisać w postaci następującego pseudokodu:

```
PRF(K, A, B, Len):
        R ← pusty ciąg bitów
        for i ← 0 to (⌈Len/160⌉-1) do
        R ← R || HMAC—SHA—1(K, A || 0 || B || i)
        Return łańcuch R obcięty do długości Len bitów
```

Operator || oznacza tu konkatenację ciągów bitowych, zaś $\lceil x \rceil$ oznacza wynik zaokrąglenia *x* w górę do najbliższej liczby całkowitej, czyli najmniejszą liczbę całkowitą nie mniejszą od *x*.




**Rysunek 4.10.** Funkcja pseudolosowa IEEE 802.11i

## 4.3. PROTOKÓŁ WAP

Protokół WAP (*Wireless Application Protocol* — protokół aplikacji bezprzewodowych) jest uniwersalnym, otwartym standardem opracowanym prze organizację WAP Forum (stanowiącą obecnie część *Open Mobile Alliance — OMA*) w celu umożliwienia użytkownikom telefonów komórkowych oraz innych urządzeń

mobilnych (PDA, pagerów itp.) dostępu do telefonii i usług informacyjnych, w tym sieci WWW i innych aplikacji internetowych. WAP zaprojektowano do współpracy ze wszystkimi istniejącymi wówczas technologiami bezprzewodowymi (m.in. GSM, CDMA i TDMA) i z zachowaniem jak największej zgodności z istniejącymi standardami internetowymi — IP, XML, HTML i HTTP. W protokół WAP wbudowano także pewne mechanizmy zabezpieczeń. Pierwszą wersję (1.0) protokołu zdefiniowano w roku 1998, rok później ukazała się wersja 1.1. Obecnie obowiązującą jest wersja 2.0, zdefiniowana w 2001 roku.

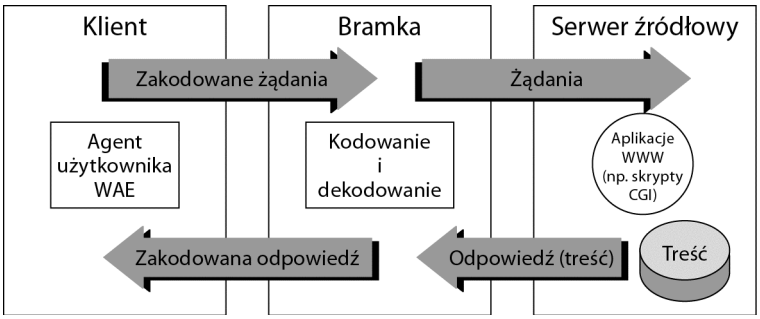
Najistotniejszym czynnikiem determinującym sposób wykorzystywania wspomnianych usług za pośrednictwem urządzeń mobilnych jest drastyczny wymiar ograniczoności tychże urządzeń oraz sieci, za pomocą których się łączą: typowy telefon komórkowy ma niezbyt wydajny procesor, minimalną pamięć, baterię o niewielkiej pojemności, a niewielki wyświetlacz istotnie ogranicza funkcjonalność interfejsu użytkownika. Sieci komórkowe cechują się relatywnie niską przepustowością, dużym opóźnieniem, a kwestia ich dostępności i stabilności jest daleko mniej przewidywalna niż w przypadku tradycyjnych sieci przewodowych. Co więcej, użytkownicy urządzeń mobilnych mają oczekiwania nieco inne niż użytkownicy komputerów — telefon komórkowy musi być w obsłudze znacznie łatwiejszy niż stacja robocza.

Protokół WAP stworzono z intencją sprostania tym właśnie wyzwaniom — jego specyfikacja obejmuje:

- model programowania oparty na modelu programistycznym WWW;
- język znaczników WML (*Wireless Markup Language*) wzorowany na języku XML;
- specyfikację niewielkiej przeglądarki, odpowiedniej do gabarytów urządzeń mobilnych;
- uproszczony stos protokołów komunikacyjnych;
- framework dla tworzenia aplikacji telefonii komórkowej (WTA — *Wireless Telephony Applications*).

### Model operacyjny

Na model programistyczny WAP składają się trzy elementy: *klient*, *bramka* i *serwer źródłowy* (rysunek 4.11). Między serwerem źródłowym a bramką dane przesyłane są przy użyciu protokołu HTTP. Bramka pełni rolę swoistego serwera proxy domeny bezprzewodowej: jej procesory wykonują wiele funkcji odciążających urządzenia bezprzewodowe od działań, które mogłyby stanowić zbytnie obciążenie dla ich ograniczonych możliwości. Mowa tu między innymi o usłudze DNS, konwersji danych między stosem protokołów WWW (TCP/IP i HTTP) a stosem protokołów WAP, kodowaniu danych do postaci minimalizującej transmisję bezprzewodową i (vice versa) dekodowanie tych danych do postaci wymaganych przez konwencje WWW. Bramka dokonuje także cache'owania często wykorzystywanych informacji.




**Rysunek 4.11.** Model programistyczny WAP

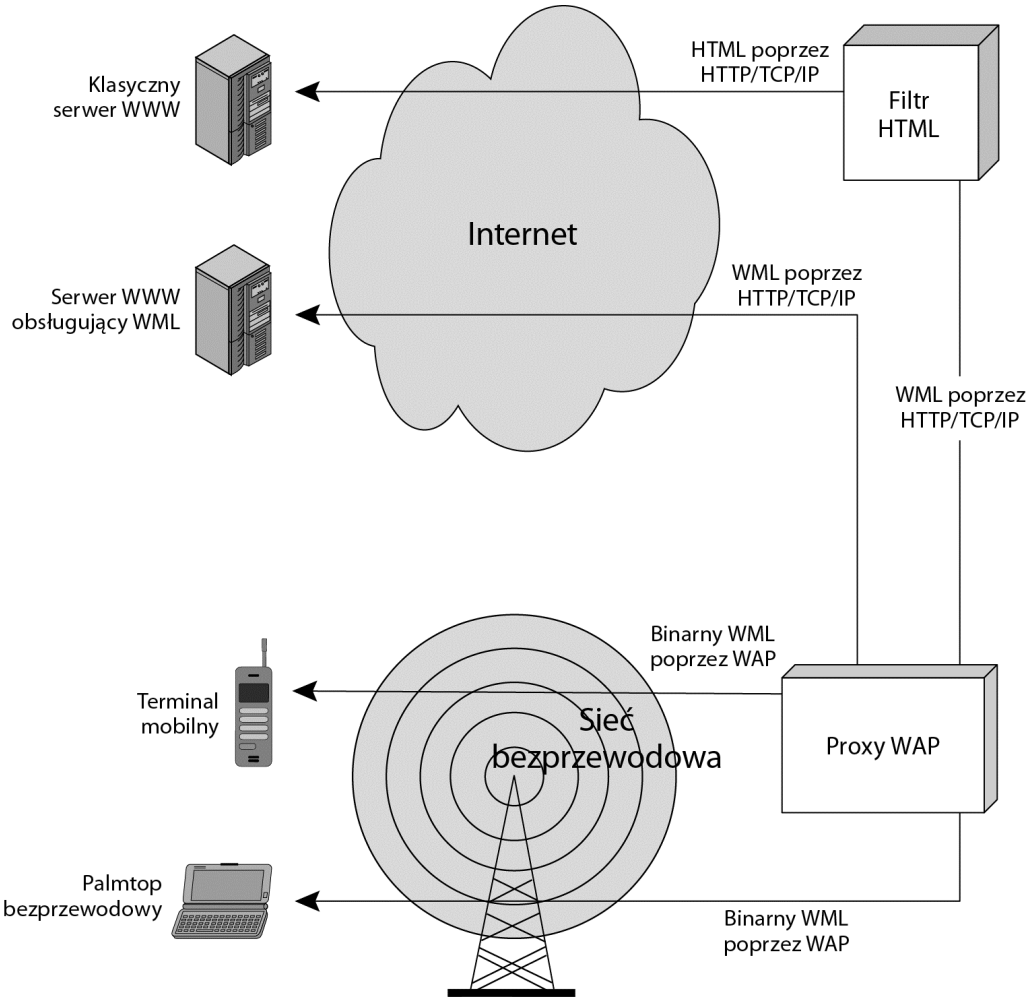
Na rysunku 4.12 widoczne są kluczowe komponenty środowiska WAP. Dzięki protokołowi WAP użytkownik urządzenia mobilnego może przeglądać treści udostępniane przez standardowy serwer WWW. Dane wychodzące z tego serwera obsługiwane są przez tradycyjne protokoły WWW (HTTP/TCP/IP), zakodowane są więc w języku HTML. W tej postaci trafiają do filtra HTML, który dokonuje ich konwersji na język WML. Filtr taki może mieć postać oddzielnego modułu fizycznego lub może być zintegrowany z proxy. W pierwszym przypadku skonwertowane do postaci WML dane trafiają do proxy, który konwertuje je do bardziej zwartej postaci zwanej „binarnym WML", w drugim przypadku obie konwersje — z HTTP/TCP/IP na WML, a następnie na binarny WML — są ze sobą połączone. W obu przypadkach dane w postaci binarnego WML przesyłane są między proxy a urządzeniem mobilnym za pomocą stosu protokołów WAP.

Architekturę WAP zaprojektowano z intencją sprostania dwojakiego rodzaju problemom: ograniczoności samych urządzeń mobilnych — w postaci niewielkiego wyświetlacza i prymitywnych raczej możliwości wprowadzania danych — oraz niewielkiej przepustowości cyfrowych sieci bezprzewodowych. Owszem, ewolucja tychże do standardu 3G i 4G jest faktem, samym urządzeniom mobilnym daleko jednak jeszcze do standardu 15-calowego monitora i standardowej klawiatury QWERTY z touchpadem. I dlatego WAP (i pokrewne mu technologie) zapewne jeszcze długo cieszyć się będzie niekwestionowanym prymatem.

### Język WML — Wireless Markup Language

Język WML pomyślany został jako standard opisu treści i formatu jej prezentacji na urządzeniach ze skromnym wyświetlaczem, niewielką mocą przetwarzania oraz ograniczonymi możliwościami wprowadzania danych, przeważnie przy użyciu klawiatury telefonicznej lub rysika. WML umożliwia szerokie skalowanie wyświetlanych treści — od prymitywnych, dwuwierszowych wyświetlaczy spotykanych w niektórych urządzeniach do znacznie bardziej eleganckich ekranów smartfonów.

Przeglądarka działająca w klasycznym komputerze dostarcza treści zorganizowanych w formę stron WWW kodowanych w języku HTML. Przystosowywanie owych stron na postać możliwą do wyświetlenia w urządzeniu mobilnym (poprzez tłumaczenie ich opisu na język WML) wiązać się musi nieuchronnie




**Rysunek 4.12.** Infrastruktura WAP

z usuwaniem niektórych elementów, przede wszystkim zaawansowanej grafiki i animacji. WML koncentruje się w pierwszej kolejności na tekstowych elementach stron, zawierających prawdopodobnie najbardziej istotną informację; WML dąży także do zorganizowania prezentowanej treści w formę wygodną dla użytkowników urządzeń mobilnych. Cele te realizowane są głównie poprzez następujące jego cechy:

- **Preferencję tekstu i grafiki** — polecenia kształtujące formatowanie i układ dokumentu zorientowane są na tekst i ograniczoną obsługę obrazów.
- **Metaforę talii kart** — w przeciwieństwie do stron WWW, kojarzonych ze sobą za pomocą hiperłączy, treści wyświetlane na urządzeniu mobilnym podzielone są na niewielkie jednostki zwane *kartami*, w analogii do zwykłych kart do gry. Każda karta reprezentuje z reguły jedną lub kilka jednostek interakcji (menu, akapit tekstu, pole wprowadzania danych), użytkow-

nik ma możliwość nawigowania po „talii" takich kart. Taka „talia" stanowi analogię strony HTML w tym sensie, że identyfikowana jest za pomocą adresu URL i stanowi logiczną jednostkę transmitowanej informacji.

- **Wsparcie dla nawigowania między kartami talii oraz między taliami** — nawigowanie to realizowane jest za pomocą obsługi zdarzeń, umożliwiającej także uruchamianie skryptów.

W przeglądarce bazującej na języku HTML użytkownik porusza się po serwisie, klikając hiperłącza. W urządzeniu interpretującym język WML nawigacja odbywa się poprzez przełączanie między kartami.

### Architektura WAP

Rysunek 4.13, zaczerpnięty z dokumentu opisującego architekturę WAP, przedstawia hierarchię stosu protokołów w implementacji klienta. Najogólniej rzecz ujmując, jest to model pięciowarstwowy, w którym każda z warstw świadczy — poprzez dobrze zdefiniowany interfejs — usługi na rzecz wyższych warstw, a także innych usług i aplikacji. Niektóre usługi oferowane są przez kilka protokołów, na przykład usługa transferu hipermediów[10] dostępna jest za pośrednictwem HTTP i WSP.

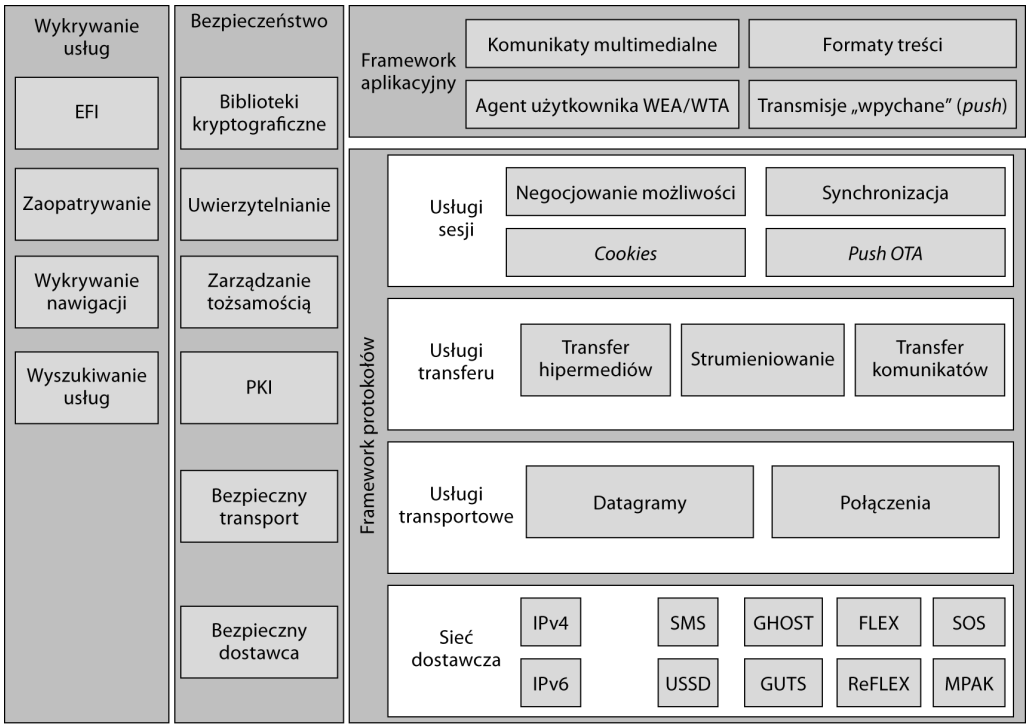
Wspólny dla wszystkich warstw jest zbiór usług powszechnie dostępnych, które podzielić można na dwie kategorie: **usługi bezpieczeństwa** i **wykrywanie usług**.

#### *USŁUGI BEZPIECZEŃSTWA*

Specyfikacja WAP obejmuje mechanizmy zapewniające poufność, ochronę integralności, uwierzytelnianie i niezaprzeczalność. Mechanizmy te dostępne są poprzez następujące usługi:

- **Szyfrowanie** — biblioteki frameworku aplikacyjnego dostarczają usług realizujących podpisywanie danych w celu ochrony ich integralności i niezaprzeczalności ich autorstwa.
- **Uwierzytelnianie** — WAP dostarcza różnych mechanizmów do uwierzytelniania klienta i serwera. W warstwie usług sesji do uwierzytelniania klienta wobec proxy lub serwera aplikacji służy usługa *HTTP Client Authenitication*, opisana w dokumencie RFC 2617, natomiast w warstwie usług transportowych wzajemne uwierzytelnianie klienta i serwera może być realizowane za pomocą protokołów TLS i WTLS.
- **Zarządzanie tożsamością** — moduł WIM (*WAP Identity Module*) dostarcza funkcji magazynowania i przetwarzania informacji niezbędnych do identyfikowania i uwierzytelniania użytkowników.

[10] „Hipermedia" to naturalne rozszerzenie hipertekstu, z którym przeplatają się audio, wideo, tekst i system odsyłaczy, tworząc nieliniowe medium przekazu informacji (w przeciwieństwie do multimediów, które są z natury liniowe). Klasycznym przykładem hipermediów jest sieć WWW — *przyp. tłum.*, na podstawie *http://encyklopedia.helion.pl.*




**Rysunek 4.13.** Architektura WAP

- **PKI** — ta grupa usług związana jest z wykorzystywaniem kryptografii kluczami publicznymi oraz certyfikatów kluczy publicznych.
- **Bezpieczny transport** — protokoły warstwy usług transportowych definiują metody bezpiecznego dostarczania treści, i tak WTLS oferuje bezpieczny transfer datagramów, TLS natomiast zapewnia bezpieczeństwo połączeń.
- **Sieć dostawcza** — niektóre sieci dostawcze oferują własne mechanizmy bezpieczeństwa, na przykład sieci IP (zwłaszcza w wersji IPv6) implementują w tym celu zbiór protokołów IPsec.

*WYKRYWANIE USŁUG*

Informowanie klienta i serwera o dostępnych usługach i możliwościach jest zadaniem usług z grupy wykrywania usług. Przykładowymi usługami tego typu są:

- **EFI** — *External Functionality Interface* (interfejs zewnętrznej funkcjonalności) umożliwia aplikacji uruchomionej na komputerze lub urządzeniu mobilnym określenie zestawu funkcji dostępnych w tym urządzeniu.
- **Zaopatrywanie** (*provisioning*) — usługa ta dostarcza urządzeniu parametry niezbędne do korzystania z usług sieciowych.

- **Wykrywanie nawigacji** — dzięki tej usłudze urządzenia mogą wykrywać nowe usługi sieciowe, na przykład bezpieczne „ciągnione" proxy (*secure pull proxies*) w trakcie operacji nawigacyjnych związanych (na przykład) z pobieraniem zasobów z serwera hipermediów. Przykład wykorzystania usługi tego typu do całościowego zabezpieczenia transmisji WAP na poziomie warstwy transportowej przedstawiamy w sekcji 4.5.
- **Wyszukiwanie usług** — usługa ta umożliwia określanie parametrów innych usług za pomocą skatalogowanych nazw mnemonicznych. Sztandarowym przykładem usługi tego typu jest system nazw domen (DNS — *Domain Name System*).

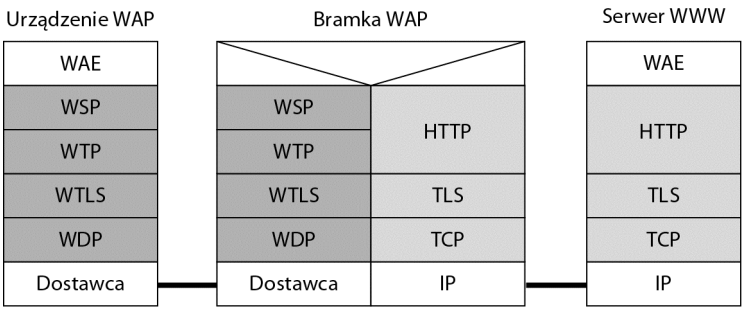
### Środowisko aplikacji bezprzewodowych

Tytułowe środowisko (oznaczane akronimem WAE — *Wireless Application Environment*) to framework obejmujący narzędzia i formaty ułatwiające tworzenie aplikacji dla urządzeń mobilnych — telefonów komórkowych, pagerów i PDA — implementujących protokół WAP. Podstawowymi elementami modelu WAE są (rysunek 4.13):

- **Agent użytkownika WAE** — oprogramowanie działające w ramach urządzenia mobilnego, oferujące użytkownikowi niezbędną funkcjonalność (na przykład wyświetlanie treści).
- **Aplikacje telefonii bezprzewodowej** (WTA — *Wireless telephony applications*) — kolekcja rozszerzeń związanych stricte z telefonią, zapewniających między innymi nawiązywanie połączeń telefonicznych z poziomu aplikacji oraz reagowanie przez aplikację na zdarzenia zachodzące w sieci telefonicznej.
- **Standardowe kodowanie treści** — zdefiniowano je w celu ułatwienia agentom użytkownika (głównie mikroprzeglądarkom) nawigowania po treści WWW; realizowane na bazie tzw. generatorów treści (*content generators*). Owe generatory to nic innego jak aplikacje webowe uruchamiane na serwerze źródłowym w odpowiedzi na żądania agentów użytkownika działających w urządzeniach mobilnych. WAE nie precyzuje bliżej natury wspomnianych generatorów, ograniczając się do sformułowania oczekiwania, iż będą to aplikacje działające na typowych serwerach HTTP, wykorzystywanych dziś w sieciach WWW.
- **Wpychanie** (*push*) to przyjmowanie przez urządzenie „niezamówionych" transmisji, czyli nie stanowiących odpowiedzi na żądania formułowane przez użytkownika, lecz wysyłanych z inicjatywy serwera. Do obsługi takich „wpychanych" do urządzenia transmisji przeznaczona jest usługa sesji *Push-OTA* (*Push Over The Air*).
- **Komunikaty medialne** — to transfer i przetwarzanie komunikatów pochodzących np. od aplikacji e-mail czy komunikatorów.

### Architektura protokołów WAP

Widoczna na rysunku 4.13 architektura determinuje zarówno kolekcję usług w każdej warstwie, jak i specyfikacje interfejsów na styku dwóch warstw. Ponieważ zależnie od okoliczności te same usługi WAP mogą być świadczone przez różne protokoły, stos protokołów WAP może przyjmować różną strukturę; ta widoczna na rysunku 4.14 to najczęstsza konfiguracja połączenia urządzenia klienckiego z serwerem źródłowym za pośrednictwem bramki WAP w przypadku, gdy urządzenie wspomniane implementuje wersję 1 WAP, jak również w przypadku urządzenia implementującego WAP2, gdy sieć dostawcza nie obsługuje protokołu TCP/IP.




**Rysunek 4.14.** Przykładowa konfiguracja protokołów WAP

Zajmiemy się teraz szczegółami kolejnych protokołów WAP, z wyjątkiem protokołu WTLS, któremu poświęcimy oddzielną sekcję 4.4.

#### *WSP — BEZPRZEWODOWY PROTOKÓŁ SESJI*

Protokół ten (WSP — *Wireless Session Protocol*) dostarcza aplikacjom interfejsu do dwóch usług sesji. Usługa **sesji połączeniowej** (*connection-oriented session*) funkcjonuje na bazie WTP, natomiast usługa **sesji bezpołączeniowej** (*connectionless session*) wykorzystuje niepewny protokół WDP. Zasadniczo protokół WSP stanowi rozszerzenie HTTP o nowości i modyfikacje optymalizujące jego wykorzystywanie w kanałach bezprzewodowych, cechujących się niską przepustowością i podatnością na zrywanie połączeń wskutek słabego sygnału lub przeciążenia sieci komórkowych.

WSP jest protokołem zorientowanym na transakcje ustanawiane na zasadzie „żądanie-odpowiedź". Każda jednostka danych (PDU) tego protokołu składa się z ciała (*body*) — mogą się w nim znajdować polecenia języka WML, skrypty w języku WMLScript lub obrazki — oraz nagłówka (*header*) opisującego zawartość ciała i zawierającego informacje związane z transakcją. WSP definiuje także transmisje „wpychane" (*push*) przez serwer do urządzenia, związane na przykład z rozgłaszaniem (*broadcast*) usługi lub serwisami abonowanymi przez klientów.

*WTP — BEZPRZEWODOWY PROTOKÓŁ TRANSAKCJI*

WTP (*Wireless Transaction Protocol*) zajmuje się zarządzaniem transakcjami poprzez transmitowanie żądań i odpowiedzi między agentem użytkownika (na przykład przeglądarką WAP) a serwerem aplikacji (działającym na przykład w ramach sklepu internetowego). WTP zapewnia niezawodną usługę transportową, uwolniony został jednak od wielu uciążliwości charakterystycznych dla protokołu TCP, przez co stał się protokołem „wagi lekkiej", przydatnym do zaimplementowania w warunkach „cienkiego klienta" (jakim jest typowe urządzenie mobilne) i sieci o względnie niskiej przepustowości. Wśród możliwości protokołu WTP wymienić należy przede wszystkim:

- trzy klasy usług transakcyjnych;
- opcjonalną funkcjonalność „użytkownik-użytkownik" — użytkownik WTP otrzymuje potwierdzenia o dostarczeniu każdego z wysłanych komunikatów;
- opcjonalną obsługę dodatkowych informacji zawartych w ostatnim potwierdzeniu — mogą to być na przykład statystyki wydajności połączenia;
- konkatenowanie jednostek protokołu (PDU) i opóźnianie potwierdzeń w celu zminimalizowania liczby wysyłanych komunikatów;
- transakcje asynchroniczne.

WTP jest więc zorientowany raczej na transakcje niż na połączenia — nie występuje w nim jawne nawiązywanie i rozwiązywanie połączeń, lecz raczej realizowanie transakcji w trybie bezpołączeniowym.

Wspomniane trzy klasy usług transakcyjnych wywoływanych przez WSP i warstwy wyższe to:

- **klasa 0** — niepewny komunikat wywołujący, bez komunikatu wynikowego;
- **klasa 1** — niezawodny komunikat wywołujący, bez komunikatu wynikowego;
- **klasa 2** — niepewny komunikat wywołujący, z niezawodnym dostarczeniem komunikatu wynikowego.

**Klasa 0** dostarcza niepewnej transmisji opartej na datagramach, wykorzystywanej głównie w ramach „wpychanych" transakcji. Dane przejmowane od użytkownika hermetyzowane są przez „nadawczą" encję WTP (inicjator) w postaci PDU i przesyłane do encji docelowej („respondera") bez potwierdzenia doręczenia. Docelowa encja WTP dostarcza otrzymane dane użytkownikowi.

**Klasa 1** to niezawodna transmisja oparta na datagramach, wykorzystywana w niezawodnych transakcjach „wypychanych". Podobnie jak w klasie 0 PDU hermetyzujące komunikat dostarczane jest przez inicjator do respondera, który po jego otrzymaniu odsyła inicjatorowi zwrotny komunikat ACK, który inicjator przekazuje swemu użytkownikowi. Responder utrzymuje jeszcze przez jakiś czas informacje o stanie połączenia na wypadek zagubienia komunikatu ACK i (lub) retransmisji PDU przez inicjator.

**Klasa 2** zapewnia usługę transakcyjną typu „żądanie-odpowiedź" i wykonywanie wielu transakcji w ramach jednej sesji WSP. Podobnie jak poprzednio dane użytkownika, hermetyzowane przez inicjator, dostarczane są do respondera, który z kolei dostarcza je użytkownikowi docelowemu. Użytkownik docelowy tworzy odpowiedź i odsyła ją użytkownikowi po stronie inicjatora. Ponieważ przygotowanie wspomnianej odpowiedzi może wiązać się ze znaczącym opóźnieniem, przekraczającym dopuszczalny limit, w celu zapobieżenia niepotrzebnym retransmisjom ze strony inicjatora responder wypełnia oczekiwanie okresowym wysyłaniem komunikatów ACK.

*WDP — BEZPRZEWODOWY PROTOKÓŁ DATAGRAMÓW*

WDP (*Wireless Datagram Protocol*) wykorzystywany jest w celu przystosowania wyższych warstw protokołu WAP do mechanizmu komunikacyjnego (określanego mianem **dostawcy** — *bearer*) funkcjonującego między urządzeniem mobilnym a bramką WAP. Wspomniane „przystosowywanie" obejmuje m.in. partycjonowanie danych na segmenty odpowiedniej wielkości oraz pośredniczenie w komunikacji z siecią dostawczą — WDP skrywa przed wyższymi warstwami WAP wiele szczegółów tej komunikacji. WDP implementowany jest często na bazie IP.

## 4.4. PROTOKÓŁ WTLS — BEZPIECZEŃSTWO BEZPRZEWODOWEJ WARSTWY TRANSPORTOWEJ

Zadaniem protokołu WTLS jest zabezpieczenie komunikacji urządzenia mobilnego (klienta) z bramką WAP. WTLS oparty jest na przemysłowym standardzie TLS, który z kolei jest wynikiem udoskonalenia protokołu SSL[11]. WTLS jest bardziej efektywny od TLS, wiąże się bowiem z wymianą mniejszej liczby komunikatów; TLS jest natomiast wykorzystywany na odcinku między bramką WAP a serwerem źródłowym. Zlokalizowana na styku obu wspomnianych odcinków bramka WAP (jak na rysunku 4.14), dokonująca translacji między protokołami TLS i WTLS, jest w tym łańcuchu najbardziej wrażliwym ogniwem i wymaga szczególnie starannego zabezpieczenia przed atakami z zewnątrz.

WTLS oferuje następujące możliwości:

- **ochronę integralności danych**, czyli zabezpieczenie przed ich zmodyfikowaniem, poprzez uwierzytelnianie komunikatów przesyłanych między klientem a bramką;
- **ochronę prywatności** poprzez szyfrowanie czyniące przesyłane treści nieczytelnymi dla nieuprawnionych podmiotów;
- **uwierzytelnianie** komunikujących się encji na podstawie certyfikatów;
- **zapobieganie paraliżowaniu usług** poprzez odrzucanie komunikatów powtarzanych lub niezweryfikowanych.

[11] Protokoły SSL i TLS opisywaliśmy w rozdziale 3., nie ma jednak konieczności powracania do tego opisu — prezentowany tu opis jest wystarczający.

### Sesje i połączenia WTLS

Dwiema najważniejszymi koncepcjami WTLS są bezpieczna sesja i bezpieczne połączenie:

- **Bezpieczne połączenie** to połączenie typu *peer-to-peer* między warstwami transportowymi (w kategoriach modelu odniesienia OSI) zapewniające odpowiedni typ usługi. Ma charakter tymczasowy i zawsze istnieje w ramach konkretnej sesji.
- **Bezpieczna sesja** to wynik skojarzenia klienta z bramką WAP. Ustanowienie sesji wiąże się ze zdefiniowaniem zestawu parametrów używanych przez połączenia nawiązywane w ramach tej sesji. Koncepcja sesji pozwala zaoszczędzić czasochłonnego negocjowania parametrów dla każdego połączenia z osobna.

W danej chwili między klientem a bramką może istnieć wiele bezpiecznych połączeń. Teoretycznie możliwe jest jednoczesne istnienie wielu sesji, choć w praktyce raczej z możliwości tej się nie korzysta.

Każda sesja może w danej chwili znajdować się w różnych stanach. Gdy zostanie ustanowiona, znajduje się w stanie ustalonym dla odczytu i zapisu (czyli odbierania i wysyłania danych); ponadto w czasie tworzenia sesji przez podprotokół powitalny (*handshake*) tworzony jest stan przejściowy (*pending state*), który po zakończeniu działania tego protokołu staje się stanem ustalonym.

Stan bezpiecznej sesji WTLS określony jest przez następujące parametry:

- **identyfikator sesji** — dowolny ciąg bajtów wybrany przez bramkę do identyfikowania stanu sesji;
- **wersję** używanego protokołu WTLS;
- **certyfikat partnera** — nieobowiązkowy;
- **metodę kompresji** — algorytm wykorzystywany do kompresowania danych przed ich szyfrowaniem;
- **specyfikację szyfru** — określenie algorytmu szyfrowania (opcjonalne, na przykład RC5 lub DES), algorytmu haszowania wykorzystywanego do obliczenia kodu MIC (np. MD5 lub SHA-1) oraz atrybutów kryptograficznych, m.in. `hash_size`;
- **tajny kod główny** — ciąg 20 bajtów współdzielony przez klienta i bramkę i nieznany nikomu innemu;
- **sposób numerowania** — metoda nadawania numerów sekwencyjnych przesyłanym PDU: jawna (*explicit*), domyślna (*implicit*) albo rezygnacja z numerowania (*off*);
- **odświeżanie** — określenie częstotliwości odświeżania niektórych parametrów kryptograficznych (klucza szyfrowania, sekretu głównego i wektora inicjacyjnego *IV*);
- **znacznik wznawiania** — określenie, czy w ramach sesji mogą być tworzone nowe połączenia.

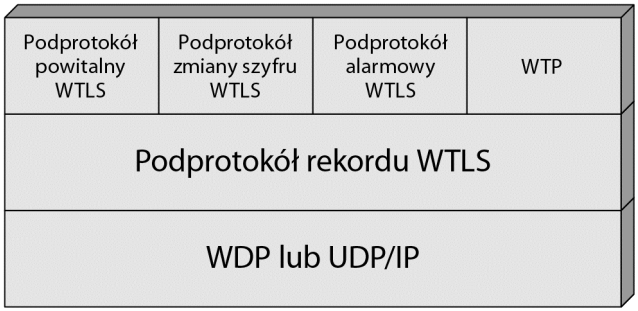
Stan bezpiecznego połączenia określony jest przez środowisko operacyjne podprotokołu rekordu i obejmuje wszystkie parametry operacji kryptograficznych (szyfrowania, deszyfracji oraz obliczania i weryfikowania kodów MIC), a ponadto następujące elementy:

- **klasyfikację nadawcy** — wskazanie, czy encja wysyłająca PDU jest klientem, czy bramką;
- **algorytm szyfrowania** — dane związane z szyfrowaniem, między innymi rozmiar klucza dla danego algorytmu, efektywnie wykorzystywany rozmiar klucza[12], typ szyfru (blokowy albo strumieniowy) i rozmiar bloku (dla szyfru blokowego);
- **algorytm MIC** — rozmiar klucza wykorzystywanego do obliczania kodu MIC oraz rozmiar samego kodu MIC;
- **algorytm kompresji** — wszelkie informacje związane z algorytmem kompresowania rekordów;
- **tajny kod główny** — ciąg 20 bajtów współdzielony między klienta i bramkę;
- **losowy parametr kliencki** — 16-bitowa wartość losowa dostarczana przez klienta;
- **losowy parametr bramki** — 16-bitowa wartość losowa dostarczana przez bramkę WAP;
- **sposób numerowania** — metoda nadawania numerów sekwencyjnych przesyłanym PDU: jawna (*explicit*), domyślna (*implicit*) albo rezygnacja z numerowania (*off*);
- **odświeżanie** — określenie częstotliwości odświeżania niektórych parametrów kryptograficznych (klucza szyfrowania, sekretu głównego i wektora inicjacyjnego *IV*). Jeżeli oznaczymy ten parametr przez $r$, to odświeżanie odbywa się co $n = 2^r$ rekordów, czyli wtedy, gdy numer sekwencyjny osiągnie wartość 0, $n$, $2n$, $3n$ itd.

### Architektura protokołu WTLS

WTLS nie ma struktury monolitycznej, lecz podzielony jest na dwie warstwy, jak pokazano to na rysunku 4.15. Rezydujący w warstwie niższej **podprotokół rekordu** (*WTLS Record Protocol*) zapewnia podstawowe usługi na użytek podprotokołów rezydujących w warstwie wyższej. Jednym z tych podprotokołów jest opisywany wcześniej WTP, trzy pozostałe — **podprotokół powitalny** (*Handshake Protocol*), **podprotokół zmiany szyfru** (*Change Cipher Spec Protocol*) i **podprotokół alarmowy** (*Alert Protocol*) są integralną częścią WTLS. Przyjrzyjmy się im nieco bliżej.

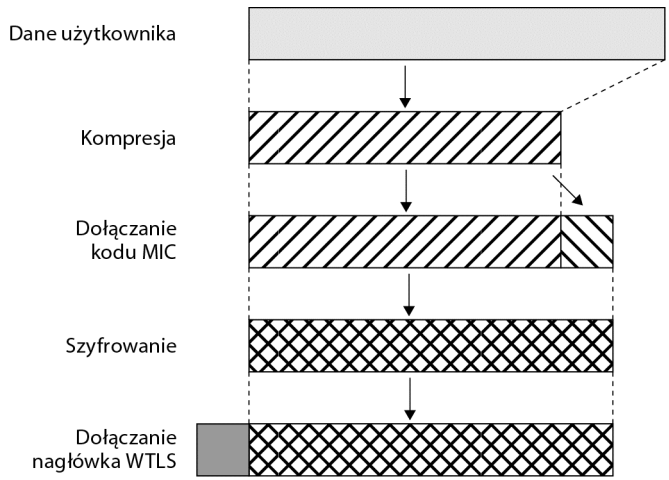
[12] Protokół WTLS obsługuje krótkie klucze do szyfrowania, w takim wypadku efektywnie wykorzystywany rozmiar klucza jest mniejszy niż rozmiar klucza dla danego algorytmu — *przyp. tłum.*




**Rysunek 4.15.** Stos protokołów WTLS

*PODPROTOKÓŁ REKORDU WTLS*

Podprotokół rekordu przejmuje dane od jednego z podprotokołów warstwy wyższej i hermetyzuje je w formie ciągu pakietów PDU według scenariusza przedstawionego poglądowo na rysunku 4.16.




**Rysunek 4.16.** Operacje podprotokołu rekordu WTLS

**Krok 1**. Treść pakietu jest kompresowana w sposób odwracalny (czyli za pomocą algorytmu kompresji bezstratnej).

**Krok 2**. Dla skompresowanych danych obliczany jest kod MIC przy użyciu funkcji HMAC wykorzystującej najczęściej algorytm MD-5 lub SHA-1 (choć są także inne możliwości). Jeżeli kod MIC w ogóle jest tworzony, jego długość wynosi 5 lub 10 bajtów i jest on konkatenowany ze skompresowanymi danymi.

**Krok 3**. Utworzona w kroku 2. konkatenacja skompresowanych danych i kodu MIC zostaje zaszyfrowana przy użyciu algorytmu (do wyboru) DES, 3DES, RC5 lub IDEA.

**Krok 4**. Szyfrogram utworzony w kroku 3. poprzedzany jest nagłówkiem protokołu.

Nagłówek, o którym mowa w kroku 4., ma strukturę przedstawioną na rysunku 4.17 i obejmuje następujące pola:

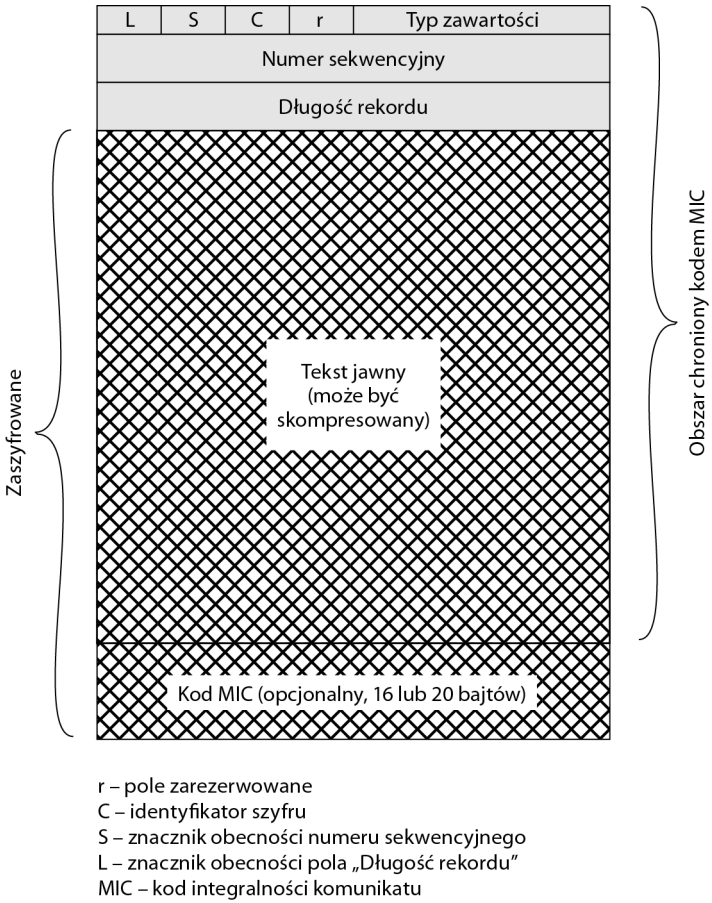
- **Typ rekordu** — ośmiobitowe pole składające się z czterech podpól określających kolejno:
  - **istnienie** (bit równy `1`) lub nieistnienie (bit równy `0`) **pola długości rekordu**;
  - **obecność** (bit równy `1`) lub nieobecność (bit równy `0`) **numeru sekwencyjnego**;
  - **stosowanie** (bit równy `1`) lub niestosowanie (bit równy `0`) **ochrony kryptograficznej** — bit o wartości zero oznacza, że nie jest wykonywana kompresja, obliczanie kodu MIC ani szyfrowanie;
  - **typ zawartości** (4 bity) identyfikujący ten podprotokół warstwy wyższej, dla którego przeznaczone są (lub od którego pochodzą) dane hermetyzowane w rekordzie.
- **Numer sekwencyjny** — 16-bitowa liczba całkowita zwiększająca niezawodność przesyłania PDU za pomocą niepewnej usługi transportowej.
- **Długość rekordu —** 16-bitowa liczba całkowita określająca rozmiar skompresowanych danych (lub danych oryginalnych, gdy kompresja nie jest stosowana).

*PODPROTOKÓŁ ZMIANY SZYFRU*

Jednym z elementów konfiguracji bieżącej transakcji jest określenie parametrów kryptograficznych: algorytmu szyfrowania, algorytmu haszowania wykorzystywanego przez funkcję HMAC, rozmiaru kodu MIC itd. Parametry te stanowią część informacji determinującej stan sesji po jej utworzeniu; dodatkowo w trakcie działania podprotokołu powitalnego tworzony jest stan nieustalony, który po zakończeniu tego działania staje się bieżącym stanem operacyjnym. Podprotokół zmiany szyfru (*Change Cipher Spec Protocol*) jest jednym — i jednocześnie najprostszym — z trzech podprotokołów WTLS warstwy wyższej. W ramach tego podprotokołu wymieniany jest tylko jeden komunikat, w najprostszej chyba możliwej formie — pojedynczego bajtu o wartości 1. Jedynym zadaniem tego komunikatu jest uczynienie stanu nieustalonego sesji jej bieżącym stanem operacyjnym (dla zapisu po stronie nadawcy i dla odczytu po stronie adresata), w wyniku czego zaktualizowany zostaje zestaw szyfrowy używany dla następnych połączeń.

*PODPROTOKÓŁ ALARMOWY*

Zadaniem podprotokołu alarmowego jest informowanie partnera o sytuacjach wyjątkowych związanych z protokołem WTLS. Komunikaty tego podprotokołu są kompresowane i szyfrowane zgodnie z ustawieniami aktualnego stanu połącze-




**Rysunek 4.17.** Format rekordu WTLS

nia. Każdy taki komunikat składa się z dwóch bajtów. W pierwszym bajcie znajduje się wskaźnik istotności błędu: wartość 1 oznacza ostrzeżenie, wartość 2 — sytuację krytyczną, wartość 3 — błąd fatalny. W drugim bajcie znajduje się kod określający bliżej przyczynę błędu. Wystąpienie błędu fatalnego (3) powoduje natychmiastowe zakończenie bieżącego połączenia i zablokowanie możliwości nawiązywania nowych połączeń w tej samej sesji; kontynuowane są jedynie pozostałe połączenia istniejące już w jej ramach. Błąd krytyczny (2) powoduje natychmiastowe zakończenie bieżącego połączenia, jednakże bez konsekwencji dla samej sesji, w ramach której w dalszym ciągu nawiązywać można nowe połączenia.

Mechanizm alertów służy również do rozwiązywania (zamykania) połączeń i sesji. Alert `connection_close_nofity` (wartość 0) lub `session_close_notify` (wartość 1) może być wysłany przez każdą ze stron; druga strona po jego odebraniu ignoruje ewentualne następne komunikaty w ramach bieżącego połączenia lub sesji, powinna natomiast obowiązkowo także wysłać bliźniaczy alert jako potwierdzenie.

Alerty są standardowym środkiem radzenia sobie przez encje z sytuacjami wyjątkowymi. Encja, która taką sytuację wykryje, informuje o niej encję-partnera; dalszy przebieg wydarzeń uwarunkowany jest specyfiką konkretnego błędu. Wśród błędów fatalnych wymienić należy między innymi poniższe:

- `unexpected_message` (wartość 10) — oznacza otrzymanie nieprawidłowego lub nierozpoznanego komunikatu;
- `bad_record_mac` (wartość 20) — oznacza nieadekwatność kodu MIC dołączonego do komunikatu;
- `decompression_failure` (wartość 30) — oznacza niewykonalność dekompresji lub otrzymanie w jej wyniku bloku o rozmiarze przekraczającym dopuszczalną wartość;
- `handshake_failure` (wartość 40) — oznacza niemożność wynegocjowania (w ramach dostępnych opcji) zbioru parametrów bezpieczeństwa akceptowalnego przez obie strony komunikacji;
- `illegal_parameter` (wartość 47) — oznacza, że przynajmniej jedno z pól komunikatu podprotokołu powitalnego ma wartość wykraczającą poza dopuszczalny zakres lub niespójną z zawartością pozostałych pól.

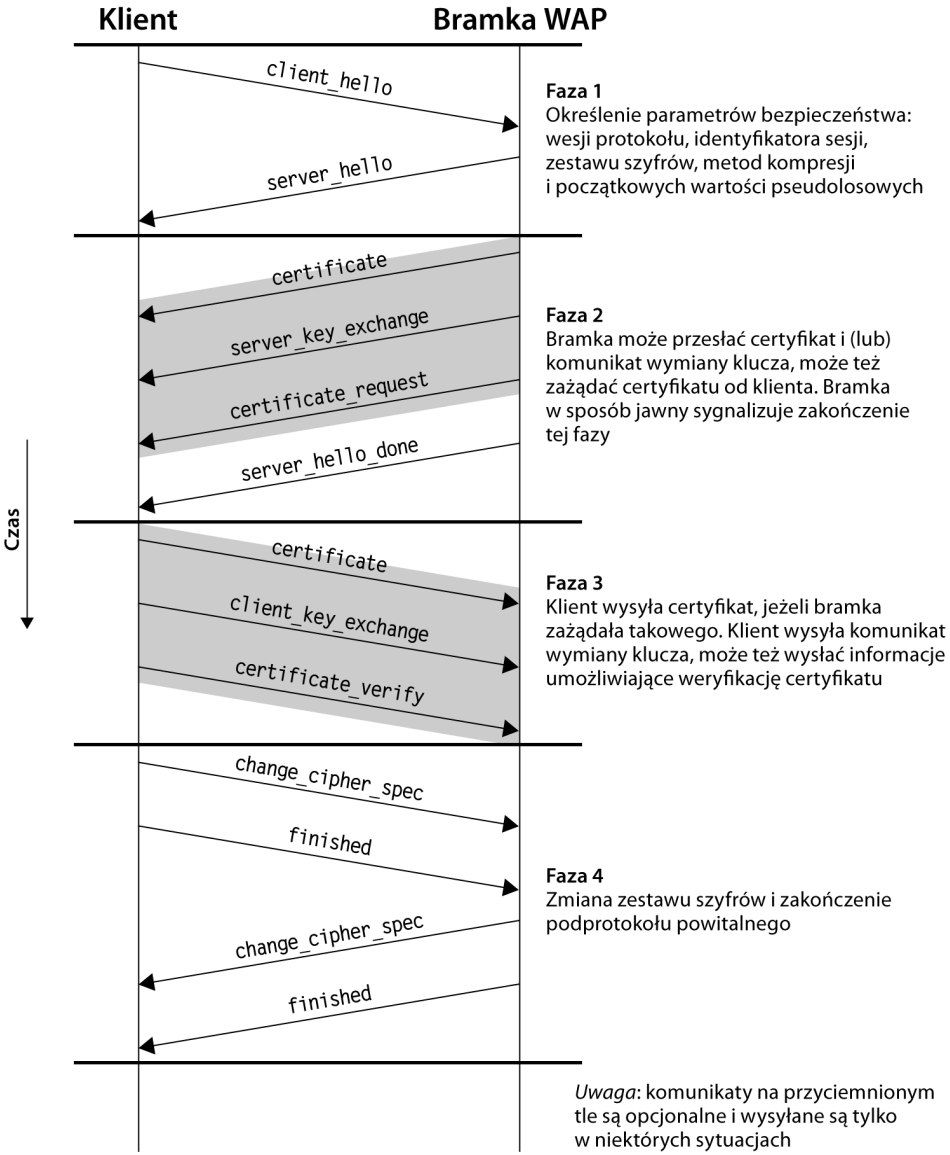
Do alertów niefatalnych zaliczają się natomiast (między innymi) następujące:

- `bad_certificate` (wartość 42) — otrzymany certyfikat jest uszkodzony, na przykład zawarty w nim podpis został negatywnie zweryfikowany;
- `unsupported_certificate` (wartość 43) — otrzymano certyfikat nieobsługiwanego typu;
- `certificate_revoked` (wartość 44) — otrzymano certyfikat unieważniony przez wydawcę;
- `certificate_expired` (wartość 45) — otrzymano certyfikat przeterminowany;
- `certificate_unknown` (wartość 46) — odrzucono certyfikat z przyczyn innych niż wymienione powyżej.

*PODPROTOKÓŁ POWITALNY*

Podprotokół powitalny (*WTLS Handshake protocol*) to najbardziej skomplikowany podprotokół WTLS. Jego zadaniem jest wzajemne uwierzytelnianie klienta i bramki WAP oraz negocjowanie parametrów kryptograficznych chroniących połączenie — algorytmów oraz kluczy szyfrowania i obliczania kodów MIC. W ramach podprotokołu powitalnego skonstruowany zostaje **sekret wstępny** (*pre-master secret*) służący do utworzenia **sekretu głównego** (*master secret*), który z kolei wykorzystywany jest do generowania rozmaitych kluczy kryptograficznych.

Funkcjonowanie protokołu powitanego wiąże się z wymianą serii komunikatów między klientem a bramką WAP według scenariusza przedstawionego na rysunku 4.18. Scenariusz ten rozpatrywać można w podziale na cztery fazy.




**Rysunek 4.18.** Akcje podprotokołu powitalnego WTLS

W **fazie pierwszej** następuje zainicjowanie połączenia i uzgodnienie mechanizmów chroniących jego bezpieczeństwo. Fazę tę rozpoczyna klient, wysyłając do bramki komunikat `client_hello`, zawierający między innymi identyfikator sesji oraz listę proponowanych algorytmów szyfrowania i kompresji, w kolejności malejących preferencji. Po wysłaniu komunikatu klient oczekuje na odpowiedź bramki w postaci komunikatu `server_hello`, zawierającego między innymi wybór algorytmu kompresji i algorytmu szyfrowania spośród zaproponowanych przez klienta.

**Faza druga** to uwierzytelnianie bramki i wymiana klucza. Fazę tę rozpoczyna bramka, wysyłając swój certyfikat, gdy ten jest niezbędny do uwierzytelnienia. Kolejny komunikat — `server_key_exchange` — wysyłany jest tylko dla niektórych algorytmów wymiany klucza. W następnej kolejności bramka oczekuje na certyfikat klienta, wysyłając mu w związku z tym komunikat `certificate_request`. Ostatnim, i bezwzględnie w tej fazie wymaganym, komunikatem jest wysyłany przez bramkę komunikat `server_hello_done` sygnalizujący zakończenie wysyłania komunikatów przez bramkę i jej przejście w tryb oczekiwania na komunikaty klienta (komunikat ten nie posiada żadnych parametrów).

**Faza trzecia** obejmuje uwierzytelnianie klienta oraz wymianę klucza. Po otrzymaniu komunikatu `server_hello_done` klient powinien zweryfikować, czy okazany przez bramkę certyfikat jest prawidłowy i czy poprawne są parametry przesłane w komunikacie `server_hello`. Po pomyślnym wyniku obu tych weryfikacji klient przystępuje do wysyłania komunikatów do bramki. Jeśli bramka zażądała certyfikatu, klient dostarcza takowy. Wymaganym w tej fazie komunikatem jest `client_key_exchange`, którego treść zależna jest od konkretnej metody wymiany klucza. Opcjonalnie klient może przesłać także informacje jawnie weryfikujące jego certyfikat, w postaci komunikatu `certificate_verify`.

W **fazie czwartej** finalizuje się ustanawianie bezpiecznego połączenia. Klient wysyła do bramki komunikat `change_cipher_spec` i sam uaktualnia specyfikację szyfru po swojej stronie, czyniąc stan nieustalony połączenia jego stanem bieżącym. Zauważmy, że komunikat ten nie jest uważany za część podprotokołu powitalnego, lecz wysyłany jest w ramach podprotokołu zmiany szyfru. Następnie klient wysyła komunikat `finished` zawierający hasz obliczony na podstawie nowych algorytmów, kluczy i sekretów; zadaniem tego komunikatu jest zweryfikowanie poprawności procesów uzgadniania klucza i uwierzytelniania. W odpowiedzi na oba wymienione komunikaty bramka odsyła komunikat `change_cipher_spec`, uaktualnia stan operacyjny połączenia po swojej stronie i kończy dialog wysłaniem komunikatu `finished`. W tym momencie połączenie można uznać za nawiązane, podprotokół powitalny kończy swe działanie, a klient i bramka mogą zacząć wymianę danych na poziomie warstwy aplikacji.

### Algorytmy kryptograficzne

*UWIERZYTELNIANIE*

Protokół WTLS opiera uwierzytelnianie na certyfikatach. Uwierzytelnianie może mieć charakter wzajemny między klientem a bramką, może być także ograniczone do uwierzytelniania bramki wobec klienta; co więcej, w specyfikacji WTLS uwierzytelnianie w ogóle jest procedurą opcjonalną. Obecnie WTLS rozpoznaje i honoruje certyfikaty w formatach X.509v3, X9.68 i swym własnym formacie — ten ostatni jest zoptymalizowany pod względem rozmiaru i obejmuje pola zawierające (porównaj z rysunkiem 1.14):

- wersję certyfikatu,
- algorytm podpisu na certyfikacie,

- identyfikator wydawcy,
- początkową i końcową datę ważności,
- identyfikator właściciela certyfikatu,
- typ (algorytm) certyfikowanego klucza publicznego,
- parametry certyfikowanego klucza publicznego,
- sam certyfikowany klucz,
- podpis sporządzony za pomocą klucza publicznego urzędu certyfikacji.

*WYMIANA KLUCZA*

Celem protokołu WTLS jest uzgodnienie przez klienta i bramkę wartości zwanej **sekretem wstępnym** (*pre-master secret*) i używanej do generowania **sekretu głównego** (*master secret*) w sposób opisany w dalszym ciągu. WTLS obsługuje kilka protokołów wymiany kluczy. Protokoły te podzielić można na dwie grupy: te, które wymagają obecności komunikatu `server_key_exchange` w podprotokole powitalnym, i te, które go nie wymagają.

Komunikat `server_key_exchange` wysyłany jest przez bramkę tylko wtedy, gdy informacje zawarte w wysłanym przez bramkę komunikacie `certi ↪ficate` (jeśli w ogóle taki został wysłany) nie są wystarczające do wygenerowania sekretu wstępnego przez klienta. Jest tak w przypadku trzech następujących metod wymiany klucza:

- `DH_anon` — klucz *pre-master secret* uzgodniony zostaje między klientem a bramką zgodnie z klasycznym algorytmem Diffiego-Hellmana w sposób anonimowy, czyli bez uwierzytelniania.
- `ECDH_anon` — jak w metodzie `DH_anon`, z tą różnicą, że używany jest algorytm Diffiego-Hellmana z krzywymi eliptycznymi.
- `RSA_anon` — to anonimowa wymiana kluczy za pomocą algorytmu RSA. Bramka wysyła klientowi swój klucz publiczny RSA; klient wybiera losowo 20-bajtową tajną wartość, szyfruje ją otrzymanym kluczem i odsyła do bramki, która rozszyfrowuje otrzymaną przesyłkę za pomocą swego klucza prywatnego. Konkatenacja tajnej wartości wybranej przez klienta i klucza publicznego bramki staje się uzgodnionym kluczem *pre-master secret*.

Komunikat `server_key_exchange` nie jest potrzebny w przypadku następujących metod:

- `ECDH_ECDSA` — to wymiana klucza metodą Diffiego-Hellmana z krzywymi eliptycznymi, oparta na certyfikatach podpisanych algorytmem ECDSA. Bramka przesyła klientowi swój certyfikat klucza publicznego, podpisany przez zaufanego (z perspektywy klienta) wydawcę. Klient, zależnie od tego, czy jest uwierzytelniany, czy nie, przesyła do bramki albo swój certyfikat klucza publicznego ECDH (z podpisem ECDSA), albo (wygenerowany ad

hoc, tymczasowy) klucz publiczny ECDH. Każda ze stron oblicza następnie klucz *pre-master secret* na podstawie własnego klucza prywatnego i klucza publicznego partnera.

- `RSA` — ta wymiana klucza odbywa się w oparciu o certyfikaty RSA. Bramka przesyła klientowi swój certyfikat klucza RSA, podpisany przez wydawcę cieszącego się zaufaniem klienta. Klient generuje swą tajną wartość, szyfruje ją kluczem publicznym wydobytym z otrzymanego certyfikatu i przesyła do bramki. Obie strony konstruują następnie klucz *pre-master secret* jako konkatenację tajnej wartości klienta i klucza publicznego bramki. Jeśli wymagane jest uwierzytelnienie klienta, ten podpisuje swym kluczem prywatnym zbiór komunikatów wymienianych w ramach podprotokołu powitalnego i przesyła podpis do bramki wraz z certyfikatem swego klucza.

*FUNKCJA PSEUDOLOSOWA (PRF)*

Protokół WTLS wykorzystuje funkcję pseudolosową do różnych celów. Jej argumentami są: tajna wartość (`secret`), ziarno (`seed`) i etykieta (`label`) precyzująca konkretne zastosowanie, wynik zaś jest strumieniem bajtów o żądanej długości. W standardzie TLS wykorzystywane są dwa algorytmy haszujące, by uczynić PRF jak najbardziej bezpieczną; w przypadku protokołu WTLS względy oszczędnościowe zadecydowały o ograniczeniu się tylko do jednego algorytmu, który uzgadniany jest między klientem a bramką na etapie podprotokołu powitalnego.

Obliczanie PRF opiera się na wykorzystywaniu specyficznej funkcji rozszerzającej `P_hash`, określonej wzorem

```
P_hash(secret, seed)= HMAC_hash(secret, A(1) || seed) ||
                      HMAC_hash(secret, A(2) || seed) ||
                      HMAC_hash(secret, A(3) || seed) || . . .
```

gdzie || oznacza konkatenację, `seed` jest ziarnem generowania, a wartości $A()$ definiowane są w sposób rekurencyjny:

$$A(0) = seed$$
$$A(i) = HMAC\_hash(secret, A(i-1))$$

przy czym liczba wykonywanych iteracji (maksymalna wartość $i$) uzależniona jest od żądanej długości ciągu wynikowego. Związek PRF z funkcją rozszerzającą `P_hash` wyraża się ostatecznie wzorem

```
PRF(secret, label, seed) = P_hash(secret, label || seed)
```

*GENEROWANIE SEKRETU GŁÓWNEGO*

Współdzielony **sekret główny** (*master secret key*) to niepowtarzalny, unikatowy dla danej sesji ciąg 20 bajtów (160 bitów) generowany drogą bezpiecznej wymiany klucza. Jego generowanie odbywa się w dwóch etapach: najpierw między stronami wymieniany jest sekret wstępny (*pre-master secret*), na podstawie którego obie strony przeprowadzają następnie właściwe generowanie według wzoru

```
master_secret = PRF(pre_master_secret,
                    "master secret",
                    ClientHello.random || ServerHello.random
                   )
```

gdzie `ClientHello.random` i `ServerHello.random` są wartościami wymienionymi między klientem a bramką w pierwszej fazie podprotokołu powitalnego.

Z obliczonego `master_secret` wyprowadzane są następnie klucze dla obliczania kodu MIC i szyfrowania. Obliczanie kodu MIC odbywa się przy użyciu algorytmu HMAC (patrz sekcja 12.5 (tom I)) z następującymi argumentami

```
HMAC_hash (MIC_secret,
           seq_number || WTLSCompressed.record_type
                      || WTLSCompressed.length
                      || WTLSCompressed.fragment)
```

gdzie `WTLSCompressed.fragment` odnosi się do skompresowanej porcji danych w komunikacie (a gdy kompresja nie jest stosowana — do danych oryginalnych).

Funkcja HMAC może wykorzystywać algorytm haszujący MD5 albo SHA-1.

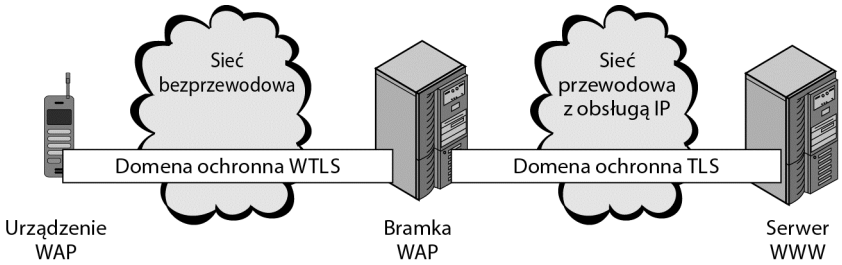
Szyfrowany jest cały rekord WTLS *z wyjątkiem nagłówka*. Dopuszczalne są następujące schematy szyfrowania:

- RC5 z kluczem 40-, 56-, 64- lub 28-bitowym;
- DES z kluczem 192-bitowym;
- 3DES z kluczem 40-bitowym;
- IDEA z kluczem 40 lub 56-bitowym.

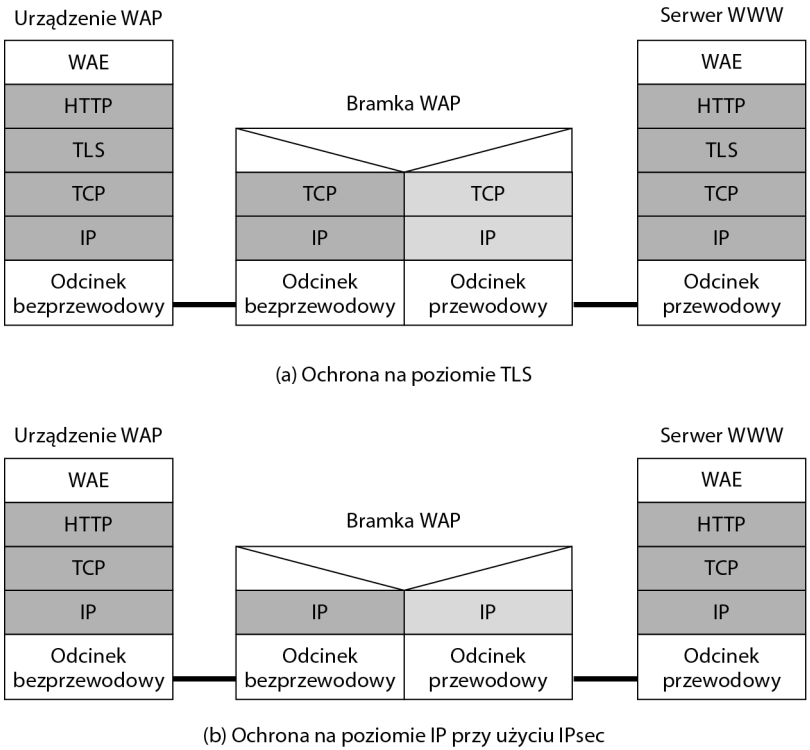
## 4.5. CAŁOŚCIOWE ZABEZPIECZENIE TRANSMISJI WAP

W podstawowym modelu transmisji WAP, widocznym na rysunku 4.19 (który jest odpowiednikiem rysunku 4.14), obejmującym klienta, bramkę i serwer WWW, istnieje zasadnicza luka: na odcinku między klientem a bramką transmisja zabezpieczana jest za pomocą protokołu WTLS, na odcinku między bramką a serwerem WWW — za pomocą protokołu TLS, natomiast sama bramka jako taka bezpieczna nie jest, ponieważ przetwarzanie danych wewnątrz niej odbywa się bez szyfrowania. Dane te mogą więc zostać łatwo skompromitowane.

Wypracowano kilka podejść do zapewnienia bezpieczeństwa na całym odcinku transmisji — od klienta do serwera WWW. W wersji 1 WAP opracowano w tym celu uproszczony zbiór protokołów przy założeniu, że sieć bezprzewodowa nie obsługuje protokołu IP. W wersji 2 WAP (WAP2) istnieje natomiast opcja implementacji w urządzeniu mobilnym protokołu TCP/IP, oczywiście przy założeniu, że sieć bezprzewodowa obsługuje protokół IP. Na rysunku 4.20 pokazano dwa sposoby realizacji tego pomysłu; w obu przypadkach urządzenie mobilne implementuje protokoły TCP/IP oraz HTTP.




**Rysunek 4.19.** Strefy ochronne w klasycznym protokole WAP

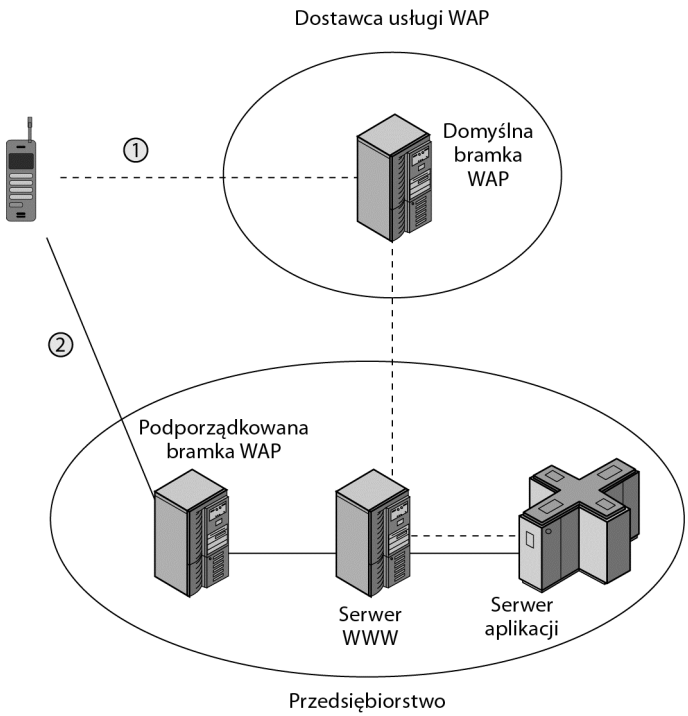



**Rysunek 4.20.** Przykładowe podejścia do całościowej ochrony transmisji WAP2

W pierwszym wariancie, widocznym w części (a) rysunku, między urządzeniem mobilnym a serwerem WWW nawiązana zostaje sesja TLS. Rola bramki WAP ogranicza się do bramy na poziomie TCP i przekaźnika transmisji między dwiema sieciami (bezprzewodową i WWW). Rekordy TLS przechodzą przez bramkę WAP w postaci zaszyfrowanej, są więc w tym miejscu bezpieczne.

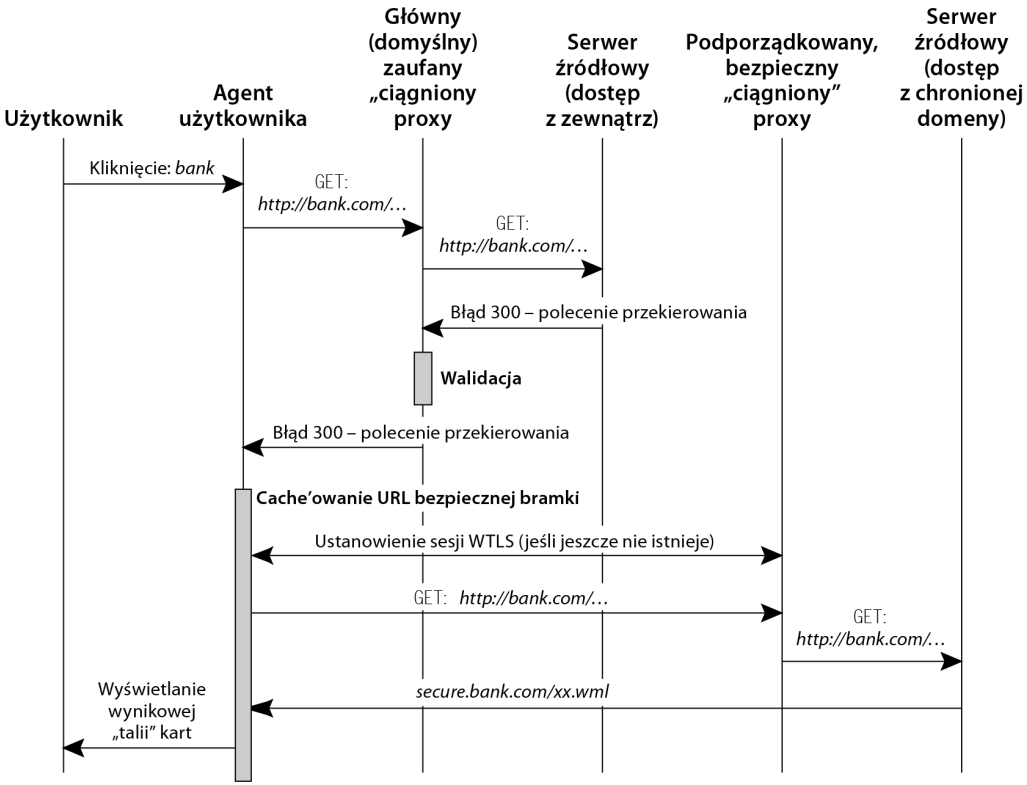
W podejściu widocznym w części (b) rysunku bramka WAP zredukowana została do roli zwykłego routera IP. Bezpieczeństwo całej transmisji zapewniane jest na poziomie protokołu IP za pomocą IPsec (opisywanego w rozdziale 6.).

Na rysunku 4.21 (zaczerpniętym z pracy [ASHL01]) pokazano natomiast rozwiązanie nieco bardziej skomplikowane, opisane przez WAP forum w specyfikacji zatytułowanej „WAP Transport Layer End-to-End Security". Bazuje ono na jednym z mechanizmów protokołu HTTP — automatycznym przekierowaniu, będącym wynikiem zwrócenia przez serwer WWW komunikatu o kodzie 300. Klient łączy się z bramką WAP, a za jej pośrednictwem z serwerem WWW. Serwer WWW odpowiada wspomnianym komunikatem, skutkującym automatycznym przekierowaniem klienta *do innej bramki WAP*, znajdującej się (wraz z serwerem WWW) w granicach chronionej domeny przedsiębiorstwa, i nawiązaniem z tą bramką połączenia WTLS. Po zakończeniu tego połączenia przywrócone zostaje skojarzenie klienta z pierwotną bramką WAP, za pośrednictwem której będzie łączył się z innymi serwerami WWW. Oczywiście opisane rozwiązanie wymaga zainstalowania bramki WAP w chronionej domenie przedsiębiorstwa i zapewnienia klientowi dostępu do tej bramki.




**Rysunek 4.21.** Całościowa ochrona transmisji WAP z wykorzystaniem przekierowania HTTP

Przebieg opisanego dialogu zilustrowano na rysunku 4.22, zaczerpniętym ze specyfikacji WAP.




**Rysunek 4.22.** Przykład całościowego zabezpieczenia transmisji WAP na poziomie warstwy transportowej, z wykorzystaniem przekierowania HTTP

## 4.6. ZALECANE MATERIAŁY UZUPEŁNIAJĄCE

Specyfikacje IEEE 802.11 i Wi-Fi opisane są szczegółowo w książce [STAL07]. Doskonałym ujęciem tematyki jest także książka [ROSH04]. W publikacji [FRAN07] potraktowano tematykę IEEE 802.11i w sposób bardzo szczegółowy, lecz jednocześnie bardzo przystępny. Ogólne ujęcie IEEE 802.11i dostępne jest w pracy [CHEN05].

ASHL01 Ashley P., Hinton H., Vandenwauver M., „Wired versus Wireless Security: The Internet, WAP and iMode for E-Commerce", *Proceedings, Annual Computer Security Applications Conference*, 2001.

CHEN05 Chen J., Jiang M., Liu Y., *Wireless LAN Security and IEEE 802.11i*, „IEEE Wireless Communications", luty 2005.

FRAN07 Frankel S., Eydt B., Owens L., Scarfone K., *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Special Publication SP 800-97, luty 2007.

ROSH04 Roshan P., Leary J., *802.11 Wireless LAN Fundamentals*, Cisco Press, Indianapolis, 2004.
STAL07 Stallings W., *Data and Computer Communications, Eighth Edition*, Prentice Hall, Upper Saddle River, 2007.

### Polecane strony WWW

- **The IEEE 802.11 Wireless LAN Working Group**: dokumenty grupy roboczej i archiwa dyskusji.
- **Wi-Fi Alliance**: grupa organizacji promująca współdziałanie produktów 802.11 i ich współpracę z Ethernetem.
- **Wireless LAN Association**: wprowadzenie do technologii sieci bezprzewodowych wraz z dyskusją na tematy implementacyjne i analizami przypadku dostarczonymi przez użytkowników. Strona zawiera odsyłacze do innych stron o podobnej tematyce.
- **Extensible Authentication Protocol (EAP) Working Group**: grupa robocza IETF odpowiedzialna za protokół EAP i związane z nim problemy. Strona zawiera dokumenty RFC i szkice standardów.
- **Open Mobile Alliance**: strona organizacji powstałej z połączenia WAP Forum i Open Mobile Architecture Initiative. Zawiera specyfikację WAP i odsyłacze do powiązanych stron.

## 4.7. KLUCZOWE TERMINY, PYTANIA PRZEGLĄDOWE I PROBLEMY

### Kluczowe terminy

4-stronne potwierdzanie (*4-way handshake*)
algorytm Michael
bezpieczeństwo bezprzewodowej warstwy transportowej (*Wireless Transport Layer Security* — WTLS)
bezprzewodowy protokół datagramów (*Wireless Datagram Protocol* — WDP)
bezprzewodowy protokół sesji (*Wireless Session Protocol* — WSP)
bezprzewodowy protokół transakcji (*Wireless Transaction Protocol* — WTP)
chroniony dostęp Wi-Fi (*Wi-Fi Protected Access* — WPA)
funkcja pseudolosowa (*pseudorandom function* — PRF)
IEEE 802.11
IEEE 802.11i
IEEE 802.1X
jednostka danych protokołu MAC (*MAC protocol data unit* — MPDU)
jednostka danych usługi MAC (*MAC service data unit* — MSDU)
język WML (*Wireless Markup Language*)
klucze grupowe (*group keys*)
klucze selektywne (*pairwise keys*)
kod integralności komunikatu (*message integrity code* — MIC)
niezależny BSS (*independent BSS* — IBSS)

podprotokół alarmowy (*Alert Protocol*)
podprotokół powitalny (*Handshake Protocol*)
podprotokół rekordu WTLS (*WTLS Record Protocol*)
podprotokół zmiany szyfru (*Change Cipher Spec Protocol*)
podstawowy zbiór usług (*basic service set* — BSS)
protokół aplikacji bezprzewodowych (*Wireless Application Protocol* — WAP)
protokół CCMP (*Counter Mode-CBC MAC Protocol*)
protokół TKIP (*Temporal Key Integrity Protocol*)
protokół WEP (*Wired Equivalent Privacy*)
punkt dostępowy (*access point* — AP)
Robust Security Network (*Robust Security Network* — RSN)
rozszerzony zestaw usług (*extended service set* — ESS)
sieć bezprzewodowa (*wireless LAN* — WLAN)
sterowanie dostępem do nośnika (*media access control* — MAC)
sterowanie łączem logicznym (*logical link control* — LLC)
system dystrybucyjny (*distribution system* — DS)
środowisko aplikacji bezprzewodowych (*Wireless Application Environment* — WAE)
*Wi-Fi*

## Pytania przeglądowe

**4.1.** Jakie są podstawowe komponenty sieci bezprzewodowej standardu IEEE 802.11?
**4.2.** Zdefiniuj pojęcie rozszerzonego zestawu usług.
**4.3.** Wymień i krótko zdefiniuj usługi standardu IEEE 802.11.
**4.4.** Czy system dystrybucyjny jest siecią bezprzewodową?
**4.5.** W jaki sposób koncepcja skojarzenia związana jest z koncepcją mobilności?
**4.6.** Jakie aspekty bezpieczeństwa uwzględnione zostały w standardzie IEEE 802.11i?
**4.7.** Opisz krótko cztery fazy operacji IEEE 802.11i.
**4.8.** Czy TKIP różni się od CCMP?
**4.9.** Jaka jest różnica między filtrem HTML a proxy WAP?
**4.10.** Jakie usługi udostępniane są przez WSP?
**4.11.** W jakich zastosowaniach okazują się przydatne poszczególne klasy transakcji WTP?
**4.12.** Wymień i krótko zdefiniuj usługi bezpieczeństwa oferowanie przez WTLS.
**4.13.** Opisz krótko cztery podprotokoły protokołu WTLS.
**4.14.** Wymień i krótko zdefiniuj klucze używane przez protokół WTLS.
**4.15.** Opisz trzy podejścia do zapewnienia bezpieczeństwa na całym odcinku łączności między urządzeniem bezprzewodowym a serwerem WWW.

## Problemy

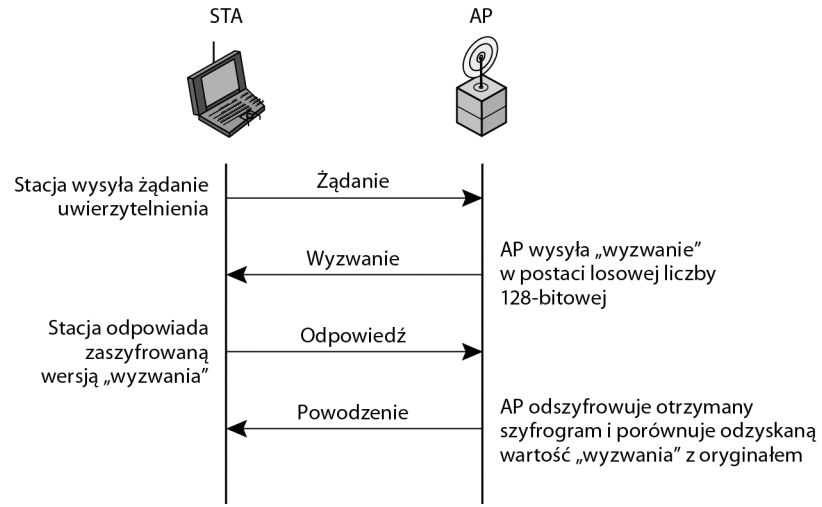
**4.1.** Uwierzytelnianie otwarte (*open system authentication*), zdefiniowane w IEEE 802.11, obejmuje prostą wymianę dwóch komunikatów. Klient wysyła komunikat zawierający identyfikator stacji (najczęściej jest to jej adres MAC), a punkt dostępowy (router) odpowiada komunikatem sygnalizującym akceptację albo odmowę; jednym z powodów odmowy może być obecność przesłanego adresu MAC na liście wykluczeń punktu dostępowego.
**a)** Jakie korzyści wynikają z takiego schematu uwierzytelniania?
**b)** Jakie zagrożenie niesie ze sobą ten schemat?

**4.2.** Przed pojawieniem się standardu IEEE 802.11i podstawowym schematem zabezpieczenia sieci bezprzewodowych standardu IEEE 802.11 był WEP (*Wired Equivalent Privacy* — dosł. prywatność równoważna [osiągalnej w sieci] przewodowej). Podstawowym założeniem WEP jest współdzielenie *jednego* klucza przez wszystkie urządzenia w sieci, a uwierzytelnienie danego urządzenia sprowadza się do udowodnienia znajomości tego klucza. Ciąg związanych z tym komunikatów przedstawiony został na rysunku 4.23. STA wysyła do AP żądanie uwierzytelnienia, na co AP odpowiada „wyzwaniem" mającym postać ciągu 128 losowych bitów. STA szyfruje ów ciąg wspomnianym kluczem i odsyła szyfrogram do AP, który po rozszyfrowaniu porównuje odzyskany tekst jawny z oryginalnym „wyzwaniem" i na podstawie wyniku tego porównania akceptuje albo odrzuca żądanie STA.

**a)** Jakie są zalety takiego schematu uwierzytelniania?

**b)** W opisanym schemacie uwierzytelnienia brakuje jednego ważnego elementu — jakiego? Dlaczego jest on tak istotny? *Wskazówka*. Wspomniany brak można zniwelować za pomocą jednego lub dwóch dodatkowych komunikatów.

**c)** Jakie są słabe strony przedstawionego schematu?




**Rysunek 4.23.** Uwierzytelnianie WEP

**4.3.** W schemacie WEP integralność i poufność danych uzyskuje się za pomocą szyfru strumieniowego RC4. Nadawca MPDU wykonuje poniższy scenariusz, zwany hermetyzacją:

1. Nadawca wysyła wartość początkową wektora *IV*.
2. Wartość *IV* jest konkatenowana z kluczem WEP, dając w rezultacie ziarno stanowiące klucz wejściowy szyfru RC4.
3. Dla całego pola danych ramki MAC obliczana jest 32-bitowa suma kontrolna CRC. CRC to podstawowy środek detekcji błędów w protokołach sterowania łączem danych, w tym przypadku jednak pełniący wartość kontrolną integralności (*integrity check value*, w skrócie *ICV*).
4. Konkatenacja danych i sumy kontrolnej z punktu 3. szyfrowana jest algorytmem RC4, co daje w wyniku blok szyfrogramu.

5. Blok szyfrogramu z punktu 4. poprzedzany jest wektorem *IV* (w oryginalnej, niezaszyfrowanej postaci), w wyniku czego powstaje hermetyzowana MPDU przeznaczona do transmisji.
   a) narysuj schemat blokowy opisanej hermetyzacji;
   a) opisz kolejne kroki, jakie wykonać musi odbiorca MPDU w celu zweryfikowania jej poprawności i odzyskania oryginalnej treści;
   c) narysuj schemat blokowy scenariusza z punktu b).

**4.4.** Jednym ze słabych elementów WEP jest ochrona integralności za pomocą kodu CRC, który to kod stanowi liniową funkcję chronionych danych: można łatwo przewidzieć, które bity CRC ulegną zmianie w wyniku zmiany wartości konkretnego bitu danych wejściowych. Co więcej, można stosunkowo nietrudno zidentyfikować taki sposób zmodyfikowania oryginalnych danych, by chroniący je kod CRC pozostał niezmieniony. W protokole WEP jednak, jeśli potencjalny intruz nie zna klucza szyfrowania, nie ma dostępu do oryginalnych danych i chroniącego je CRC, bo zostały one zaszyfrowane w punkcie 4. scenariusza opisanego w zadaniu 4.3. Czy to oznacza, że atak eksploatujący opisaną własność CRC nie jest możliwy do przeprowadzenia? Uzasadnij odpowiedź.

**4.5.** Jedną z potencjalnych słabości WTLS jest wykorzystywanie trybu operacyjnego CBC, przy czym wektor inicjacyjny *IV* obliczany jest ze wzoru $IV = IV_0 \oplus S$, gdzie $IV_0$ jest oryginalną wartością wektora inicjacyjnego, a *S* jest ciągiem o długości tożsamej z długością *IV*, powstającym w wyniku wielokrotnego powtórzenia 2-bajtowego numeru sekwencyjnego rekordu (jeżeli na przykład *IV* jest 8-bajtowy, to *S* jest wynikiem czterokrotnego powtórzenia). Zgodnie z trybem CBC pierwszy blok rekordu o numerze sekwencyjnym *i* przekształcany jest na pierwszy blok szyfrogramu według następującej formuły (por. rysunek 6.4 (tom I)).

$$C_1 = \mathrm{E}\,(K, (IV \oplus S \oplus P_{s,1}))$$

gdzie $P_s$ jest rekordem o numerze sekwencyjnym *s*, *C* jest wynikowym szyfrogramem, a *S* jest ciągiem stanowiącym wynik wielokrotnego powtórzenia *s*. Rozpatrzmy aplikację terminalową (na przykład *telnet*), która każde naciśnięcie klawisza kwituje wysłaniem osobnego komunikatu; załóżmy, że w aplikacji tej Alicja wprowadza właśnie swe hasło, a podstępna Ewa dąży do odgadnięcia tego hasła. W przechwytywanych przez Ewę rekordach numery sekwencyjne nie są szyfrowane (patrz rysunek 4.17), jeżeli więc Ewa uzyska dostęp do kanału wykorzystywanego przez Alicję, może ona wprowadzać do tego kanału (niezaszyfrowane) rekordy i obserwować rezultat ich szyfrowania. Zaproponuj metodę ataku siłowego, dzięki któremu Ewa będzie mogła odgadywać poszczególne litery hasła wprowadzanego przez Alicję. *Wskazówka*. Wykorzystaj następujące właściwości operacji XOR:

$$x \oplus x = 1$$
$$x \oplus 1 = x$$

**4.6.** Wczesne wersje WTLS bazowały na uwierzytelnianiu za pomocą 40-bitowego kodu XOR MAC i szyfrowaniu za pomocą algorytmu RC4. Wspomniany kod MAC oblicza się, dopełniając komunikat bajtami zerowymi do wielokrotności 5 bajtów, następnie składając za pomocą operacji XOR kolejne porcje 5-bajtowe. Pokaż, że schemat ten nie zapewnia ochrony integralności komunikatu.

# SKOROWIDZ

## C

## D



## E



## F

## G



## H



## I

## J



## K

## Ł



## M



## N



## O

## P

## Q



## R



## S

## T



## U

## X



## Z

**Wirusy, hakerzy, szpiegostwo gospodarcze, elektroniczne podsłuchy i kradzieże — era Internetu ma także ciemną stronę, która stawia przed nami coraz większe wyzwania w zakresie bezpieczeństwa informacji**. Dla większości organizacji kwestie ochrony dostępu do danych przechowywanych w systemach komputerowych i wymienianych między nimi, a także skutecznego odpierania ataków sieciowych, stały się zagadnieniem mogącym przesądzić o ich istnieniu. Bezpieczeństwo sieci ma także ogromne znaczenie dla zwykłych użytkowników Internetu, często przetrzymujących na dyskach poufne dokumenty i korzystających z bankowości elektronicznej. Na szczęście mamy już dziś świetne technologie i narzędzia związane z bezpieczeństwem sieci komputerowych oraz kryptografią. Jedyne, co musisz zrobić, to uzbroić się w wiedzę, jak skutecznie je wykorzystać.

**Oto druga część wyczerpującego przewodnika po praktycznych zastosowaniach kryptografii oraz mechanizmach bezpieczeństwa pozwalających na skuteczną ochronę informacji, sieci i systemów komputerowych**. Ten adresowany zarówno do studentów, jak i zawodowców podręcznik podzielono na trzy naszpikowane wiedzą i ciekawymi przykładami części, wprowadzające kolejno w szyfry symetryczne, szyfry asymetryczne i kryptograficzne algorytmy ochrony integralności danych. Przeczytasz tu m.in. o trybach operacyjnych szyfrów blokowych oraz przyjrzysz się standardowi AES i generowaniu liczb pseudolosowych. Otrzymasz obszerną prezentację algorytmów kryptograficznych i doskonały przewodnik po metodach uwierzytelniania. Ponadto nauczysz się efektywnie wykorzystywać system Sage — wieloplatformowe, darmowe narzędzie z użytecznym, elastycznym i łatwym do opanowania systemem obliczeń algebraicznych związanych z kryptografią. Znajdziesz tu także gotowe dla tego systemu przykłady, ilustrujące praktyczne zastosowania teorii liczb i algorytmów kryptograficznych.

- Zarządzanie kluczami i ich dystrybucja
- Uwierzytelnianie użytkowników
- Bezpieczeństwo transportu danych
- Bezpieczeństwo sieci bezprzewodowych
- Bezpieczeństwo poczty elektronicznej
- Bezpieczeństwo protokołu IP
- Bezpieczeństwo systemu
- Wykrywanie intruzów
- Szkodliwe oprogramowanie
- Rozproszone ataki DoS
- Firewalle
- Prawne i etyczne aspekty bezpieczeństwa komputerowego
- Własność intelektualna
- Ochrona prywatności

**William Stallings** *jest autorem siedemnastu książek z zakresu technicznych aspektów bezpieczeństwa informacji i sieci komputerowych. Jest jedenastokrotnym laureatem nagrody za najlepszą książkę informatyczną roku, przyznawanej przez Text and Academic Authors Association. W trakcie ponadtrzydziestoletniej kariery zawodowej zaprojektował i zaimplementował wiele pakietów związanych z protokołami TCP/IP i OSI dla różnych platform. Jako konsultant doradzał m.in. agencjom rządowym oraz dostawcom sprzętu i oprogramowania.*



Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

Cena 79,00 zł

ISBN 978-83-246-2987-9

9 788324 629879