

DOSTĘP WARUNKOWY DLA POLSKIEJ NAZIEMNEJ TELEWIZJI CYFROWEJ

(Wersja 0.61)

Grupa problemowa do spraw techniki i sprzętu
Międzyresortowego Zespołu ds. Telewizji i Radiofonii Cyfrowej

Warszawa, sierpień 2009

Streszczenie

Niniejszy dokument opisuje zasady działania systemów dostępu warunkowego¹ stosowanych obecnie w telewizji cyfrowej systemu DVB² oraz zawiera przegląd najpopularniejszych rozwiązań spotykanych w Polsce i innych krajach europejskich. Opracowanie powstało w podgrupie ds. CAS Grupy problemowej ds. techniki i sprzętu w celu ułatwienia wyboru systemu dostępu warunkowego dla polskiej DTT zapewniającego niezbędny poziom bezpieczeństwa i szeroką akceptację rynku.

Dostęp warunkowy stosuje się do zabezpieczenia treści rozprawdzanych w sieciach telekomunikacyjnych przed nieautoryzowanym dostępem. Obok DRM jest to obecnie podstawowy sposób ochrony praw autorskich i pokrewnych w erze cyfrowego przesyłania i rejestrowania informacji. Dostęp warunkowy polega w zarysie na spowodowaniu, że transmitowana informacja o obrazie, dźwięku i danych pozostaje nieczytelna dla odbiornika niewyposażonego w odpowiednie środki techniczne.

System dostępu warunkowego stosowany w polskiej DTT powinien:

- być wygodny i przystępny dla użytkownika,
- wykorzystywać w jak największym stopniu wspólne elementy odbiornika-dekodera,
- być odpowiednio bezpieczny a zarazem elastyczny i niezbyt kosztowny,
- pozwalać na konkurencję wśród dostawców treści i usług oraz producentów odbiorników.

Na podstawie powyższych wymagań (szczegółowo diskutowanych w dalszej części tego opracowania) sformułowano zalecenia, którymi należy się kierować przy wyborze technicznego i organizacyjnego modelu świadczenia płatnych usług w polskiej DTT, pozwalającego na utrzymanie konkurencyjności z pozostałymi mediami wykorzystywanymi do dostarczania konsumentom usług telewizji cyfrowej.

Grupa problemowa do spraw techniki i sprzętu zaleca:

1. Wybór jednego systemu skramblowania używanego do wszystkich serwisów płatnych nadawanych w polskiej DTT. Zapobiegnie to sytuacji, gdy każdy skramblowany serwis trzeba będzie dekodować przy użyciu innego urządzenia.
2. Wybór jednego operatora (hurtowego) zarządzającego systemem dostępu warunkowego, tak aby użytkownik mógł za pomocą jednej karty kodowej otrzymać dostęp do różnych pakietów płatnej telewizji pochodzących od różnych dostawców. Zapobiegnie to konieczności fizycznej podmiany kart przy każdej zmianie kanału.
3. Przy wyborze całego systemu dostępu warunkowego należy wziąć pod uwagę bezpieczeństwo systemu, szczególnie jeśli chodzi o ochronę programów HD zarówno po stronie nadawczej jak i odbiorczej. W tym drugim przypadku należy zdefiniować wymagania bezpieczeństwa dla odbiorników uniwersalnych bez wbudowanego CASS. Obecnie jedynie standard CI+ zapewniający wystarczający poziom bezpieczeństwa, który może być akceptowany przez dostawców treści.

¹ Definicje użytych w dokumencie terminów zawiera rozdział 12.

² Listę użytych w dokumencie skrótów i akronimów zawiera rozdział 13.

Spis treści

1. Wprowadzenie	3
2. Model funkcjonalny CAS.....	3
2.1. Zasada działania.....	3
2.2. Tworzenie kluczy i ich transmisja	5
2.3. Odbiornik.....	5
3. Podstawowe konfiguracje CAS	5
3.1. SimulCrypt.....	6
3.2. MultiCrypt	7
3.3. CASS bez karty kodowej.....	7
3.3.1. Rozwiązanie z kanałem zwrotnym.....	7
3.3.2. Rozwiązanie bez kanału zwrotnego.....	8
4. Wybrane szczegóły techniczne CAS	8
4.1. Karta kodowa.....	8
4.2. DVB-CI.....	8
4.3. CI+	9
5. Przegląd modeli transakcyjnych CAS	10
5.1. CAS zintegrowany pionowo	11
5.2. CAS z oddzielnym operatorem.....	12
5.3. Współdzielony CAS z oddzielnym operatorem.....	12
6. Wymagania funkcjonalne CAS	13
6.1. Schematy opłat.....	13
6.2. Gospodarstwa domowe z kilkoma IRD	13
6.3. Współużytkowanie systemu CA	13
6.3.1. Odbiorniki-dekodery	13
6.3.2. System dystrybucyjny	14
6.3.3. Systemy CA	14
6.4. Transkontrola na granicach medium transmisyjnego	15
7. Wymagania operacyjne systemu CA	15
8. Przegląd europejskich rozwiązań CAS.....	16
8.1. Dostawcy systemów CA	16
8.2. Systemy CA spotykane w europejskiej DTT.....	16
8.3. Rynek dostawców płatnych usług w Polsce	16
9. Regulacje prawne dla CAS.....	17
10. Kryteria oceny rozwiązań CAS.....	17
10.1. Wygoda użytkownika	18
10.2. Bezpieczeństwo systemu	18
10.3. Otwarty rynek dostawców odbiorników TV.....	18
10.4. Otwarty rynek dostawców treści.....	19
10.5. Niezależność funkcjonowania dostawców usług.....	19
10.6. Niskie koszty początkowe i operacyjne.....	19

11.	Wnioski i zalecenia	19
11.1.	Wnioski	19
11.2.	Zalecenia	20
12.	Definicje.....	20
13.	Skróty i akronimy.....	22
14.	Bibliografia.....	23

1. Wprowadzenie

Niniejszy dokument opisuje zasady działania systemów dostępu warunkowego stosowanych obecnie w telewizji cyfrowej systemu DVB oraz zawiera przegląd najpopularniejszych rozwiązań spotykanych w Polsce i innych krajach europejskich. Opracowanie powstało w podgrupie ds. CAS Grupy problemowej ds. techniki i sprzętu w celu ułatwienia wyboru systemu dostępu warunkowego dla polskiej DTT zapewniającego niezbędny poziom bezpieczeństwa i szeroką akceptację rynku.

Dostęp warunkowy stosuje się do zabezpieczenia treści rozprowadzanych w sieciach telekomunikacyjnych przed nieautoryzowanym dostępem. Obok DRM jest to obecnie podstawowy sposób ochrony praw autorskich i pokrewnych w erze cyfrowego przesyłania i rejestrowania informacji. Dostęp warunkowy polega w zarysie na spowodowaniu, że transmitowana informacja o obrazie, dźwięku i danych pozostaje nieczytelna dla odbiornika niewyposażonego w odpowiednie środki techniczne.

2. Model funkcjonalny CAS

Niniejszy rozdział przedstawia zasadę działania systemów dostępu warunkowego stosowanych w telewizji cyfrowej DVB oraz ich podstawowe elementy.

2.1. Zasada działania

Podstawowym zadaniem CAS w radiodifuzji jest ograniczenie zasięgu odbioru wyłącznie do odbiorników (IRD), którym operator systemu nadał uprawnienie do dostarczania abonentowi konkretnych programów i usług. Powody, dla których ogranicza się dostęp mogą być następujące:

- wymuszenie opłat za dostęp do określonych programów i usług,
- usługi w rodzaju PPV lub VoD,
- możliwość sterowania zasięgiem geograficznym rozpowszechnianych informacji,
- ochrona małoletnich.

System dostępu warunkowego (CAS) składa się z kombinacji skramblowania i szyfrowania w celu uniemożliwienia nieautoryzowanego odbioru określonych programów i usług. Skramblowanie jest procesem przekształcania informacji o obrazie, dźwięku i danych do postaci niezrozumiałej dla odbiornika (mieszanie danych). Szyfrowanie jest procesem zabezpieczenia tajnego klucza przesyłanego razem ze skramblowanym sygnałem do deskrablera aby mógł poprawnie działać. Sposoby przesyłania słów kontrolnych i zarządzania nimi są różne w różnych systemach dostępu warunkowego.

W ramach Projektu DVB nie udało się uzgodnić jednego, europejskiego systemu dostępu warunkowego. Za standaryzacją CA opowiadali się przede wszystkim nadawcy publiczni, przeciwnikami tej koncepcji byli operatorzy telewizji płatnej (Pay-TV) oraz urzędy antymonopolowe. Ostatecznie ustalono, że pewne rozwiązania techniczne elementów dostępu warunkowego w systemach DVB mogą stanowić własność operatorów, a więc na rynku funkcjonować będzie wiele różnych systemów CA.

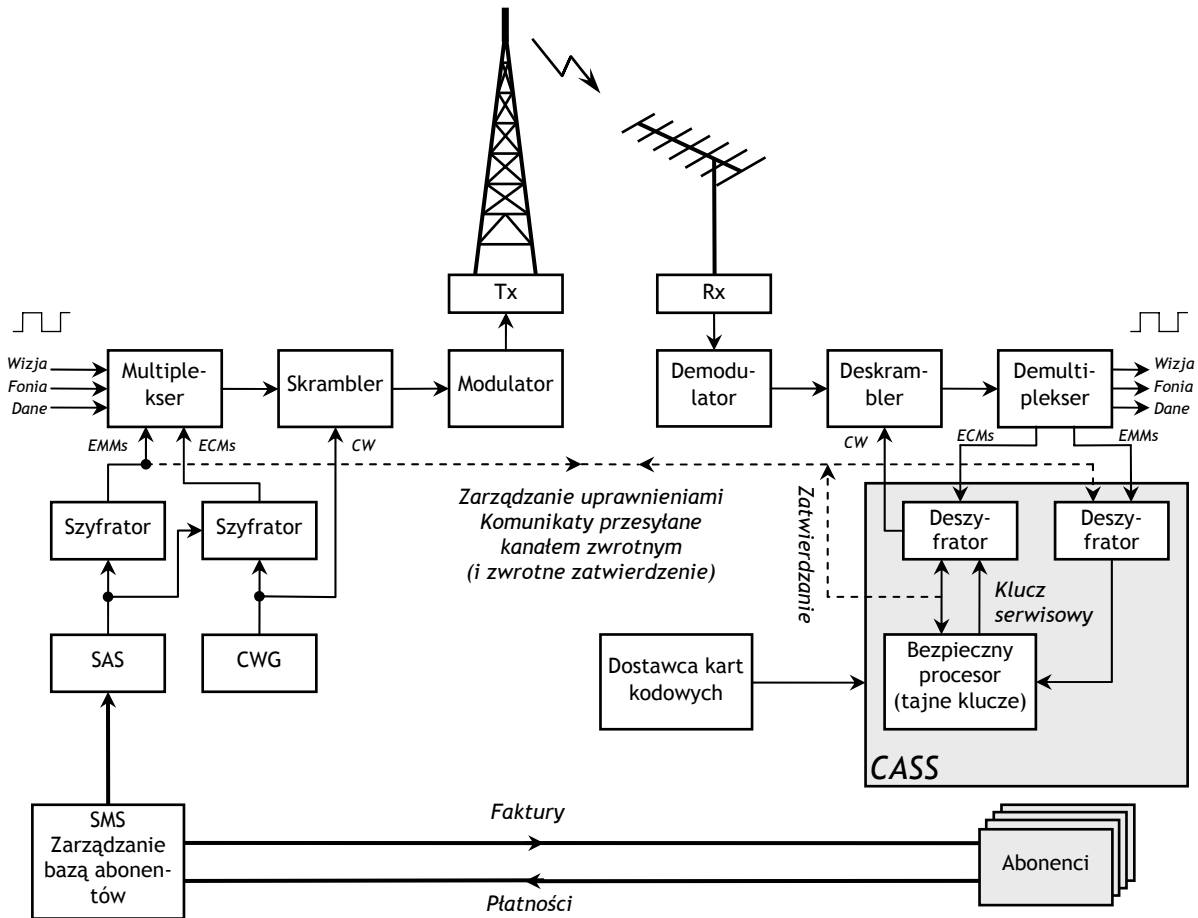
Odstępując od koncepcji uniwersalnego CA, członkowie Projektu DVB uznali za celowe opracowanie wspólnego algorytmu skramblowania (CSA) dla transmisji cyfrowej. Tak powstała specyfikacja składająca się z trzech części: pierwsza dotyczy deskrablera, druga – skramblera, a trzecia – generowania i przesyłania słów kontrolnych do skramblera. Szczegóły koncepcji skramblowania, związane z zabezpieczeniem przesyłanych sygnałów nie są publikowane, są natomiast udostępniane przez Europejski Instytut Standardów Telekomunikacyjnych (ETSI) tym organizacjom i wytwórcom, którzy podpiszą zobowiązanie do nieujawniania tych informacji. System skramblowania podlega regulacjom kontroli eksportu, a w niektórych krajach regulacjom dotyczącym ich stosowania.

Przyjęcie zasady wspólnego algorytmu skramblowania umożliwia stosowanie różnych systemów CA w różnych, ale współpracujących ze sobą mediach transmisyjnych, jak na przykład satelity i sieci kablowe. Na granicy między tymi mediami proces przejścia z jednego systemu CA na drugi (tzw. transkontrola) odbywa się wówczas bez konieczności deskrablowania i ponownego skramblowania, a więc przejście kontroli nad przesyłanym sygnałem dokonywane jest w sposób prostszy i tańszy.

Wymagania, które powinien spełniać skuteczny system skramblowania:

- sygnał po skramblowaniu powinien być niezrozumiały (ukryty),
- skramblowanie powinno być całkowicie odwracalne,
- koszty operacyjne powinny być niskie, deskramblery powinny być tanie,
- skramblowanie powinno być skuteczne dla sygnału każdego rodzaju,
- skramblowanie powinno umożliwiać obsługę różnego typu modeli biznesowych,
- powinien być na tyle skomplikowany, aby jego złamanie było nieopłacalne.

Rysunek 1 przedstawia typowy system dostępu warunkowego (CAS) obejmujący skramblowanie z wykorzystaniem szyfrowanych słów kontrolnych (CW) i komunikatów kontroli uprawnień (EMM) oraz zarządzania bazą abonentów (SMS).



Rys. 1. Schemat CAS z SMS oraz szyfrowaniem CW i EMM

Działaniem skramblera steruje słowo kodowe (CW), które zmienia się co kilka sekund aby uniemożliwić jego ustalenie. CW powinno pochodzić z generatora pseudolosowego CWG (Control Word Generator).

Zadaniem CAS jest szyfrowanie słowa kodowego z wykorzystaniem klucza (lub wielu kluczy w przypadku szyfrowania wielopoziomowego) i informacji o autoryzowanych abonentach oraz transmisja wraz ze skramblowaną treścią w sieci telekomunikacyjnej. Użytkownicy dekodują sygnały korzystając z adresowalnych modułów CASS, najczęściej w postaci karty kodowej (ang. *smart-card*), używanej w większości systemów europejskich. Karty kodowe mogą być uniwersalne lub współpracujące tylko z wybranym modelem odbiornika. Karta kodowa zawiera część lub całość CAS w postaci zaprogramowanego układu mikroprocesorowego, z „zaszytym” wewnątrz algorytmem deszyfrowania wiadomości odzyskującym klucze. W procesie deszyfrowania uczestniczy klucz użytkownika, zapisany na karcie, nietransmitowany w sieci telekomunikacyjnej. Ostatecznie, po odzyskaniu wszystkich kluczy uzyskuje się słowo CW sterujące deskramblerem. Algorytm deszyfrowania jest ściśle związany

z algorytmem szyfrowania słów kodowych CW. Proces szyfrowania wykorzystuje techniki kryptograficzne wysokiego poziomu. Istnieje kilkanaście popularnych systemów szyfrowania i transmisji kluczy. Operatorzy Pay-TV mają możliwość wyboru systemu a także jego zmiany i aktualizacji. Jest to konieczne w walce o utrzymanie piractwa na możliwie niskim poziomie.

2.2. Tworzenie kluczy i ich transmisja

Słowa CW mają 60 bitów istotnych i są zmieniane co 2 do 10 s. Informacja o słowach CW jest w zaszyfrowanej postaci transmitowana do odbiornika jako wiadomość ECM. Wiadomości ECM zawierają także atrybuty programów, czyli warunki dostępu.

Jeśli poszczególne programy w strumieniu mają mieć zdefiniowane prawa dostępu, konieczne może być uaktualnianie ECM wraz z każdą ramką strumienia, czyli częściej niż wymagają tego względy bezpieczeństwa. Wiadomości ECM są umieszczone w strumieniu transportowym TS w tablicy określonej standardem MPEG-2.

Proces szyfrowania słów CW jest uzależniony od wartości klucza serwisowego (SK), zmienianej w odstępach czasu od miesiąca do roku. Klucz SK jest szyfrowany jako wiadomość EMM wraz z informacją o subskrypcji każdego abonenta. Informacje o abonentach są na bieżąco aktualizowane dzięki systemowi SAS.

SAS jest odpowiedzialny za szyfrowanie i dostarczanie kluczy. SAS jest nadzorowany przez system SMS o charakterze biznesowym, określającym prawa poszczególnych abonentów do usług, programów, kanałów, itp. Ze względu na swój charakter, wiadomości EMM mogą być transmitowane nie tylko wraz z głównym strumieniem TS, ale także innymi drogami, np. linią telefoniczną, kanałem zwrotnym sieci kablowej, poprzez kartę kodową. Wiadomości EMM są szyfrowane z użyciem kluczy Master Key, odpowiadających kluczom przydzielonym każdemu z użytkowników. Zakresy przydziału tych kluczy muszą być uzgodnione pomiędzy operatorami.

O ile sposób transmisji wiadomości ECM i EMM podlega standaryzacji, to format ECM i EMM jest zależny od formatu biznesowego, systemu rozliczeń, itp.

2.3. Odbiornik

Odbiornik, czyli IRD może być samodzielnym urządzeniem (STB) dołączanym do telewizora lub stanowić część zintegrowanego odbiornika TV (iDTV). Większość modułów IRD stanowią standardowe podzespoły elektroniczne. Moduł dostępu warunkowego, jego budowa, działanie i lokalizacja, zależy od systemu CA współpracującego z danym odbiornikiem. Moduł CA powinien być dołączony do wyjścia modułu podającego odebrany strumień transportowy TS. Po deskramblowaniu w module CA strumień może trafić do dekodera MPEG.

Moduł CA składa się z:

- bloku deskramblowania,
- bloku „wyławiania” ze strumienia TS, kontroli i przetwarzania wiadomości EMM i ECM,
- bloku współpracy z nośnikiem klucza prywatnego (karta kodowa),
- bloku sterowania.

Elementy modułu CA mogą w całości znajdować się wewnątrz IRD (poza kartą kodową) lub ich część może znajdować się na karcie CASS dołączanej do odbiornika przez ustalony interfejs. Moduł CASS może być w całości zrealizowany jako karta kodowa.

3. Podstawowe konfiguracje CAS

W zależności od tego, czy bierze się pod uwagę stronę nadawczą czy odbiorczą można wyróżnić następujące konfiguracje CAS.

Po stronie nadawczej:

- pojedynczy,

- MultiCrypt,
- Simulcrypt.

Po stronie odbiorczej:

- z wbudowanym CASS:
 - z kartą kodową,
 - bez karty kodowej;
- z zewnętrznym modulem CASS:
 - z kartą kodową,
 - bez karty kodowej (niespotykany).

Wersja z pojedynczym CAS została opisana w rozdziale 2.1, SimulCrypt w rozdziale 3.1 a MultiCrypt w rozdziale 3.2. Konfiguracja odbiornika nie ma zasadniczego wpływu na możliwość pracy w którejkolwiek konfiguracji występującej po stronie nadawczej. Jednak CASS w postaci wymiennalnego modułu predestynuje odbiornik do współpracy z konfiguracją MultiCrypt. Dlatego została przedstawiona łącznie.

Konfiguracją odbiornika zasługującą na osobny opis jest konfiguracja bez karty kodowej przedstawiona w rozdziale 3.3.

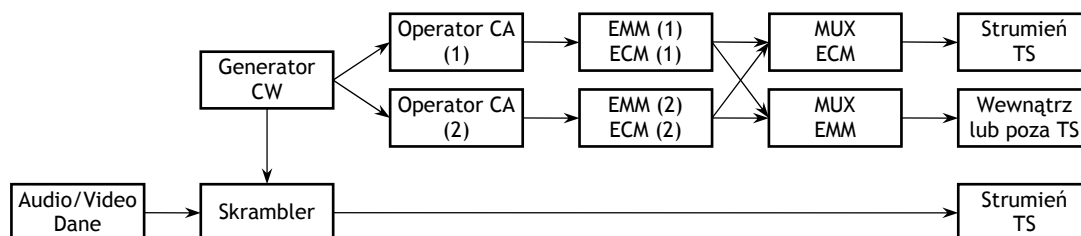
3.1. SimulCrypt

Stosowanie wspólnego algorytmu skramblowania (CSA) do transmisji sygnałów cyfrowych w strumieniu transportowym TS MPEG-2 pozwala na wprowadzenie do przesyłanego strumienia danych szeregu informacji, które umożliwiają kontrolę tego samego zakodowanego programu, choć generowane są przez kilka różnych systemów warunkowego dostępu. Ma to zapewnić kompatybilność z różnymi systemami CA. Skramblery pracują z użyciem tych samych słów CW, ale stosują własne systemy szyfrowania ECM i EMM. Technika ta, nosząca nazwę SimulCrypt, pozwala na:

- dostarczanie tego samego programu odbiorcom posiadającym dekodery z różnymi systemami dostępu warunkowego, oraz
- płynne przejście z jednego systemu dostępu warunkowego na drugi w dowolnej grupie odbiorców posiadających dekodery, na przykład dla ochrony przed piractwem.

Proces skramblowania sterowany jest przez słowo kontrolne (CW), które pochodzi ze wspólnego źródła ale może też być generowane w jednym z systemów warunkowego dostępu. To słowo kontrolne jest dostarczane do grupy dekoderek typu 1, pracujących w systemie CA1 lub do grupy dekoderek typu 2, pracujących w systemie CA2. Dane obu systemów przesyłane są w multipleksie wraz z programem.

Rysunek 2 przedstawia przykładowy schemat stacji czołowej działającej w trybie SimulCrypt z dwoma operatorami CAS.



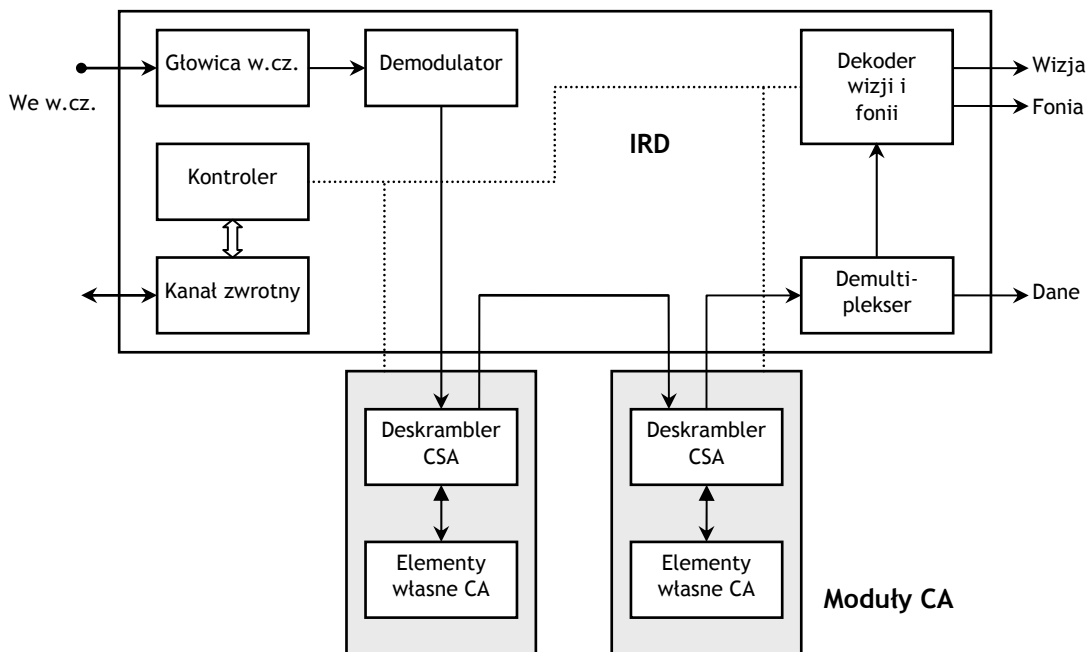
Rys. 2. Schemat działania SimulCryptu

Działanie systemu bazuje na współpracy dostawców programów i usług z operatorami CAS. Korzyścią dla abonenta jest możliwość używania tylko jednego IRD i jednej karty kodowej dla odbioru wielu serwisów.

3.2. MultiCrypt

MultiCrypt to system otwarty, eliminujący blok dostępu warunkowego z IRD. Cały podsystem (CASS) włącznie z układem deskramblowania umieszczony jest w oddzielnym module dołączanym do odbiornika poprzez złącze CI. Odbiornik może mieć kilka złączy CI dla kilku różnych systemów CA.

Rysunek 3 przedstawia schemat odbiornika (IRD) współpracującego z dwoma modułami CA.



Rys. 3. Schemat działania CI

Złącze CI wywodzi się i odpowiada komputerowemu interfejsowi PCMCIA. Rozwiązanie takie upraszcza budowę odbiornika i praktycznie w całości go standaryzuje, pozwalając na pełną konkurencję pomiędzy producentami sprzętu i szeroki wybór modeli dla użytkowników. Aktualizacja systemu CA dotyczy wówczas tylko wymiany modułu CAM, zrealizowanego jako układ współpracujący z kartą kodową. Oprogramowanie odbiornika nie wymaga żadnej aktualizacji, pod warunkiem poprawnej współpracy z nowym modulem CA. Mimo tych zalet MultiCrypt jest słabo rozpowszechniony. Zdecydowała o tym niechęć operatorów CAS z powodu relatywnie większych kosztów MultiCryptu w porównaniu z SimulCryptem oraz zagrożeniem dostępu do jawnego strumienia TS za złącza PCMCIA.

Komisja Europejska wymaga stosowania CI we wszystkich zintegrowanych odbiornikach telewizji cyfrowej (iDTV) o przekątnej ekranu powyżej 30 cm. Zwykle dekodery IRD mogą mieć wbudowane systemy CA na stałe oraz złącza CI dla ewentualnej rozbudowy. Złącze CI może służyć także do innych celów niż CAS.

3.3. CASS bez karty kodowej

Ostatnio pojawiły się na rynku rozwiązania oparte wyłącznie na wykorzystaniu oprogramowania nie wymagające stosowania karty kodowej w odbiorniku.

3.3.1. Rozwiązanie z kanałem zwrotnym

W tym scenariuszu, bezpieczeństwo dostarczanych treści jest oparte na odpowiedniej i certyfikowanej architekturze urządzeń odbiorczych oraz module oprogramowania licencjonowanego i dostarczanego producentom urządzeń odbiorczych przez dostawcę systemu CA. Moduł ten jest nierozdzielnie zintegrowany z oprogramowaniem odbiornika i w celu pobrania i aktualizacji informacji niezbędnych do deszyfrowania chronionych treści w sposób ciągły komunikuje się z systemem nadawczym.

Rozwiązanie to wykorzystuje powszechnie stosowane algorytmy skramblowania takie jak CSA i szyfrowania jak AES. Jego wadą jest konieczność utrzymywania połączenia zwrotnego i utrata ano-

nimowości użytkownika, co go praktycznie dyskwalifikuje w służbie radiodifuzyjnej opierającej się właśnie na anonimowości odbiorcy.

3.3.2. Rozwiązanie bez kanału zwrotnego

To rozwiązanie jest wynikiem ewolucji rozwiązania wykorzystującego kanał zwrotny. W tym przypadku bezpieczeństwo dostarczanych treści jest również oparte na odpowiedniej i certyfikowanej architekturze urządzeń odbiorczych oraz module oprogramowania licencjonowanego i dostarczanego producentom urządzeń odbiorczych przez dostawcę systemu dostępu warunkowego. Moduł ten jest nierozdzielnie zintegrowany z oprogramowaniem odbiornika. Identyfikacja i autoryzacja po deszyfrowaniu kodowanych treści następuje przez dodatkowe informacje dosyłane drogą rozsiewczą (jednokierunkowo) przez kanały sieci kablowych, satelitarnych lub naziemnych.

Rozwiązanie to wykorzystuje powszechnie stosowane algorytmy skramblowania takie jak CSA i szyfrowania jak AES.

4. Wybrane szczegóły techniczne CAS

W tym rozdziale zostały opisane elementy systemu dostępne dla użytkownika i podlegające ewentualnej wymianie, tzn. karty kodowe i karty PCMCIA.

4.1. Karta kodowa

Karta kodowa (ang. *smart-card*, *chip card*, *integrated circuit card*) służy obecnie jako podstawowy nośnik zaszyfrowanej informacji o prywatnym kluczu kodowym abonenta. Pierwszym masowym zastosowaniem była karta telefoniczna we Francji w 1983 r. Obecnie coraz skuteczniej wypiera karty kredytowe z paskiem magnetycznym, ponieważ zapewnia większe bezpieczeństwo danych. Kolejnym obszarem zastosowania są elektroniczne karty identyfikacyjne, które również mogą wykorzystywane w usługach typu e-Urząd lub e-Państwo.

Karta kodowa wyglądem i rozmiarami odpowiada znormalizowanej karcie kredytowej o wymiarach $85,6 \times 54,0 \times 0,76$ mm z zatopionym wewnątrz układem scalonym zawierającym mikroprocesor, pamięć i układ wejścia/wyjścia. Karty mogą być stykowe tzn. podczas wymiany informacji z czytnikiem potrzebny jest galwaniczny kontakt z końcówkami modułu lub zbliżeniowe, które komunikują się z czytnikiem drogą radiową.

Rysunek 4 pokazuje wygląd przykładowej bankowej karty kodowej.



Rys. 4. Bankowa karta kodowa

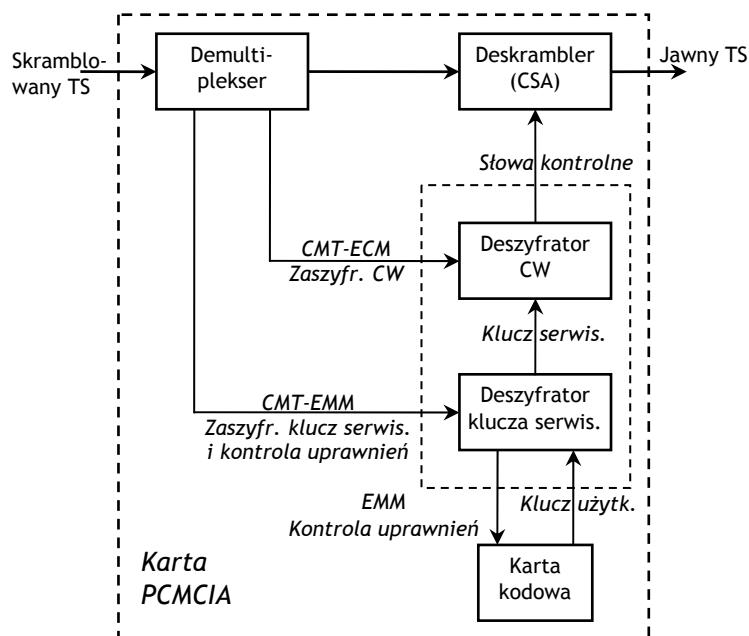
Większość stosowanych czytników w odbiornikach-dekoderach płatnej telewizji wykorzystuje karty stykowe.

4.2. DVB-CI

Grupa DVB opracowała specyfikację wspólnego interfejsu CI. Umożliwia on wykorzystywanie wspólnego deskramblera razem z elementami własnymi różnych systemów warunkowego dostępu.

Cały ten układ wykonany jest w postaci oddzielnego modułu, dołączanego do gniazda interfejsu w odbiorniku DVB. Interfejs znajduje się pomiędzy tym modulem a zespołem, który zawiera demultiplikser i dekodek MPEG oraz tuner i demodulator. Koncepcja wspólnego interfejsu stwarza więc możliwość połączenia w jednym systemie standardowych elementów MPEG/DVB z tymi elementami warunkowego dostępu, o których rozwiązaniu i zastosowaniu decydują poszczególni operatorzy Pay-TV.

Rysunek 5 przedstawia uproszczony schemat budowy modułu dostępu warunkowego (CAM).



Rys. 5. Schemat budowy CAM

Fizyczne wykonanie modułu interfejsu z 68-kontaktowym złączeniem odpowiada standardowi PC Card, opracowanego dla komputerów osobistych. Pierwsza demonstracja CI odbyła się w grudniu 1996 r., a proces standaryzacji przeprowadzono w 1997 r. pod auspicjami CENELEC.

Najwięksi producenci odbiorników iDTV używają tego interfejsu dla zapewnienia sobie kompatybilności z różnymi systemami skramblowania dostępnymi w Europie jak i na całym świecie. Dla tych producentów implementacja wbudowanego CAS jest nieopłacalna, ponieważ zwykle jeden model odbiornika jest przewidziany do sprzedaży w kilku państwach, gdzie używane są różne systemy skramblowania.

Rysunek 6 przedstawia fotografie kilku modułów CAM.



Rys. 6. Wygląd kilku CAM dostępnych na rynku

Wadą tego rozwiązania jest wysoka cena modułu. Może być porównywalna z ceną najprostszego STB a w przypadku uniwersalnego modułu PowerCam nawet znacznie wyższa.

4.3. CI+

Moduł CI w wersji 1 miał pełnić rolę łatwego i kompatybilnego interfejsu, który pozwalał uniezależnić odbiornik od systemu kodowania. Niestety, w czasach kiedy był tworzony jak również w dalszym okresie nie koncentrowano się na ogólnym bezpieczeństwie całego systemu (kart kodowych,

modułu CAM i odbiornika). Doprowadziło to do sytuacji, w której wytwórcy drogiego materiału HD uznali to rozwiązanie kontroli dostępu za niebezpieczne i zwykle zastrzegają sobie prawo do ograniczenia lub wyłączenia możliwości odbioru tego typu treści przez moduły CI w wersji 1.

Słabość systemu opartego na CI w wersji 1 jest widoczna na jego wyjściu. Z modułu CA w tej wersji dostaje się czysty strumień elementarny dla wybranego serwisu (rozszyfrowanej wizji i fonii w postaci cyfrowej). Dane w tej postaci można bezpośrednio zapisywać na nośniki i publikować w sieci w przeciągu bardzo krótkiego czasu (czasami bez konieczności dodatkowej obróbki). Dla serwisów HD są to dane obrazu o wysokiej rozdzielczości w postaci cyfrowej. Łatwość dostępu i możliwość nielegalnego publikowania tych danych jest problemem interfejsu CI w wersji 1.

Konsorcjum DVB, które tworzyło standard CI w wersji 1 rozpoczęło nawet prace na CI w wersji 2, który miał być bezpieczniejszym następcą swojego poprzednika. Niestety, postęp prac nad tym standardem był niewspółmierny do wymagań rynkowych i nawet do dzisiaj nie został opublikowany.

Następstwem braku postępu w pracach DVB nad bezpieczniejszym interfejsem CI było opracowanie przemysłowego standardu CI+. Standard CI+ powstał głównie w wyniku zapotrzebowania rynku na bezpieczniejszy system dekodowania programów Pay-TV dla odbiorników niewspierających wbudowanego CASS.

Standard CI+ jest rozszerzeniem standardu CI w wersji 1. Prace nad nim prowadziło konsorcjum producentów iDTV: Panasonic, Philips, Samsung i Sony oraz producentów modułów CA: SmarDTV i Neotion.

Główną zaletą tego rozwiązania jest zabezpieczenie strumienia cyfrowego na wyjściu modułu CA. W tej wersji strumień danych cyfrowych wizji i fonii jest szyfrowany mocnym algorytmem. Następnie strumień ten dostarczany jest do odbiornika, gdzie jest ponownie deszyfrowany. Dane zdekodowane w formie czystego strumienia elementarnego nie są dostępne poza chipsetem odbiornika tak, jak to ma miejsce w systemie z wbudowanym CASS. W rezultacie bezpieczeństwo systemu (karta kodowa, CAM i odbiornik) opartego na standardzie CI+ jest porównywalne z systemami z wbudowanym CASS, natomiast odbiornik nadal zachowuje niezależność od konkretnego systemu skramblowania.

Do zabezpieczania strumienia wyjściowego na styku pomiędzy CAM a odbiornikiem używa się:

- DES z kluczem o długości 64 bitów dla programów w jakości SD,
- AES z kluczem o długości 128 bitów dla programów w jakości HD.

Ponieważ algorytmy te są dobrze zdefiniowane, różne moduły CAM oraz różne odbiorniki wspierające CI+ są w pełni kompatybilne ze sobą. Moduły CAM i odbiornik mają funkcję uwierzytelniania za pomocą certyfikatów, więc tylko uwierzytelnione pary tych urządzeń mogą tworzyć system dekodowania płatnych programów. Po uwierzytelnieniu CAM i odbiornik wymieniają się kluczami, które są używane do szyfrowania i deszyfrowania strumienia danych audiowizualnych. Dodano również zaawansowane mechanizmy zarządzania certyfikatami oraz uprawnieniami, które mogą być kontrolowane przez operatora Pay-TV. Ze względu na oferowane bezpieczeństwo, systemy oparte na CI+ powinny być akceptowane przez twórców treści wysokiej rozdzielczości, ponieważ nie będzie można już w łatwy sposób nagrywać i udostępniać danych cyfrowych w formacie HD. Standard CI+ jest również wstecznie kompatybilny z standardem CI w wersji 1.

Przy okazji tworzenia nowego standardu dodano rozszerzoną obsługę warstwy graficznej związanej z interfejsem CI+. Aby zwiększyć możliwości graficzne, CI+ definiuje MHEG-5 jako obowiązkowy standard dla interaktywnych aplikacji, które mogą znajdować się w module CAM.

5. Przegląd modeli transakcyjnych CAS

Typowy model dostępu do płatnych usług jest taki, że po zakupieniu uniwersalnego odbiornika telewizji cyfrowej użytkownik może kupić kartę kodową oraz – gdy jest o konieczne – również moduł CAM. Moduł CAM jest czasami dostarczany bezpośrednio przez nadawcę płatnych usług, ponieważ w nowszych wersjach systemów skramblowania wymaga on tzw. parowania karty kodowej z jej czytnikiem i dekoderym sygnału zakodowanego. Niektóre systemy wymagają korzystania z wyspecja-

lizowanego odbiornika-dekodera, który należy dołączyć do telewizora wykorzystując odpowiedni interfejs.

W niektórych krajach można spotkać model nadawania, w którym kilku niezależnych dostawców dostarcza swoje płatne usługi poprzez ten sam kanał transmisyjny. Wtedy to użytkownik podpisuje umowę z każdym z nich i dostaje od każdego kartę kodową z uprawnieniami do oglądania konkretnego pakietu danego dostawcy. System kodowania dla wszystkich z dostawców pozostaje ten sam.

W innych krajach mamy też do czynienia z modelem, gdzie poza oddzielnymi umowami użytkownik jest również zmuszony do posiadania odbiornika obsługującego różne systemy skramblowania, co czasami wiąże się z koniecznością ich podmiany (moduły CAM dla telewizorów cyfrowych).

Robiąc przegląd modeli nadawania możemy wyznaczyć kilka podstawowych sytuacji:

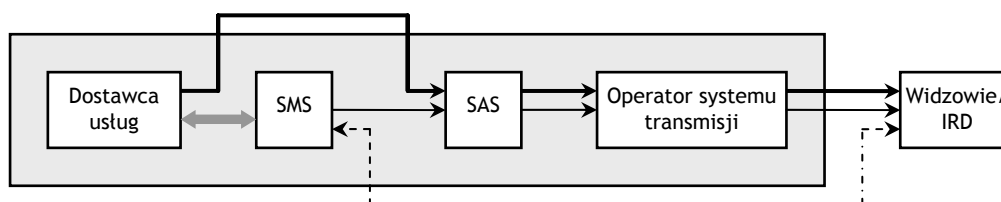
- a) jeden operator DTT i zarazem hurtowy dostawca usług płatnych, jeden system skramblowania (model wertykalny),
- b) jeden operator DTT, kilku dostawców usług płatnych, narzucony z góry konkretny jeden system skramblowania dla wszystkich,
- c) kilku operatorów DTT, kilku dostawców usług płatnych, narzucony z góry jeden konkretny system skramblowania dla wszystkich,
- d) kilku operatorów DTT, tyle samo dostawców usług płatnych, dowolność operatorów co do używanego systemu CAS.

W większości krajów europejskich można spotkać model opisany podpunktem (a) lub (b).

Za pomocą odpowiednich modeli można zilustrować podstawowe transakcje handlowe odbywające się w ramach radiodifuzyjnego systemu dostępu warunkowego niezależnie od zastosowanych rozwiązań technicznych. Podobne analogie są czasami stosowane do opisu sprzedaży dóbr poprzez sieci detaliczne i hurtowe: w tej sytuacji mamy do czynienia ze strumieniem dóbr i usług płynących w jednym kierunku – od wytwórcy do końcowych klientów – oraz ze strumieniem pieniędzy w przeciwnym kierunku.

5.1. CAS zintegrowany pionowo

Model systemu CA zintegrowanego pionowo (wertykalnego) został pokazany na rys. 7.



Rys. 7. CAS zintegrowany pionowo

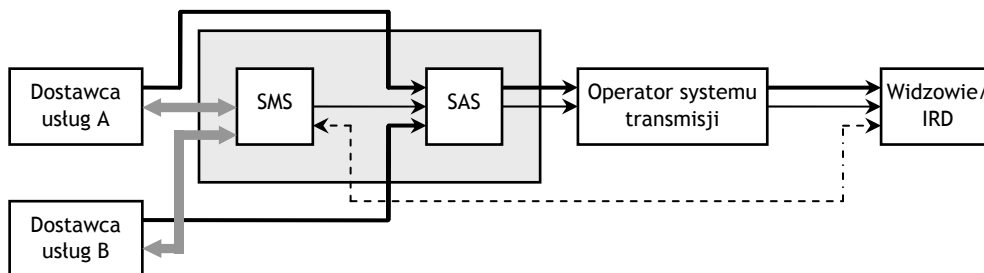
Połączenia między blokami na rysunkach od 7 do 9 oznaczają:

- > Programy,
- > Uprawnienia do oglądania,
- > Pieniądze, adresy i rachunki,
- ←———— Pieniądze i adresy.

W tym modelu dostawca usług jest równocześnie operatorem sieci i systemu CA. Historycznie systemy CA powstały właśnie w tej postaci a model ten działa obecnie w wielu systemach kablowych: operator TVK działa jako dostawca usług (zwykle zakupując prawa do pokazywania programów wytworzonych przez inne podmioty) jak również jako dostawca sygnału i operator CAS. W takiej sytuacji, w szczególności gdzie – jak w większości systemów kablowych – operator TVK dostarcza i pozostaje właścicielem dekoderek, pojedynczy zamknięty system jest do zaakceptowania, ponieważ nie ma potrzeby udostępniać konkurentom jakiegokolwiek części systemu.

5.2. CAS z oddzielnym operatorem

Model systemu CA z oddzielnym operatorem został pokazany na rys. 8.

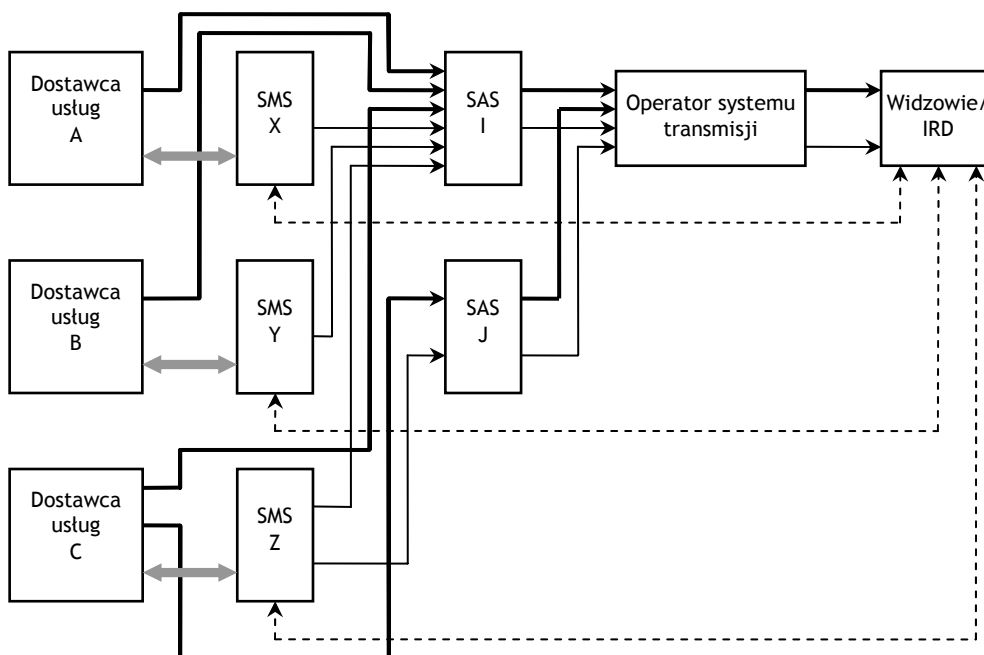


Rys. 8. CAS z oddzielnym operatorem

W tym modelu funkcje dostawcy usług i operatora CAS zostały rozdzielone. W przykładzie pokazanym na rys. 8 są dwaj niezależni dostawcy usług A i B współużytkujący wspólny system transmisyjny, który jest własnością i jest zarządzany przez osobny podmiot, oraz wspólny system CA będący własnością i zarządzany przez jeszcze inny podmiot. Tak więc, wszystkie operacje dotyczące bilingów i zbierania pieniędzy są wykonywane przez operatora systemu CA, który przekazuje płatności właściwym dostawcom usług odpowiednio do ich praw wobec dostarczanych programów. Ten model funkcjonuje w wielu systemach satelitarnych i stosuje się również do rynku detalicznego, na którym działa tylko jeden sprzedawca. Należy zauważyć, że operator CAS dysponuje danymi o nazwiskach, adresach i statusie uprawnień wszystkich widzów. Natomiast dostawcy usług mają dostęp jedynie do danych odbiorców swoich usług.

5.3. Współdzielony CAS z oddzielnym operatorem

Współdzielony model z oddzielnym operatorem CAS został pokazany na rys. 9.



Rys. 9. Współdzielony CAS z osobnym operatorem

W pokazanym przykładzie działają dwaj niezależni operatorzy systemów autoryzacji abonentów (SAS) I i J. System J jest wykorzystywany tylko przez dostawcę usług C, natomiast system I jest używany przez wszystkich trzech dostawców usług. Przeciwnie, dostawcy usług A i B wykorzystują tylko system I, natomiast dostawca usług C stosuje systemy I i J. Tak więc, odbiorcy usług dostarczanych przez C mogą stosować dekodery dostosowane do systemu I lub J. Kolejną cechą tego modelu jest to, że bilingi i pieniądze płyną bezpośrednio pomiędzy widzami a operatorami SMS, a nie płyną przez

operatorów SAS ani przez operatorów systemu transmisji. W rezultacie, dane wrażliwe o nazwiskach i adresach abonentów są znane wyłącznie odpowiednim dostawcom usług.

6. Wymagania funkcjonalne CAS

6.1. Schematy opłat

Ważne jest aby CAS mógł obsługiwać szeroki zakres schematów obciążania konta i wnoszenia opłat. Najważniejsze z nich to:

- *Abonament* (przedpłata za okres oglądania),
- *Pay-per-View* (przedpłata za wybraną audycję lub grupę audycji),
- *Pay-per-View impulsowy* (opłata za wybrany program lub grupę programów bez wcześniejszego zgłoszenia).

Dwie ostatnie możliwości zwykle wymagają zestawienia kanału zwrotnego pomiędzy widzem i operatorem CAS. Kanał zwrotny jest wykorzystywany do rejestracji historii oglądania, co jest ważne kiedy uwzględnia się kwestie praw do audycji.

6.2. Gospodarstwa domowe z kilkoma IRD

W sytuacji kiedy w jednym gospodarstwie domowym występuje więcej niż jeden IRD należy ustalić czy wnoszone opłaty zezwalają na:

1. korzystanie wyłącznie z jednego IRD do odbioru i dekodowania usług;
2. korzystanie z pełnego wyposażenia gospodarstwa domowego, które może dysponować kilkoma IRD i PVR;
3. korzystanie przez jedną osobę gdziekolwiek w obrębie gospodarstwa domowego, co oznacza że uprawnienie powinno się dawać przenieść z jednego IRD do innego prawdopodobnie przez użycie wyjmowanego przyrządu bezpieczeństwa jak np. karta kodowa.

W trzecim przypadku pokazanym powyżej, występuje konflikt z koniecznością legalizacji przyrządu bezpieczeństwa do używania wyłącznie z konkretnym dekoderm. Dlatego każdy dekoderm powinien mieć swój własny CASS a lista wszystkich CASS w gospodarstwie domowym powinna tworzyć grupę w SMS aby umożliwić odpowiednie i uzasadnione rozliczanie.

6.3. Współużytkowanie systemu CA

Aby stworzyć warunki do rozwoju otwartego i dającego równe szanse rynku dla dostępu warunkowego w radiodifuzji, ważne jest aby pewne elementy systemu CA dały się współużytkować. Dotyczy to następujących elementów:

6.3.1. Odbiorniki-dekodery

Jeden podstawowy odbiornik-dekoderm (IRD) powinien być w stanie odebrać i zdekodować programy pochodzące od różnych nadawców, prawdopodobnie wykorzystujących różne media transportowe (tj. kablowe, satelitarne, naziemne). Z tego może wynikać, że odbiornik może wspierać jednocześnie użycie kilku przyrządów bezpieczeństwa albo jeden przyrząd bezpieczeństwa może być współdzielony przez kilku dostawców usług. W tym ostatnim przypadku, przyrząd bezpieczeństwa powinien być rozdzielony na niezależne strefy w taki sposób, aby operatorzy mieli dostęp do zapisu i odczytu wyłącznie w strefach, które zawierają informacje o uprawnieniach do oglądania ich własnych programów. Kiedy operatorzy współdzielą przyrząd bezpieczeństwa ważne jest rozstrzygnięcie kto wydaje i będzie wymieniał przyrząd bezpieczeństwa – szczególnie w przypadku złamania bezpieczeństwa wymagającego wymiany przyrządu bezpieczeństwa.

Wyjątkowo istotnym a zarazem trudnym do spełnienia wymaganiem, które wynika z konieczności współużytkowania dekoderm, jest pozwolenie IRD aby się dostrajał do emisji nie niosących tych samych EMM. Chociaż opłaca się monitorowanie jak największej liczby strumieni EMM nawet kiedy odbiornik jest w stanie oczekiwania, to ze względu na wymóg oszczędnego zużycia energii potrzebne

jest rozwiązaniem, które uruchamia przeszukiwanie strumieni transportowych przez IRD w wybranych momentach czasu..

W niektórych wypadkach (np. transmisja komunikatów) nadawca musi dotrzeć do wielkiej liczby dekodowników w krótkim czasie. W takich sytuacjach korzystne jest wykorzystanie współdzielonych kluczy w celu skrócenia czasu dostępu do szerokiej widowni. Widownia zostaje podzielona na grupy widzów, każda osoba w określonej grupie ma ten sam współdzielony klucz składający się na całe słowo kontrolne. Można również połączyć w jeden komunikat różne komunikaty przeznaczone dla tego samego widza.

6.3.2. System dystrybucyjny

Oczywiste jest, że dowolne medium transportowe (tj. sieć kablowa, transponder satelitarny lub radiodifuzyjny kanał naziemny) powinno pozwalać na współużytkowanie przez różnych i prawdopodobnie rywalizujących ze sobą nadawców. Mniej oczywiste jest ale prawdopodobnie równie ważne, aby dowolny strumień transportowy dawał się dekodować przez dekodery różnych typów, co oznacza, że pojedynczy program może być dostępny jednocześnie w różnych CAS. Jest to koncepcja Simulcryptu opisana w rozdziale 3.1.

6.3.3. Systemy CA

Kiedy analizuje się współużytkowanie systemów CA po stronie nadawczej, ważne jest aby można było podzielić na dwa funkcjonalnie oddzielne składniki:

a) System obsługi abonentów (SMS)

SMS zasadniczo odpowiada za rozsyłanie rachunków i odbierania opłat od widzów. Nie jest wymagane ani zalecane aby SMS był związany z konkretnym systemem CA. SMS przechowuje komercyjnie wrażliwe informacje jak np. bazę danych o nazwiskach, adresach i upoważnieniach abonentów. Współużytkowanie SMS przez konkurujących nadawców jest możliwe, jeżeli będzie on zarządzany przez osobny zaufany podmiot i jeżeli tylko zostaną ustalone odpowiednie zapory aby każdy dostawca usług miał dostęp wyłącznie do informacji o własnych abonentach. Chociaż współużytkowanie SMS może się wydawać niepożądane, to jeżeli przyjmiemy, że koszt uruchomienia własnego SMS może być zaporowy dla dostawców usług z startujących z niewielką liczbą abonentów, dla nich może być jedyną szansą rozpoczęcia działalności.

Obsługa SMS powinna być zlecona zaufanej firmie zewnętrznej, tj. bezpiecznej i odpowiedzialnej organizacji jak np. bank. Tam powinna się znaleźć baza danych abonentów a system powinien radzić sobie z modyfikacjami dotyczącymi abonamentu, problemami instalacyjnymi, marketingiem, bilingiem i dystrybucją kart. SMS również zarządza ekipą instalatorów oraz wysyła EMM do kolejki Systemu Autoryzacji Abonentów (SAS).

W celu zapewnienia poufności informacji zawartych w bazie danych o abonentach, SMS powinien dostarczać widzom wymieniane karty kodowe i moduły CA zwykłą pocztą. Karty powinny być autoryzowane przed wysyłką przez operatora CAS lub powinny być autoryzowane po dystrybucji przez SAS poprzez kanał radiowy wykorzystując adresy wirtualne dostarczone przez SMS.

b) System Autoryzacji Abonentów (SAS)

Podstawowym zadaniem SAS jest rozsyłanie kanałem radiowym komunikatów upoważniających (EMM) i legalizujących przyrzady bezpieczeństwa. SAS potrzebuje unikalnego numeru seryjnego (adresu) dla każdego przyrzadu bezpieczeństwa IRD ale nie potrzebuje dostępu do komercyjnie wrażliwych informacji jak np. nazwiska i adresy abonentów. Dlatego współużytkowanie SAS jest możliwe dla konkurujących ze sobą nadawców, chociaż należy rozwiązać problem czasu oczekiwania komunikatów w kolejce. Karty kodowe można autoryzować pośrednio poprzez kanał radiowy przez SAS.

SAS generuje słowo kontrolne skramblera, szyfruje dane dostępu warunkowego, kolejkuje i nadaje priorytety EMM z SMS oraz skrambluje obraz i dźwięk. Nowe komunikaty z SMS

trafiają do kolejki pośredniej, skąd są wysyłane tak szybko jak to możliwe, jak również trafiają do regularnej kolejki cyklicznej, gdzie pozostają aż do momentu utraty ważności. Częstotliwość wysyłki zależy od długości kolejki a komunikaty tracą ważność zgodnie z przyznaną kategorią. Należy ustalić maksymalny limit czasu odpowiedzi, po przekroczeniu którego system staje się bezużyteczny. Komunikaty dezaktywujące mogą mieć nieskończony czas życia, podczas gdy komunikaty aktywujące mogą mieć czas życia ok. miesiąca. Ze względów bezpieczeństwa komunikacja pomiędzy SMS i SAS powinna być szyfrowana chyba, że odbywa się w całości w bezpiecznym środowisku.

6.4. Transkontrola na granicach medium transmisyjnego

Często zdarza się, że sygnał radiowo-telewizyjny dociera do widza po przejściu dwóch lub więcej mediów transmisyjnych. Dotyczy to głównie telewizji kablowej, w której retransmituje się programy oryginalnie nadawane drogą satelitarną lub naziemną. W takich przypadkach należy zmienić kontrolę upoważnień na granicy mediów bez konieczności deskramblowania i ponownego skramblowania sygnału.

7. Wymagania operacyjne systemu CA

Ze względów bezpieczeństwa ważne jest aby CAS spełniał jak najwięcej spośród funkcji wymienionych poniżej:

a) *Aktywacja/dezaktywacja karty*

Pojedyncze karty kodowe lub grupy kart kodowych (lub innych przyrządów bezpieczeństwa) powinny umożliwiać aktywację lub dezaktywację poprzez kanał radiowy.

b) *Aktywacja/dezaktywacja całego programu*

Pojedyncze karty kodowe lub grupy kart kodowych (lub innych przyrządów bezpieczeństwa) powinny umożliwiać aktywację lub dezaktywację poprzez kanał radiowy w zakresie dekodowania konkretnego programu.

c) *Wysyłanie komunikatu do dekodera*

Komunikat tekstowy jest wysyłany do pojedynczych dekoderek lub grup dekoderek w celu wyświetlenia na ekranie; alternatywnie, komunikat wysłany drogą radiową może zawierać rozkaz i adres komunikatu zapisanego wcześniej w pamięci dekodera lub karty kodowej, np. ostrzeżenie o zbliżającej się utracie ważności lub prośba o kontakt z SMS z powodu problemów z kontem abonenckim.

d) *Pokaż numer identyfikacyjny karty kodowej konsumenta*

Numer identyfikacyjny karty kodowej lub innego środka identyfikacyjnego (ID) jest wyświetlany na ekranie. Nie jest to tajny numer ukryty w karcie tylko numer niechroniony, który bywa wydrukowany na karcie. Ta funkcja jest użyteczna do celów serwisowych.

e) *Zmiana daty przełączenia i ważności*

Ważną funkcją bezpieczeństwa jest możliwość zmiany algorytmów służących do deszyfrowania komunikatów upoważnień wysyłanych drogą radiową i odzyskiwania słów kontrolnych. W celu umożliwienia płynnego przejścia od jednego do następnego zestawu algorytmów wygodnie jest, jeżeli karta kodowa (lub inny przyrząd bezpieczeństwa) może przechowywać oba algorytmy wraz z datą przejścia od jednego do drugiego; data ta może być zmieniona zdalnie przez kanał radiowy. Dotyczy to również daty ważności, po upływie której karta staje się martwa.

8. Przegląd europejskich rozwiązań CAS

W różnych krajach europejskich stosowane są systemy kodowania pochodzące od różnych dostawców. Często też w jednym kraju można spotkać różne systemy kodowania w tym samym medium transmisyjnym (naziemnym, kablowym lub satelitarnym).

8.1. Dostawcy systemów CA

W krajach europejskich w systemach telewizji cyfrowej najczęściej spotyka się systemy CA oferowane przez:

- Conax AS (Conax),
- France Télécom SA (Viaccess),
- Irdeto Access BV (Irdeto, CryptoWorks),
- Latens Systems Ltd. (BCAS),
- NAGRAVISION SA (Mediaguard, Nagravision, SECA),
- NDS Group Ltd. (VideoGuard),
- SIDA (KeyFly).

Systemy te mogą być stosowane niezależnie od sposobu nadawania sygnału, tzn. są używane w systemach naziemnych, kablowych i satelitarnych. Systemy te są tak skonfigurowane, aby można było je używać zarówno w odbiornikach z wbudowanym CAS jak i za pomocą modułów CAM. Jest to podyktowane bardzo dużym udziałem w rynku odbiorników naziemnych, które wykorzystują moduły CAM do dekodowania sygnału skramblowanego.

8.2. Systemy CA spotykane w europejskiej DTT

Użycie poszczególnych systemów skramblowania dla cyfrowej telewizji naziemnej w wybranych krajach europejskich wygląda następująco:

- Dania: najprawdopodobniej wprowadzony będzie Viaccess przez operatora szwedzkiego (Boxer), który wygrał przetarg na budowę i dystrybucję cyfrowej telewizji naziemnej w Danii;
- Estonia: Conax (ZUUM TV);
- Finlandia: Conax (PlusTV, Canal Digital);
- Francja: MediaGuard/Nagra (Canal+), Viaccess (TNtop);
- Hiszpania: Nagra (TDT Premium);
- Holandia: Conax (KPN/Digitenne);
- Litwa: Conax (TEO/GalaTV);
- Łotwa: Conax (Lattelecom);
- Niemcy: Conax (RTL);
- Norwegia: Conax (RiksTV);
- Szwecja: Viaccess (Boxer, Viasat);
- Węgry: Conax (Terra+/Antenna Hungaria);
- Wielka Brytania: Nagravision (Top Up TV, Setanta Sports);
- Włochy: Irdeto (La7/Dahlia TV), Nagra (Mediaset), Conax (regionalni operatorzy), wszystkie trzy rozwiązania są zintegrowane w jednym oprogramowaniu, ale żadne z nich nie oferuje zaawansowanych mechanizmów bezpieczeństwa (produkty MPEG-2/SD).

Powyższa lista pokazuje, że w większości krajów występuje tylko jeden system skramblowania sygnału w telewizji naziemnej, co chroni użytkownika przed uciążliwością używania kilku różnych dekodowników (STB jak i CAM) do dostępu do usług telewizji płatnej.

8.3. Rynek dostawców płatnych usług w Polsce

Do największych dostawców płatnych usług na polskim rynku telewizyjnym zalicza się:

- Operatorzy TV-SAT: Cyfra+, Cyfrowy Polsat, Platforma n, TP,
- Operatorzy TVK: UPC, Vectra, Multimedia Polska, Aster, TOYA, INEA.

Na obecnym rynku płatnej telewizji cyfrowej nie widać dominacji żadnego z systemów kontroli dostępu do płatnych usług.

9. Regulacje prawne dla CAS

Zadaniem, jakie postawiła sobie grupa DVB, było opracowanie takiego rozwiązania, które umożliwiłoby konsumentowi posiadanie tylko jednego odbiornika i związanego z nim układu CA dla odbioru wszystkich dostępnych, zaszyfrowanych programów. W toku prac nie udało się osiągnąć całkowitego konsensusu w postaci jednego zestawu uzgodnień operacyjnych, związanych z funkcjonowaniem systemów warunkowego dostępu. Niemniej osiągnięty został pewien poziom standaryzacji wspólnych rozwiązań, które stały się inspiracją dla europejskiej legislacji.

Najważniejszym dokumentem prawnym dotyczącym systemów dostępu warunkowego jest Dyrektywa 95/47/WE Parlamentu Europejskiego i Rady o standardach transmisji telewizyjnej.

Dyrektywa ta zaleca stosowanie wspólnego deskramblera we wszystkich europejskich urządzeniach powszechnego użytku dla telewizji cyfrowej, w których dokonywany jest deskramblowanie. O transkontroli na granicy mediów mówi się w art. 4 lit. b w następujący sposób:

Funkcjonujące na europejskim rynku systemy dostępu warunkowego powinny mieć możliwości techniczne dla efektywnej cenowo transkontroli w kablowych stacjach czołowych, zapewniającej możliwość całkowitej kontroli, na poziomie lokalnym lub regionalnym, usług wykorzystujących takie systemy dostępu warunkowego.

Oznacza to, że operatorzy kablowi będą mogli w swoich stacjach czołowych wyselekcjonować cyfrowe usługi telewizyjne z całego, przesyłanego przez satelitę strumienia zmultipleksowanych i zaszyfrowanych informacji, a następnie ponownie zaszyfrować te usługi dla dystrybucji w swoich sieciach.

Do odbioru Pay-TV potrzebne są przystawki do odbiorników (set-top box), których koncepcja techniczna stanowi często własność operatora systemu CA, i których funkcje są przez tego operatora kontrolowane.

Do polskiego systemu prawnego regulacje dotyczące dostępu warunkowego zostały wprowadzone ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zmianami) w art. 133-135. Regulacje te, w największym skrócie, obligują operatorów CAS do oferowania nadawcom swoich usług na równych i niedyskryminacyjnych warunkach oraz dają upoważnienie ministrowi ds. łączności do wydania rozporządzenia określającego WT-E dla CAS i zakres usług oferowanych nadawcom. Ponadto, obligują dostawców rozwiązań CAS do zawierania umów licencyjnych na równych i niedyskryminacyjnych warunkach z producentami IRD, pozwalających na umieszczenie w odbiornikach elementów właściwych dla innych CAS³.

10. Kryteria oceny rozwiązań CAS

Do podstawowych kryteriów oceny różnych rozwiązań CAS należy zaliczyć:

- wygodę użytkownika,
- bezpieczeństwo systemu (odporność na piractwo),
- koszty po stronie odbiorczej,
- koszty po stronie nadawczej.

³ Jest to transpozycja zapisów Załącznika 1 Dyrektywy 2002/19/WE o dostępie do sieci łączności elektronicznej i urządzeń towarzyszących oraz wzajemnych połączeń (dyrektywa o dostępie)

10.1. Wygoda użytkownika

Od strony użytkownika CAS poza koniecznością wnoszenia opłat powinien być jak najmniej widoczny. W szczególności nie powinien wymagać specjalnych działań podczas zmiany kanałów (np. zmiany karty kodowej) lub wprowadzać znaczącego opóźnienia po wybraniu nowego kanału. Ponadto, uzyskanie dostępu do płatnych usług nie powinno się wiązać z nadmiernymi wydatkami i zabiegami. Idealna sytuacja będzie wtedy, gdy kompletny system będzie zintegrowany w odbiorniku telewizyjnym, dając możliwość dostępu do dowolnej kombinacji programów i usług dodatkowych opłaconych przez konkretnego abonenta.

Obecne systemy skramblowania charakteryzują się zbliżoną funkcjonalnością i są porównywalne jeśli chodzi o sposób użytkowania. Dzisiejsze systemy wbudowane CASS jak i odbiorniki, które wykorzystują moduły CAM nie różnią się pod względem wygody korzystania. Dobra konfiguracja systemu, poczynając od nadawcy a kończąc na odbiorniku, powinna pozwalać na jednokrotną instalację odbiornika wraz z kartą kodową i użytkowanie go przez cały czas bez potrzeby ingerencji manualnej czy też z poziomu menu.

System CA powinien udostępniać dane związane z danym abonentem w celu szybkiej identyfikacji w razie sytuacji awaryjnych. Dane te powinny być dostępne z poziomu menu dla użytkownika, który może je podać w razie potrzeby osobie z obsługi usług płatnych.

Czynnikami pogarszającymi wygodę użytkownika są (uszeregowane w od najbardziej uciążliwych):

- a) różne systemy skramblowania (od różnych producentów),
 - w przypadku urządzeń z wbudowanym CASS zwykle konieczność posiadania kilku urządzeń,
 - w przypadku urządzeń z CI konieczność posiadania kilku modułów CAM i ich podmiany w trakcie przełączania między kanałami,
- b) skomplikowane modele biznesowe – różne karty kodowe do różnych pakietów.

10.2. Bezpieczeństwo systemu

Dobry CAS powinien się cechować odpowiednią skutecznością w przeciwdziałaniu piractwu czyli dostępu do programów i usług przez osoby nieuprawnione. Choć nie istnieje CAS całkowicie bezpieczny, to łączne zastosowanie odpowiednich środków technicznych i przepisów prawa skierowanych przeciwko piractwu powinno czynić ten proceder trudnym i nieopłacalnym. Karty kodowe powinny być trudne do podrobienia.

Ważne są relacje pomiędzy dostawcami treści a operatorem CAS. Powinny one zobowiązywać operatora do podjęcia skutecznego przeciwdziałania piractwu, jeżeli osiągnie ono określony poziom.

10.3. Otwarty rynek dostawców odbiorników TV

Konsumenci powinni korzystać z dobrodziejstw szerokiego wyboru odbiorników cyfrowych iDTV i STB produkowanych przez wielu wytwórców konkurujących na otwartym rynku. Wymaga to zdefiniowania minimalnego zestawu wymagań techniczno-eksploatacyjnych dla odbiornika, opartych na normach międzynarodowych. Pełna standaryzacja nie może dotyczyć szczegółów CA ale powinna zapewniać niezbędną elastyczność w tym zakresie.

Rynek producentów odbiorników telewizji cyfrowej możemy podzielić na trzy poniższe grupy:

- iDTV,
- STB,
- inne (w tym karty PC/USB).

Ostatnia grupa urządzeń wykracza poza obszar niniejszego opracowania.

Producenci odbiorników iDTV nie planują wprowadzenia wbudowanego CASS do swoich produktów. Wynika to z potrzeby zapewnienia uniwersalności odbiorników np. dla całego rynku europejskiego.

Większość urządzeń z grupy STB ma wbudowany CASS jednego producenta a konkretny model jest dedykowany na jedno państwo lub konkretnego operatora. Podyktowane jest to kosztami produkcji. Istnieją natomiast wyjątki gdy w kraju ustalony jest jeden system skramblovania, co daje możliwość używania urządzenia w różnych sieciach.

10.4. Otwarty rynek dostawców treści

Wszystkie koncesjonowane programy powinny być dostępne dla każdego użytkownika posiadającego IRD spełniającego odpowiednie wymagania i mającego specjalne upoważnienia wydane przez właściwego operatora CAS. Także dostawcy treści i usług dopuszczonych do rozpowszechniania powinni mieć prawo dostępu do odpowiednich platform dostępowych na równych i godziwych warunkach.

Do dostawców treści zalicza się producentów, którzy produkują materiał audiowizualny lub oferują go w postaci filmów i różnego typu programów. Podmioty te mają znaczący wpływ na wybór całego systemu skramblovania, biorąc głównie pod uwagę jego bezpieczeństwo. O ile dla materiałów nadawanych w jakości SD, dostawcy treści dopuszczają stosowanie rozwiązań mniej bezpiecznych (np. CI w wersji 1), to dla materiałów w jakości HD wymagają najbezpieczniejszych obecnie dostępnych rozwiązań pod groźbą zerwania kontraktów na dostarczanie materiału.

10.5. Niezależność funkcjonowania dostawców usług

Podstawowa umowa jest zawierana pomiędzy dostawcą usług a widzem. Pomimo tego, że w procesie rozpowszechniania mogą być zaangażowane inne podmioty (jak np. operatorzy sieci nadawczych lub operatorzy CAS), to system CA i inne części całego łańcucha przekazywania treści nie powinny wymagać od dostawcy usług ujawniania konkurentom danych wrażliwych, które mogłyby posłużyć do identyfikacji klientów i ich upoważnień do oglądania.

10.6. Niskie koszty początkowe i operacyjne

Koszty uruchomienia i funkcjonowania CAS są znaczne ale nie mogą być zaporowe. W szczególności, powinny pozwalać na skalowanie rozmiarów systemu w celu minimalizacji kosztów rozruchu przy niewielkiej liczbie abonentów.

System nie powinien ograniczać maksymalnej liczby obsługiwanej gospodarstw domowych, która może osiągać rząd kilku dziesiątek milionów. Koszty ulepszeń i odzyskiwania naruszonego bezpieczeństwa powinny być minimalizowane przez wybór niezawodnego i bezpiecznego systemu.

11. Wnioski i zalecenia

11.1. Wnioski

Z powyższych rozważań wynika, że decyzja o wybraniu zarówno systemu skramblovania jak i modelu transakcyjnego jest bardzo ważna dla przyszłych usług płatnej telewizji naziemnej.

Należy zwrócić uwagę, że mimo istnienia teoretycznej możliwości dopuszczania na rynek urządzeń przystosowanych do różnych systemów skramblovania, istnieje duże prawdopodobieństwo, że wprowadzenie wybranego rozwiązania w niektórych albo znacznej większości produktów się nie powiedzie. W większości przypadków już teraz do zabezpieczania programów płatnych wymagane są bezpieczniejsze wersje systemów skramblovania, które wykorzystują dedykowane rozwiązania sprzętowe, a w przyszłości należy spodziewać się, że będzie to obowiązującym standardem. To wyklucza łatwą i taną możliwość wymiany lub dołożenia systemu skramblovania do odbiorników cyfrowych. Mowa głównie o urządzeniach, które mają wbudowany CASS (STB).

Należy zauważyć również, że w większości krajów europejskich ustalony został jeden system skramblovania dla telewizji naziemnej, a nawet w niektórych ten sam jest używany dla wszystkich trzech mediów: naziemnego, kablowego i satelitarnego.

11.2. Zalecenia

1. Wybór jednego systemu skramblowania używanego do wszystkich serwisów płatnych nadawanych w polskiej DTT. Zapobiegnie to sytuacji, gdy każdy skramblowany serwis trzeba będzie dekodować przy użyciu innego urządzenia.
2. Wybór jednego operatora (hurtowego) zarządzającego systemem dostępu warunkowego, tak aby użytkownik mógł za pomocą jednej karty kodowej otrzymać dostęp do różnych pakietów płatnej telewizji pochodzących od różnych dostawców. Zapobiegnie to konieczności fizycznej podmiany kart przy każdej zmianie kanału.
3. Przy wyborze całego systemu dostępu warunkowego należy wziąć pod uwagę bezpieczeństwo systemu, szczególnie jeśli chodzi o ochronę programów HD zarówno po stronie nadawczej jak i odbiorczej. W tym drugim przypadku należy zdefiniować wymagania bezpieczeństwa dla odbiorników uniwersalnych bez wbudowanego CASS. Obecnie jedynie standard CI+ zapewniający wystarczający poziom bezpieczeństwa, który może być akceptowany przez dostawców treści.

12. Definicje

Określenia użyte w dokumencie oznaczają:

- 12.1. Algorytm – dokładny przepis wykonania w określonym porządku skończonej liczby operacji, pozwalający na rozwiązanie każdego zadania danego typu.
- 12.2. Audycja – część programu stanowiąca odrębną całość ze względu na treść, formę, przeznaczenie i autorstwo.
- 12.3. Bukiet – zestaw usług RTV oferowanych jako oddzielna całość.
- 12.4. Deszyfrowanie – proces zamiany szyfrogramu na tekst jawny z wykorzystaniem szyfru i klucza.
- 12.5. Deskrablowanie – proces usuwania skutków skramblowania w celu odzyskania dostępu do zaszyfrowanych wiadomości.
- 12.6. Dostęp warunkowy – zapewnianie przez nadawców i operatorów stosujących odpowiednie środki techniczne, możliwości odbioru przesyłanych usług tylko uprawnionym do tego osobom.
- 12.7. Karta kodowa – (ang. *smart-card*) „karta-klucz” rozmiarów karty kredytowej wkładana do czytnika w celu uzyskania możliwości odbioru programu(ów), za które abonent poniósł opłatę. Także: karta elektroniczna, karta czipowa.
- 12.8. Klucz – w kryptografii parametr, którego wartość wpływa na wynik procesu szyfrowania i deszyfrowania.
- 12.9. Klucz elektroniczny – ogólne określenie dla sygnałów danych używanych do kontrolowania procesu deskrablowania w dekodernach. Istnieje wiele różnych poziomów klucza służących do: identyfikacji sieci, do których abonent ma prawo dostępu, usług dostępnych dla abonenta w tych sieciach oraz szczegółowych informacji sterujących działaniem deskramblera. ECM jest jednym ze składników danych klucza.
- 12.10. Komunikat kontroli uprawnień – (ECM) szyfrogram słowa kontrolnego i warunków dostępu. ECM jest ściśle określonym elementem sygnału klucza elektronicznego o informacji adresowej odbieranej przez wejście antenowe. ECM jest stosowany do sterowania deskramblerem i przesyłany w postaci zaszyfrowanej w strumieniu TS.
- 12.11. Komunikat zarządzania uprawnieniami – (EMM) wiadomość pozwalająca abonentowi na deskrablowanie usługi. EMM jest ściśle określonym elementem sygnału klucza elektronicznego o informacji adresowej odbieranej przez wejście antenowe. EMM jest stosowany do włączania/wyłączania grup lub pojedynczych dekodernów i przesyłany w postaci zaszyfrowanej w strumieniu TS lub łączem telekomunikacyjnym.

- 12.12. MultiCrypt – otwarty CAS wykorzystujący zewnętrzny CAM dołączany do IRD poprzez standardowy interfejs (CI, CI+) i eliminujący konieczność umieszczania w IRD bloku dostępu warunkowego.
- 12.13. Multipleks – strumień danych cyfrowych składający się z programów i usług dodatkowych, przesyłany w jednym kanale.
- 12.14. Odbiornik cyfrowy – urządzenie przeznaczone dla użytkownika końcowego do odbioru sygnałów telewizji cyfrowej zawierające co najmniej tuner (obejmujący głowicę w.cz. i demodulator), demultiplekser i dekodery odbieranych usług oraz wyświetlacz obrazu (iDTV) albo nie zawierające wyświetlacza obrazu (STB).
- 12.15. Nadawca – podmiot, który tworzy lub zestawia programy oraz przekazy z nimi związane, uprawniony do ich rozpowszechniania.
- 12.16. Platforma cyfrowa – zestaw składający się z oprogramowania (software, middleware) i sprzętu (hardware) zapewniający dostęp do usług cyfrowych dostarczanych określonym kanałem telekomunikacyjnym. Innymi słowy, platforma to jest to, co można odebrać za pomocą odbiornika-dekodera telewizji cyfrowej spełniającego określony zestaw wymagań techniczno-eksploatacyjnych.
- 12.17. Podsystem dostępu warunkowego – (CASS) część IRD odpowiedzialna za deszyfrowanie kluczy elektronicznych oraz odzyskiwania informacji niezbędnej do kontrolowania sekwencji deskrambrowania.
- 12.18. Program – uporządkowany zestaw audycji radiowych lub telewizyjnych, reklam oraz przekazów o charakterze pomocniczym w stosunku do zawartości audycji lub programu, regularnie rozpowszechniany, wytworzony przez jednego nadawcę.
- 12.19. Radiodyfuzja – służba radiokomunikacyjna polegająca na rozpowszechnianiu bezprzewodowym (naziemnym i satelitarnym) przeznaczonym zasadniczo do dostarczania szerokiej publiczności sygnałów wizyjnych, fonicznych, usług multimedialnych i przesyłania danych. Do dostarczania informacji do ogólnie dostępnych odbiorników powszechnego użytku, rozpowszechnianie bezprzewodowe wykorzystuje system „punkt – wszędzie”.
- 12.20. Rozpowszechnianie – udostępnianie odbiorcom programów i informacji z nim związanych.
- 12.21. SimulCrypt – system pozwalający na odbiór skramblowanych sygnałów przez dekodery wykorzystujące różne systemy dostępu warunkowego, ponieważ stosuje wspólny CSA i CW.
- 12.22. Skramblowanie – operacja wykorzystywana w telekomunikacji do takiego przekształcenia (zniekształcenia) sygnału niosącego wiadomość po stronie nadawczej aby uczynić ją nieczytelną dla odbiornika pozbawionego odpowiedniego urządzenia tzw. deskramblera. Początkowo termin ten odnosił się do transmisji analogowej, w odróżnieniu do szyfrowania stosowanego w domenie cyfrowej. Inna nazwa to randomizacja.
- 12.23. Słowo kontrolne – (CW) klucz używany przez deskrambler.
- 12.24. System autoryzacji abonentów – (SAS) centrum odpowiedzialne za organizację, sekwencje oraz dostarczanie strumieni danych EMM i ECM pod nadzorem SMS.
- 12.25. System dostępu warunkowego – (CAS) system stosowany w celu kontrolowania pobierania opłat i ochrony praw autorskich. W systemie takim emitowany program jest szyfrowany – rozkodowanie, czyli dostęp, jest możliwe dzięki odpowiedniemu dekoderoowi lub poprzez ważne narzędzie dostępu (na przykład w postaci karty-kłucza wkładanej do czytnika w dekodерze).
- 12.26. System obsługi abonentów – (SMS) centrum wydające karty kodowe, wysyłające faktury i zbierające opłaty od abonentów. Podstawą działania SMS jest baza danych o abonentach, numerach seryjnych dekodерów oraz opłaconych usługach.
- 12.27. Szyfr – para algorytmów służących do szyfrowania i deszyfrowania.
- 12.28. Szyfrogram – wiadomość, która została zaszyfrowana.

- 12.29. Szyfrowanie – proces przekształcania tekstu jawnego w szyfrogram za pomocą szyfru i klucza.
- 12.30. Usługa (serwis) – sekwencja zdarzeń, audycji lub danych, tu: program.
- 12.31. Zdarzenie (ang. *event*) – grupa nadawanych elementarnych strumieni danych należących do tej samej usługi ze zdefiniowanym czasem początku i końca (np. połowa meczu, reklama, zająwka).

13. Skróty i akronimy

Użyte w dokumencie skróty i akronimy oznaczają:

AES	Advanced Encryption Standard (Zaawansowany standard szyfrowania)
CA	Conditional Access (Dostęp warunkowy)
CAM	Conditional Access Module (Moduł dostępu warunkowego)
CAS	Conditional Access System (System dostępu warunkowego)
CASS	CAS Subsystem (Podsystem CAS)
CATV	Cable TV (Telewizja kablowa – TVK)
CENELEC	Comité Européen de Normalisation ELEctrotechnique (Europejski Komitet Normalizacji Elektrotechniki)
CI	Common Interface (Wspólny interfejs)
CI+	Common Interface Plus (Rozszerzenie wspólnego interfejsu)
CSA	Common Scrambling Algorithm (Wspólny algorytm skramblowania)
CW	Control Word (Słowo kontrolne)
CWG	Control Word Generator (Generator CW)
DRM	Digital Right Management (Cyfrowe zarządzanie prawami)
DES	Data Encryption Standard (Standard szyfrowania danych)
DTT	Digital Terrestrial TV (Naziemna telewizja cyfrowa)
DVB	Digital Video Broadcasting (Telewizja cyfrowa DVB)
DVB-T	Digital Video Broadcasting – Terrestrial (Naziemna telewizja cyfrowa DVB)
ECM	Entitlement Control Message (Komunikat kontroli uprawnień)
EMM	Entitlement Management Message (Komunikat zarządzania uprawnieniami)
EN	European Norm (Norma Europejska)
ETR	ETSI Technical Report (Raport Techniczny ETSI)
ETSI	European Telecommunications Standards Institute (Europejski Instytut Norm Telekomunikacyjnych)
HD	High Definition (Wysoka rozdzielczość – tu: 1920 × 1080 lub 1280 × 720 pikseli)
HDTV	High-Definition TeleVision (Telewizja o wysokiej rozdzielczości)
iDTV	integrated Digital TV (Zintegrowany odbiornik TV cyfrowej: IRD + wyświetlacz)
IEC	International Electrotechnical Commission (Międzynarodowa Komisja Elektrotechniczna)
IRD	Integrated Receiver-Decoder (Zintegrowany odbiornik i dekodery)
ISO	International Organisation for Standardisation (Międzynarodowa Organizacja Standaryzacyjna)
MHEG	Multimedia and Hypermedia Experts Group (Grupa Ekspertów ds. Multimediów i Hipermidiów)
MHEG-5	Standard obsługi aplikacji interaktywnych poziomu podstawowego opisany normą ISO/IEC 13522-5
MPEG	Moving Picture Experts Group (Grupa Ekspertów ds. Ruchomych Obrazów)
MPEG-2	Rodzina standardów kodowania wizji i fonii opisana normą ISO/IEC 13818

PCMCIA	Personal Computer Memory Card International Association (Międzynarodowe Stowarzyszenie Kart Pamięci Komputerów Osobistych)
PIN	Personal Identification Number (Osobisty numer identyfikacyjny)
PPV	Pay-per-View (Opłata z góry za konkretną audycję)
PVR	Personal Video Recorder (Osobisty Rejestrator Wideo)
SAS	Subscriber Authorization System (System autoryzacji abonentów)
SD	Standard Definition (Standardowa rozdzielczość – tu: 720 × 576 pikseli)
SDTV	Standard-Definition TeleVision (Telewizja o standardowej rozdzielczości)
SMS	Subscriber Management System (System obsługi abonentów)
STB	Set-Top Box (IRD w postaci samodzielnego urządzenia dołączanego do odbiornika TV)
TR	Technical Report (Raport techniczny ETSI)
TS	Technical Specification (Przed 6-cyfrowym numerem – Specyfikacja techniczna)
TS	Transport Stream (Strumień transportowy)
TV	TeleVision (Telewizja)
VoD	Video on Demand (Wideo na życzenie)

14. Bibliografia

- [1] Functional model of a conditional access system. EBU Technical Review. Winter 1995.
- [2] Conditional Access System. Damian Gajewski, Politechnika Poznańska 2005.
- [3] DVB A011 Common Scrambling Algorithm. DVB Blue Book A011.
- [4] EN 300 468 Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems. ETSI.
- [5] ETR 162 Digital Broadcasting Systems for Television, Sound and Data Services; Allocation of Service Information (SI) Codes for Digital Video Broadcasting (DVB) Systems. ETSI.
- [6] ETR 289 Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access within digital broadcasting systems. ETSI.
- [7] TR 101 211 Digital Broadcasting Systems for Television, Sound and Data Services; Guidelines on the Implementation and Usage of DVB Service Information. ETSI.
- [8] TS 101 699 Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification. ETSI.
- [9] TS 102 201 Digital Video Broadcasting (DVB); Interfaces for DVB Integrated Receiver Decoder (DVB-IRD). ETSI.
- [10] ISO/IEC 7816, 1-3 Identification cards – Integrated circuit cards with contacts, Parts 1-3.
- [11] ISO/IEC 13818-1 Information Technology – Generic Coding of Moving Pictures and Associated Audio Information. Part 1: Systems.
- [12] EN 50221:1997 Common Interface for Conditional Access and other DVB Decoder Applications. CENELEC.
- [13] R206-001:1998 Guidelines for Implementation and Use of the Common Interface for DVB Decoder Applications. CENELEC.
- [14] Recommendation ITU-R BT.810 Conditional-access broadcasting systems.
- [15] CI Plus Specification. Content Security Extensions to the Common Interface V1.2. April 2009.CI Plus LPP.
- [16] Dyrektywa 95/47/WE Parlamentu Europejskiego i Rady o standardach transmisji telewizyjnej.

- [17] Dyrektywa 2002/19/WE o dostępie do sieci łączności elektronicznej i urządzeń towarzyszących oraz wzajemnych połączeń (dyrektywa o dostępie).
- [18] Ustawa z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zmianami).
- [19] Rozporządzenie Ministra Infrastruktury z dnia ... 2009 r. w sprawie wymagań technicznych i eksploatacyjnych dla urządzeń konsumenckich służących do odbioru cyfrowych naziemnych transmisji telewizyjnych. Dz. U. nr
- [20] Wymagania na odbiornik dla polskiej naziemnej telewizji cyfrowej Profil 0, 1 i 2 w. 0.6. Maj 2009.