Obrázek 1 - princip šifrování v režimu 1 (obrázek 1 normy)

Pro zašifrování kontrolního slova norma poskytuje 2 režimy. Při režimu 1 se použije standardní předsdílená tabulka TISA ke generování klíčů a při režimu 2 se použije specifická tabulka, kterou výrobce a poskytovatel na základě podepsané smlouvy mezi sebou nasdílí. Pro generování klíče služby v režimu 1 specifikace využívá 2 předsdílených tajemství, tabulku klíčů TISA a tabulku 16 krátkých náhodných čísel.

Článek 6.3 popisuje zašifrování a rozšifrování užitečného obsahu rámce služeb. Je popsán "režim blokové šifry", jedná se o způsob provázání bloků, aby se symetrická šifra dala použít na šifrování proudu dat. Článek odkazuje konkrétní normy které se mají pro daný účel použit a které k šifrovacím metodám obsahují více informací. Také je popsána struktura a účel tzv. inicializačního vektoru.

Článek 6.4 popisuje zašifrování a rozšifrování kódových slov (CW), kódová slova jsou při přenosu zašifrována klíčem služby, používá se režim ECB podle specifikace NIST 800-38A.

Článek 6.5 popisuje složení klíče služby určeného k šifrování CW. Klíče nejsou přenášeny, ale jsou nakombinovány z již existujících informací a přijaté konfigurace. Je přesně popsán způsob složení klíče pro oba režimy. Tento popis je doplněn konkrétním příkladem (1 strana).

7 Struktura LTE a zahrnutí do rámce služby TPEG

Tato kapitola (rozsah 3 strany, 3 obrázky) popisuje struktury LTE obrázkem a UML modelem.

Nejprve je uvedeno, jak je šifrování zahrnuto do rámce služby (článek 7.2), a poté je představen UML model celé struktury LTE (článek 7.3).

Obrázek 2 - Složení, komprese, šifrování a rámec pro TPEG LTE (obrázek 7 normy)

Článek 7.4 uvádí jedním obrázkem v normě stanovené tabulky (viz kap 10). Článek 7.5 (odstavec a 5 odrážek) popisuje přesný postup složení inicializačního vektoru a článek 7.6 (4 odrážky) popisuje přesný postup složení klíče služby.

8 Komponenty zprávy LTE

Tato kapitola (rozsah 3 stran, 5 tabulek) obsahuje popis komponent LTE.

Struktury se skládají ze složitých či jednoduchých datových objektů, výskyt každé položky datové struktury (tj. její multiplicita) je doplněn datovým typem a popisem. Tabulka níže uvádí datové struktury stanovené v této kapitole.

Tabulka 1 - Seznam stanovených datových typů (zdroj: autor extraktu)

Komponenta LTE	popis
LteInformation	verze, režim, indikátor metody komprese a parametry rámce
LteParameters	verze kódového slova (CW) použitého pro zašifrování rámce
LteMode2Parameters	viz výše + inicializační kód "nonce", počet zákazníků a informace o oprávněních jednotlivých zákazníků v režimu 2.
Mode1EMMessage	informace o oprávněních v režimu 1, index klíče z tabulky klíčů TISA, zašifrované kódové slovo CW.
Mode2EMMessage	identifikace zákazníka, verze kódového slova, režim šifrování a zašifrované kódové slovo CW.

9 Datové typy LTE

Tato kapitola (rozsah 0,5 strany) obsahuje definice 2 datových položek typu Int, kódového slova (ControlWord) a inicializace (Nonce).

10 Tabulky LTE

Tato kapitola (rozsah 1 strana, 2 tabulky) obsahuje definice jedné struktury a 1 výčtového typu. Struktura LteMode1Parameters stanovuje použití konkrétní verze kódového slova, inicializačního slova a režimu zprávy.

Jeden výčtový typ lte001:LightEncryptionMode, obsahuje hodnoty “režim 1” a “režim 2”

Příloha A (normativní) – TPEG-bin reprezentace LTE

Tato příloha (rozsah 6 stran) stanovuje binární reprezentaci obsahu datového rámce služby při použití režimů Light Encryption 1 nebo 2 pro použití v digitálním rozhlase (DAB). Pro popis binární reprezentace je použit pseudokód, kde pro každé klíčové slovo zapsané struktury je znám jeho binární tvar.

Příloha nejprve popisuje specifikaci rámce s LTE poté atributy a následně obsahuje samostatně uvedené binární reprezentace zprávy LTE a jejích součástí, prvků určených pro budoucí rozšíření a datových typů.

Specifikace rámce vychází z CEN TS 21219-5 a stanoví použití identifikátoru služby, který musí obsahovat ServEncID a indikaci režimu, dále stanoví, jak přenášet (resp. s jakými údaji) zašifrované složky služby.

Atributy stanoví velikost a způsob výpočtu CRC, použití kryptografické funkce AES128 a použití komprese.

V následující tabulce je uveden příklad pseudokódu binární specifikace prvku LteInformation .

Tabulka 2 - Příklad pseudokódu binární specifikace prvku LteInformation (článek A.3.2 normy)

<LteInformation(0)>:=	
<**IntUnTi**>(0),	: id této komponenty
<**IntUnLoMB**>(lengthComp),	: počet bajtů v komponentě
<**IntUnLoMB**>(lengthAttr),	: počet bajtů v atributech
<**MajorMinorVersion**> (specVersionID),	: Major a Minor verze specifikace Light Encryption, která se používá k šifrování (a případně kompresi) multiplexu komponenty služby.
<lte001:LightEncryptionMode> (lteMode),	: Aktivní režim šifrování používaný poskytovatelem služby pro tuto službu. Používaný šifrovací režim se může pro službu v průběhu času měnit, ale po každé změně šifrovacího režimu musí všechny rámce používat stejný šifrovací režim až do další změny šifrovacího režimu.
...	...

Příloha B (normativní) – TPEG-ML reprezentace LTE

Tato příloha (rozsah 5 stran) obsahuje nejprve samostatně uvedené XML schéma rámce TPEG, zašifrované zprávy a jejích součástí, prvků určených pro budoucí rozšíření a datových typů LTE (definovaných jako xs:complexType). Následně uvádí výše zmíněné samostatně uvedené XML schémata v jednom funkčním XML schématu.

```
<xs:element name="LteInformation" type="LteInformation"/>
<xs:complexType name="LteInformation">
 <xs:complexContent>
  <xs:extension base="tsf:ApplicationRootMessageML">
   <xs:sequence>
    <xs:element name="specVersionID" type="tdt:MajorMinorVersion"/>
    <xs:element name="lteMode" type="lte001_LightEncryptionMode"/>
    <xs:element name="payloadCompressionServEncID" type="tdt:IntUnTi"/>
    <xs:element name="lteParamsForFrame" type="LteParameters"/>
   </xs:sequence>
  </xs:extension>
 </xs:complexContent>
</xs:complexType>
```

Obrázek 3 - Výstřižek XML schématu stanovujícího strukturu prvku LteInformation (část B.2.1 normy)

Příloha C (informativní) – Pokyny pro jednoduché šifrování

Tato příloha (rozsah 4 strany) popisuje pravidla pro použití jednoduchého šifrování klientem a serverem služby TPEG.

Článek 2 přílohy popisuje 2 režimy provozu, kdy je šifrování použito za účelem omezení přístupu k právě testované, aktualizované službě či ryze komerční režim, pro omezení přístupu některým zákazníkům (b2b). Výčtem jsou popsány případy užití jednoho či druhého režimu.

Článek 3 popisuje pravidla pro poskytovatele služby, jsou popsány (odstavec textu) 4 případy užití od použití komprese, přes změnu kódového slova až po změnu oprávnění zákazníka v režimu 2.

Článek 4 popisuje pravidla pro uživatele (výrobce terminálů), je popsáno (odstavec textu) 7 případů užití od “Zjištění služby LTE v režimu 1” přes monitorování a kešování kódových slov po povinnosti výrobce pro autorizovaný přístup ke službě.

Související normy

- ISO TS 21219-1 - Inteligentní dopravní systémy – Dopravní a cestovní informace v dopravním protokolu expertní skupiny, druhá generace (TPEG2) – Část 1: Úvod, číslování a verze
- ISO TS 21219-2 - ITS – Dopravní a cestovní informace v dopravním protokolu expertní skupiny, druhá generace (TPEG2) – Část 2: Pravidla modelování pomocí UML
- CEN ISO TS 21219-3 - ITS – Zprávy TTI předávané označovacím jazykem s možností rozšíření Expertní skupiny protokolů pro dopravu, druhá generace (TPEG 2) – Část 3: Pravidla pro konverzi z UML do binárního kódu
- CEN ISO TS 21219-4 - ITS – Zprávy TTI předávané označovacím jazykem s možností rozšíření Expertní skupiny protokolů pro dopravu, druhá generace (TPEG 2) – Část 4: Pravidla pro konverzi UML do XML
- ISO TS 21219-5 - Inteligentní dopravní systémy – Dopravní a cestovní informace v dopravním protokolu expertní skupiny, 2. generace (TPEG2) – Část 5: Rámec pro služby TPEG
- ISO/TS 21219-9 - Inteligentní dopravní systémy – Dopravní a cestovní informace v dopravním protokolu expertní skupiny, druhá generace (TPEG2) – Část 9: Informace o službách a síti
- CEN ISO TS 21219-7 - ITS – Zprávy TTI předávané označovacím jazykem s možností rozšíření Expertní skupiny protokolů pro dopravu, druhá generace (TPEG 2) – Část 7: Kontejner pro odkazování na polohu

Související termíny

- dopravní protokol expertní skupiny

© Silmos, s.r.o. 2018 - 2025. *Pomůžeme Vám se zorientovat v oboru Dopravní telematiky a najít správnou normu.*