EXTRAKT z technické specifikace ISO

Extrakt nenahrazuje samotnou technickou normu, je pouze informativním materiálem o normě.

Inteligentní dopravní systémy – Dopravní a cestovní informace v dopravním protokolu expertní skupiny, druhá generace (TPEG2) – Část 10: Informace o podmíněném přístupu

ISO/TS 21219-10

01 8259

Vydána 2016, 10 stran

Úvod

Technická specifikace ISO 21219 se zabývá druhou generací protokolu TPEG pro **poskytování informací o dopravě koncovým uživatelům**, označovaným TPEG2.

ISO/TS 21219 obsahuje řadu částí, které pokrývají úvod, pravidla, "sady nástrojů" (toolkity) a jednotlivé aplikace. TPEG2 je postaven na modelování v UML, se sadou základních pravidel stanovujících strategii modelování a pravidla konverze modelu do dvou fyzických formátů: binárního pro vysílání v DAB a XML pro šíření Internetem (části 2, 3, 4 normy). Pro snazší udržovatelnost specifikace se změny provádí pouze na úrovni obecného modelu v UML (XMI soubor) a následně pomocí automatizovaných nástrojů převádějí do popisů jednotlivých fyzických formátů (dokument s přílohami pro každý fyzický formát). Tato koncepční témata jsou řešena částmi, které se nazývají sady nástrojů (toolkity).

TPEG2 stanovuje použití tří dílčích částí (kontejnerů): management zpráv (část 6 normy), dopravní aplikaci (mnoho částí) a odkazování na polohu (část 7 normy).

ISO/TS 21219 se skládá z těchto částí (tučně je zvýrazněna část popisovaná v tomto extraktu):

- **Toolkity** (nástroje): TPEG2-INV (část 1: Úvod, číslování a verze), TPEG2-UML (část 2: Pravidla modelování pomocí UML), TPEG2-UBCR (část 3: Pravidla pro konverzi z UML do binárního kódu), TPEG2-UXCR (část 4: Pravidla pro konverzi UML do XML), TPEG2-SFW (část 5: Rámec pro služby TPEG), TPEG2-MMC (část 6: Kontejner pro management zpráv), TPEG2-LRC (část 7: Kontejner pro odkazování na polohu)
- **Speciální aplikace**: TPEG2-SNI (část 9: Informace o službách a síti), **TPEG2-CAI (část 10: Informace o podmíněném přístupu)**, TPEG2-LTE (část 24: Slabé šifrování)
- **Odkazování na polohu**: TPEG2-ULR (část 11: Odkazování na polohu v aplikacích), TPEG2-ETL (část 20: Odkazování na polohu metodou rozšířeného TMC), TPEG2-GLR (část 21: Geografické odkazování na polohu), TPEG2-OLR (část 22: Odkazování na polohu metodou OpenLR)
- **Aplikace**: TPEG2-RTM (část 12: Aplikace pro zprávy o silniční dopravě), TPEG2-PTI (část 13: Aplikace pro informace o veřejné dopravě), TPEG2-PKI (část 14: Aplikace pro informace o parkování), TPEG2-TEC (část 15: Aplikace pro vybrané dopravní události), TPEG2-FPI (část 16: Aplikace pro informace o cenách pohonných hmot), TPEG2-SPI (část 17: Aplikace pro informace o rychlostních omezeních), TPEG2-TFP (část 18: Aplikace pro informace o stavu dopravního proudu a jeho predikci), TPEG2-WEA (část 19: Aplikace pro informace o počasí), TPEG2-RMR (část 23: Aplikace pro informace o multimodálních trasách), TPEG2-EMI (část 25: Nabíjecí infrastruktura pro elektromobily) a další.

Na rozdíl od RDS-TMC, které je svým způsobem popisu události jednoúrovňové, umožňuje TPEG informace členit strukturovaně se zvyšující se mírou detailu. Dopravní události popisuje TPEG úzkoprofilově, je vždy zaměřen na jeden konkrétní typ situací (například pro ceny pohonných hmot, dojezdové doby atd.), které popisuje do větší hloubky, každému typu je věnována samostatná část specifikace (tzv. "aplikace TPEG").

Rozlišení TPEG/TPEG1/TPEG2 se většinou uvádí pouze v úvodu částí norem/specifikací, zatímco ostatní kapitoly již mezi TPEG a TPEG2 nerozlišují - to je implicitní dle kontextu. Stejným způsobem k tomu přistupujeme i v tomto extraktu.

Tento extrakt popisuje část 10 „Informace o podmíněném přístupu (CAI)" (dále jen "popisovaný dokument"), která specifikuje obálku komponenty CAI a popisuje vhodnost linkování komponent CAI se zašifrovaným obsahem v jiných komponentách služby.

Poznámka: Extrakt přejímá původní číslování kapitol.

Užití

Části přenášených informací mohou být zašifrovány a tím podmíněně zpřístupněné pouze odběratelům vlastnícím dešifrovací klíč. Tato část se zabývá poskytnutím informací o tom, které části služby jsou nějakým způsobem zašifrovány (a tím podmíněně přístupné).

Popisovaný dokument stanovuje obálku pro informace o podmíněném přístupu. Obálka je v rámci služby přenášena současně s ostatními komponentami služby a informuje o zašifrovaných komponentách. Dokument odkazuje na TPEG2-SNI a TPEG2-SWF, které stanovují, jak mají vypadat zašifrované komponenty služby a jak na ně odkazovat. Konkrétní struktura kontejneru aplikace CAI není v tomto dokumentu stanovena.

Popisovaný dokument je vhodný pro programátory a tvůrce zašifrovaných služeb, které informuje o způsobu předávání informací o podmíněném přístupu (zašifrovaných částech služby). Pro samotnou implementaci podmíněného přístupu nestačí, zde jsou potřeba další normy, viz výše.

Souvisící normy (výběr)

Klíčové normy, na které tento dokument odkazuje, jsou: specifikace TPEG2 části 1 až 6 a 9. Důležité jsou zejména TPEG2-SNI (část 5) a TPEG2-SWF (část 9).

1 Předmět

Popisovaný dokument definuje aplikaci TPEG2-CAI „podmíněného přístupu" na úrovni komponenty služby. Ta umožňuje chránit obsah služby TPEG před neoprávněným přístupem. Dále zmiňuje správu informací o odběratelích na klientských zařízeních za účelem nastavení, prodloužení nebo zrušení předplatného na daném klientském zařízení.

3 Termíny a definice

Tato kapitola definuje dva termíny, služba a komponenta služby.

služba *(service)* – sbírka různých informačních toků (aplikací) logicky spojených a dodaných od poskytovatele služeb koncovému uživateli

komponenta služby *(service component)* – součást služby ze kterých může být služba poskládána

4 Zkratky

Tato kapitola stanoví 16 zkratek. V kapitole jsou uvedeny pouze některé zkratky částí normy TPEG. Tyto zkratky uvádíme v úvodu tohoto extraktu, proto je zde dále neuvádíme.

TPEG dopravní protokol expertní skupiny *(transport protocol experts group)*

EncID identifikace šifrování *(encryption identifier*)

AID identifikace aplikace (*application identification)*

CAI informace o podmíněném přístupu (*conditional access information)*

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology (www.itsterminology.org).

5 Podmínky a omezení aplikace

Tato kapitola (rozsah 1/2 strany) nejprve vymezuje použití identifikátoru aplikace (AID) v rámci informací o službě; každá „aplikace" TPEG má svůj identifikátor stanovený v části 1 normy (TPEG-INV). AID je použit v TPEG2-SNI k indikaci, jakým způsobem má dekodér pracovat s předávaným obsahem.

Dále se věnuje způsobu předání informace o verzi aplikace. Verze je klíčová z pohledu dekodéru, jednotlivé verze stejné aplikace se totiž mohou od sebe lišit strukturou, obsahem, atp. Princip přidělování verzí je stanoven v popisovaném dokumentu.

CAI používá rámec komponent služby TPEG s CRC daty dle specifikace v TPEG2-UXCR.

6 Metodika podmíněného přístupu

Tato kapitola (rozsah 1 strana) uvádí, že podmíněný přístup je stanoven v normách TEPG2-SFW a TPEG2-SNI jako funkce aplikovaná na úrovni rámce služby či komponent služby. Šifrovací metoda je indikovaná pomocí identifikátoru šifrování (EncID) přímo v rámci služby či pro její komponenty prostřednictvím tabulky GST1.

Kapitola dále uvádí, že k dešifrování zašifrovaného obsahu je zapotřebí někde přenášet informace o použitém způsobu šifrování, o tom, co je a co není zašifrováno nezávisle na zašifrovaném obsahu. Ideálním způsobem, jak tyto informace přenášet, je prostřednictvím další komponenty služby s vyhrazeným AID.

Některé komponenty služby mohou být zašifrovány jedním (stejným) klíčem, zatímco jiné komponenty jiným. To umožňuje prodávat „balíčky“ služeb (pro všechny komponenty „balíčku“ je použit stejný šifrovací klíč).

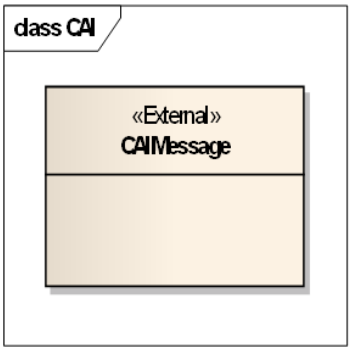
Každá zašifrovaná komponenta služby musí být propojena s relevantní komponentou CAI nesoucí informace o podmíněném přístupu. Toto se řeší prostřednictvím tabulky GST-6 Odkazy CAI.

Dále tato kapitola uvádí příklad, kdy rámec služby obsahuje 9 komponent. Komponentu SNI, dále jednu nezašifrovanou komponentu TEC a 2 zašifrované TEC (stejným klíčem), jednu zašifrovanou a nezašifrovanou komponentu PKI a dále 3 komponenty CAI. První pro indikaci skupiny TEC, druhou pro indikaci komponenty PKI a třetí pro všechny zašifrované komponenty dohromady.

Metodika dále uvádí, že popisovaný dokument stanovuje obálku, do které musí být teprve vložen obsah specifický dle použitého způsobu podmíněného přístupu (dle indikace pomocí EncID).

7 Struktura CAI

Tato kapitola (rozsah 1 obrázek) uvádí strukturu CAI. Na rozdíl od dalších aplikací TPEG nemá aplikace CAI kontejnery pro popis polohy a řízení zprávy, skládá se pouze z jedné generické komponenty, jejíž obsah v dokumentu není stanoven.



Obrázek 1 – Struktura zprávy CAI (obr. 1 normy)

8 Komponenty CAI zprávy

Tato kapitola (rozsah 1 odstavec) popisuje komponenty zprávy CAI.

Uvádí, že zpráva CAI obsahuje pouze jeden kontejner, jehož struktura je definována v jiných dokumentech (normách) pro ten který systém podmíněného přístupu. Systém podmíněného přístupu je určen indikátorem šifrování (EncID) signalizovaným v SNI.

9 Bibliografie

Tato kapitola uvádí dva odkazy, první na předchozí verzi CAI v TPEG1 a druhý na definici XML schématu.

Příloha A (normativní) **TPEG-bin reprezentace CAI**

Tato příloha o rozsahu 1 strany stanovuje binární reprezentaci aplikace informace o podmíněném přístupu (CAI) TPEG pro použití v DAB . Popis binární reprezentace je použit pseudokód, kde pro každé klíčové slovo zapsané struktury je znám jeho binární tvar.

Kapitola stanovuje identifikátor zprávy CAI a strukturu zprávy pomocí instrukce „external“, nestanovuje tedy strukturu obsahu, ale pouze „obálku“.

Příloha B (normativní) **TPEG-ML reprezentace CAI**

Tato příloha o rozsahu 1 strany obsahuje popis XML reprezentace a XML schéma rámce TPEG.

Stanovuje prázdné XML schéma a uvádí, že do tohoto prázdného schématu má být naimportováno externí schéma stanovující konkrétní strukturu kontejneru CAI dle požadavků té které aplikace.