Úvod

V mnoha zemích vyžadují náklady na zavedení a podporu služeb RDS-TMC komerční krytí. V původních normách RDS-TMC se došlo k závěru, že databáze poloh prodávaná v inteligentních kartách nebo na CD-ROM představuje model finančního krytí služby.

Aby nedošlo k vytvoření jiného přístupového systému, byli představitelé evropského průmyslu v oblasti přijímačů požádáni o vytvoření Úkolové skupiny, která by vyvinula jednu metodu šifrování a podmíněného přístupu, jež by byla všeobecně přijatelná. Požadavek se týkal širokého spektra možností, včetně aktivace terminálu v továrně, která by umožnila jejich umístění při výrobě automobilů, a také aktivaci konečným uživatelem na krátké doby.

Úkolová skupina vyvinula systém, který je popsán ve specifikaci TMC Fóra – RDS-TMC s využitím ALERT-C: Šifrování TMC a podmínky přístupu 3.0/002.

Tato specifikace udává tyto podrobnosti:

- způsob, jakým je zpráva RDS-TMC označena při šifrování;
- jaký prvek v rámci zprávy RDS-TMC je šifrován;
- způsob, jaký poskytovatel služby použije ke šifrování zprávy;
- kdy a jak lze změnit parametry šifrování;
- novou skupinu RDS-TMC „kódovací administrativní skupinu“, ve které se přenášejí některé podrobnosti ohledně použití kódovacích algoritmů. Tyto podrobnosti společně s dalšími informacemi, které poskytovatel služby propůjčuje výrobci terminálu, jsou nutnými informacemi pro výrobu terminálu, který je schopen dekódovat zprávy RDS-TMC;
- proces dešifrování;
- dešifrování je přípustné pouze tehdy, pokud byl terminál aktivován pro dešifrování;
- tuto aktivaci lze provést na bázi „na službu“, „na terminál“ a do určitého data;
- navrženou metodu pro aktivaci terminálu, kterou je výrobcem generovaný kód „PIN“;
- podmínky pro uvedení kódovaných zpráv RDS-TMC.

Předmět

Tato specifikace šifrování TMC Fóra a podmínek přístupu (1) poskytuje názorné podrobnosti a příklady, které se týkají kódovacích a dekódovacích procesů a dodatečných prvků, které je nutné přenést v případě, kdy jsou zprávy RDS-TMC kódovány. Tyto aspekty jsou „normativní“ a jsou předmětem této specifikace.

Proces, kterým se aktivuje terminál pro dešifrování zpráv, je specifikum výrobce a volba určité metody bude záviset na hardwaru terminálu, na druhu obchodu a na obchodních smlouvách mezi jednotlivými poskytovateli služeb a výrobci terminálů. Přesně stanovené postupy, kterými se terminály aktivují, se budou měnit, a proto tyto pokyny představují některé přístupy pro aktivaci použitím vstupního kódu „PIN“.

3 Aktivace terminálu pro dešifrování

Uživatel zařízení TMC potřebuje získat práva předtím, než je mu možné kódované služby TMC zpřístupnit. Poskytovatel služby poskytne práva tehdy, až všechny záležitosti spojené se smlouvou jsou vyřízeny. To lze provést individuálně s koncovým uživatelem nebo výhradně pro uzavřenou skupinu uživatelů. Jasnými příklady uzavřené skupiny uživatelů jsou výrobci aut a zařízení TMC. I když jsou práva poskytnuta, bude zařízení dodánu uzamčeno. Podmínkami přístupu se uzamčené zařízení aktivuje.

Předtím, než jakýchkoliv terminál používá dešifrování pro obnovení kódu polohy, musí se pro tuto službu aktivovat. Lze použít mnoho mechanismů, které aktivují určitý terminál, ale způsob popisovaný v tomto dokumentu je aktivace vstupním kódem „PIN“, což je velmi známý postup obecně používaný. Přesná délka a formát kódu „PIN“ je stanovena výrobcem, který se především zaměřuje na Rozhraní Člověk – Stroj.

Kód PIN se generuje výrobcem a je vypočítán tak, aby byl vhodný pro předplacené služby, každá je definována svým „Profilem Přístupu“ výrobním sériovým číslem terminálu a dalšími požadovanými prvky – například „kódem proti krádeži“.

Poněvadž zadání příslušného kódu PIN aktivuje terminál, je výrobce, který definuje strukturu kódu PIN, v mnoha případech odpovědný za generaci kódu PIN.

3.1 Aktivace terminálu pro dešifrování

Vzhledem k možné existenci mnoha odlišných komerčních podmínek lze každý terminál aktivovat nejen jedním kódem PIN, ale několika kódy. Určitý kód PIN stanovuje pro jakou službu a na jak dlouhou dobu je terminál aktivován.

Kombinace specifických parametrů, které se vztahují k určité službě, ji označují jedinečným způsobem a „den vypršení platnosti“ předplacené služby se odkazuje na „Přístupový Profil“.

Přístupové Profily se definují k usnadnění aktivace terminálů. Přístupový Profil je definován v této specifikaci a je nutné ho začlenit ve výrobku, aby byl schopen provádět dešifrování.

Od každého terminálu se očekává, že je schopen uložit 32 Přístupových Profilů, libovolný počet těchto Přístupových Profilů může být v jakoukoli dobu „aktivní“: aktivace se dosáhne vložením příslušného kódu PIN. Každý Přístupový Profil obsahuje 5 prvků: Datum vypršení platnosti, Kód Země, Číslo lokalizační databáze, Identifikátor Služby a Šifrovací Klíč Služby.

3.1.1 Datum vypršení platnosti

Schopnost terminálu dešifrovat zprávy každé služby je stanoven předem poskytovatelem služby, který nastaví „Datum vypršení platnosti“, při kterém musí terminál přestat dále dešifrovat zprávy této služby. „Datum vypršení platnosti“ může být jakékoli datum v budoucnosti, a je zřejmé, že pokud je nastaven do daleké budoucnosti (například 28. února 2100), umožňuje ve své podstatě „doživotní“ aktivaci.

Terminál používá přenášená data RDS CT (**C**lock **T**ime – Místní Čas) (skupiny typu 4A) nebo časový údaj GPS, kdy se Datum vypršení platnosti blíží a kdy již platnost vypršela. Je doporučeno, aby byl koncový uživatel upozorněn jeden měsíc před datem, kdy předplacení určité služby končí, a aby byl směrován k příslušné literatuře nebo webové adrese, kde jsou uvedeny podrobnosti obnovení přístupu.

Obchodní smlouvy mezi poskytovatelem služeb a výrobcem terminálu nebo jejich prostředníkem (například výrobcem vozidel) jsou často uzavřeny pro aktivaci na určitou dobu (například dva roky), než k určitému datu. Dále je často vhodné, že se terminál aktivuje již předem ve výrobě, což může být několik měsíců před eventuelním použitím koncovým uživatelem. Následně je doporučeno, aby Datum vypršení platnosti se vypočítalo, bylo automaticky vloženo do terminálu a bylo spuštěno například přijímáním dat od zašifrované služby po nepřetržitou dobu (například jedné hodiny). Tento způsob umožňuje terminálu, aby byl odzkoušen a krátce uveden do provozu „v době nepodléhající poplatkům“. Doba přeplacení byla zahájena pouze skutečným použitím služby koncovým uživatelem.

Datum vypršení platnosti je jedním z prvků, který tvoří Přístupový Profil služby.

Dalšími parametry identifikujícími službu jsou:

- Kód Země (CC)
- Číslo lokalizační databáze před šifrováním (LTNBE)
- Identifikátor Služby (SID)
- Šifrovací Klíč Služby (SVK)

3.1.2 Kód Země

Kód Země RDS se udává prvními čtyřmi bity kódu PI přenášené v bloku 1 každé skupiny RDS. Existuje tudíž 15 kódů země v rámci Evropské Vysílací Oblasti. Země se stejným kódem země jsou zřetelně geograficky odděleny. Výrobky pro navigaci mohou obsahovat alternativy stanovující země jedinečně, například GPS a digitální mapa. Jakmile je jedinečnost kódu země zaručena, je dovoleno tuto informaci používat.

3.1.3 Číslo lokalizační databáze (před šifrováním)

Silniční síť je jedinečná v každé zemi a tabulka číselných označení vozovek, s jejich názvy, křižovatkami a jinými referenčními body jsou umístěny v Lokalizačních Databázích specifických pro každou zemi. Žádný terminál nemůže vyrobit smysluplnou službu RDS-TMC, dokud nemá přístup k Lokalizační Databázi používanou poskytovatelem služby. Tato databáze je uložena na CD-ROM nebo podobném médiu, které je používáno terminálem. Lokalizační databáze se identifikují Číslem Lokalizační Databáze. Tato čísla jsou uzpůsobena tak, že různá čísla jsou umístěna v každé zemi, která sdílí běžný Kód Země. Z toho vyplývá, že kombinace Kódu Země a Čísla lokalizační databáze jedinečně identifikují Lokalizační databázi. Lokalizační databáze používaná na určitou službu, tedy kódy, které vznikly jejím šifrováním, jsou přenášeny jako LTNBE pomocí Šifrovací Administrativní skupiny.

LTNBE je prvkem, který přispívá k existenci Přístupového Profilu.

3.1.4 Identifikátor Služby

Pro existenci několika odlišných služeb v rámci určité země, všemi, kteří používají stejnou lokalizační databázi, stanovují poskytovatelé služby jeden nebo více Identifikátorů Služby k identifikaci odlišných služeb TMC. Obvykle si koncový uživatel předplatí určitou službu v určité zemi.

Tudíž i Identifikátor Služby přispívá k existenci Přístupového Profilu.

3.1.5 Šifrovací Klíč Služby

Parametry, které se používají k šifrování prvků lokace ve zprávách TMC jsou obsaženy v 8 šifrovacích tabulkách, každá obsahuje 32 řádků údajů. Poskytovatel služby přenáší číslo Identifikátoru Šifrování, který označuje, jaký řádek v šifrovací tabulce se používá v určitý den, ale nepřenáší informaci, jaká tabulka byla zvolena pro použití. Tabulka, kterou z 8 dostupných zvolil poskytovatel služby, se odkazuje jako Šifrovací Klíč Služby ve smlouvě mezi poskytovatelem služby a výrobcem terminálu a je informací, která je mezi těmito obchodními stranami přenášena.

Šifrovací Klíč Služby také přispívá k existenci Přístupového Profilu.

3.2 Výrobní sériové číslo terminálu

Aktivace terminálu, která umožňuje dešifrování a používání šifrované služby, je záměrně řízena na základě jednotlivého terminálu, který znemožňuje neautorizovanou aktivaci více terminálů. Tudíž kód PIN požadovaný k aktivaci terminálu musí být jeho specifikem. Z důvodu, že poskytnutí řady jedinečných kódů PIN každému jednotlivému terminálu může vyžadovat nepřijatelně dlouhý kód, který by koncový uživatel musel vložit do terminálu, může být stejný kód PIN sdílen větším počtem terminálů. Nicméně by měl výrobce terminálu vytvořit co nejvíce odlišných kódů PIN, které by splňovaly požadavky koncového uživatele pro jeho snadné zadání. Odlišné kódy PIN se musí distribuovat do terminálů nahodile.

Výrobní sériové číslo terminálu se vyžaduje jako jeden z prvků, které se používají k vygenerování příslušného kódu PIN, jenž je vyžadován pro aktivaci terminálu.

3.3 Kód proti krádeži a jiné prvky

Mnoho výrobců terminálů zavedením „bezpečnostního kódu“, který je nutné vložit pokaždé, kdy se audio příslušenství vozidla znovu připojí do elektrické sítě, zabránilo velkému množství krádeží.

TMC není pouze aplikací vyžadující Podmínky Přístupu. Telematické služby, vysílací služby a přístupnost k jejich obsahu mohou vyžadovat podobná řešení. Tato norma dovoluje výrobcům terminálů používat více vzájemně propojených aplikací, jakmile řešení podporuje základní požadavky normy.

K zajištění možnosti zadání více kódů je navrhováno, že pokud se požaduje Kód proti krádeži nebo přístupový kód pro jakoukoliv službu, je toto zahrnuto při generování kódu PIN, který aktivuje terminál pro dešifrování TMC.

4 Začlenění zařízení

Kód PIN vyžadovaný k aktivaci terminálu může být zadán osobně koncovým uživatelem nebo může být předem zadán výrobcem terminálu během procesu výroby. Druhý případ může být vhodný pro kolektivní smlouvy.

Kód PIN se používá pro dva účely:

- aktivaci terminálu
- aktivaci práv k roamingu

Existuje několik způsobů, jak nakládat s kódy PIN. Tato kapitola popisuje následující tři typy kódů PIN:

1. Kódy PIN pro přístup k jedné službě (závazné)
2. Kódy PIN pro přístup k více službám (nepovinné)
3. Inteligentní kódy PIN (nepovinné)

4.1 Kódy PIN pro vstup k jedné službě

Kódy PIN pro vstup k jedné službě jsou závazné pro terminály a umožňují aktivaci jedné služby v úplně novém terminálu nebo přidání nové služby (roaming).

Kód PIN musí být generován tímto algoritmickým výrazem:

Výrobní sériové číslo terminálu + Přístupový Profil (+privátní částí výrobce)

Základními prvky jsou Výrobní sériové číslo terminálu a Přístupový Profil, které jsou poskytnuty poskytovatelem služby. Výrobce může přidat vlastní data kódu PIN.

4.2 Kódy PIN pro přístup k více službám

Více služeb může generovat dlouhé formáty kódu PIN nebo vyvolat nevoli koncového uživatele, pokud se používají všechny závazné prvky.

Tato možnost dovoluje snížení duplicity dat (například opakování Výrobní sériové číslo terminálu a Data vypršení platnosti). Toto optimalizované řešení lze použít pro přidání přístupových práv k roamingu k různým službám.

Příklad algoritmického výrazu kódu PIN:

Výrobní sériové číslo terminálu + Seznam Přístupových Profilů bez Data vypršení platnosti + Datum vypršení platnosti (+privátní část výrobce)

4.3 Inteligentní kódy PIN

Inteligentní kódy PIN mají smysl, pokud lze použít vzájemnou provázanost různých aplikací, které sníží velikost kódu PIN a umožní snadnější přístup koncového uživatele při rozhraní Člověk-stroj. Existuje mnoho řešení. Inteligentní kódy PIN jsou objasněny následující situací:

1. výrobce vozidel získal „doživotní“ přístupová práva pro své zákazníky na tyto komerční služby TMC:

- SP1 (SVK=3) v Německu
- SP2 (SVK=5) ve Francii
- SP3 (SVK=7) ve Spojeném Království
- SP4 (SVK=2) v Nizozemí
- SP5 (SVK=1) ve Španělsku
- SP6 (SVK=6) v Itálii

Tento Profil Zákazníka se označí: C-Id$_1$

2. uživatel získal právo k používání těchto služeb na jeden rok, včetně digitální mapy:
    - Francie, Nizozemí a Španělska.
3. práva výrobce vozidel jsou známa v okamžiku, kdy je vyroben navigační terminál.

Práva TMC jsou kolektivní, s doživotním použitím a lze je předem uložit v navigační jednotce.

Práva na mapu jsou individuální a časově omezené datumem vypršení platnosti a je nutné je zadat koncovým uživatelem.

V podstatě má koncový uživatel právo použít všech šest služeb TMC. V praxi je funkčnost TMC zakázána pro služby SP2, SP4 a SP5, protože přístupová práva jsou určena pouze pro tři digitální mapy.

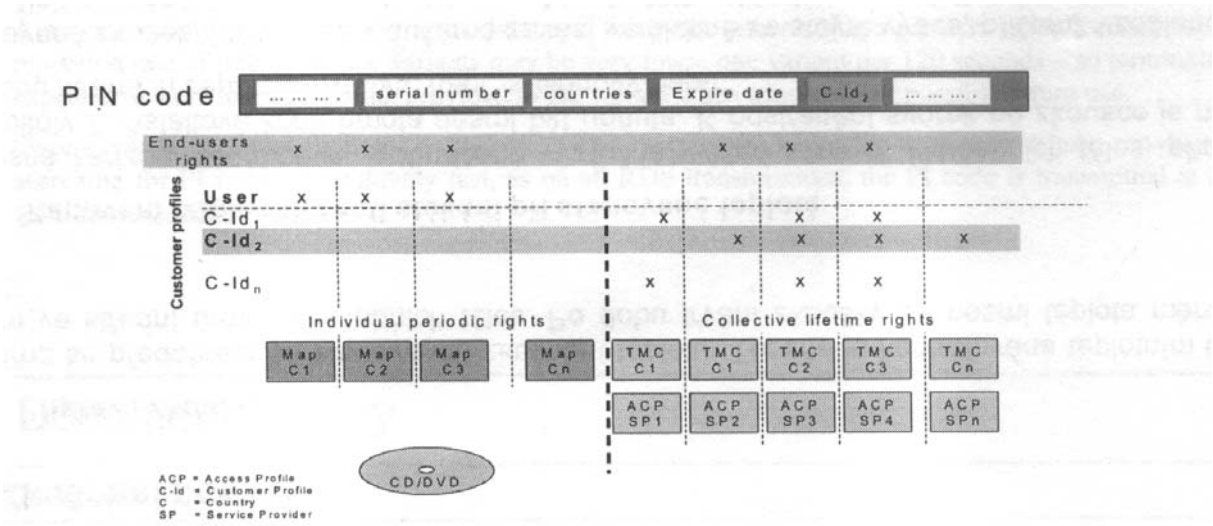
Pokud jsou práva TMC (Přístupové Profily) uloženy již během výroby terminálu, stačí se v kódu PIN odkázat na C-Id$_1$, neboť terminál může obsahovat rozličné profily zákazníka (C-Id$_n$), viz následující příklad:

Obsah kódu PIN spojeného s TMC je snížen v tomto případě na jeden C-Id.

Výhodou tohoto řešení je, že přístupová práva k jiným mapám se získají okamžitě s tím, kdy se funkčnost TMC rozšíří do dalších zemí.

Nová práva roamingu lze po jejich utvoření přidat k C-Id použitím závazného kódu PIN pro vstup k jedné službě.

Obrázek uvedený níže zobrazuje způsob, jak lze jeden Zákaznický profil předem uložit do stejného terminálu.



Zákaznický Profil C-Id$_2$ společně s osobními právy uživatele definují přístupová práva koncového uživatele. V tomto příkladě: práva na mapu pro země 1, 2 a 3 a přístup TMC ke službě poskytovatele služeb 2 (SP2) v zemi 1, SP3 v zemi 2 a SP4 v zemi 3.

5 Služební partnerství

Díky možnosti koncového uživatele cestovat přes národní nebo jiné hranice a bez přestání přijímat služby RDS-TMC se očekává, že poskytovatelé služeb v různých oblastech mohou tvořit „aliance“ nebo „Služební partnerství", které budou poskytovat služby k vzájemnému užitku svých předplatitelů.

5.1 Aktivace

K obdržení přístupu ke službě v jiné oblasti je nezbytné, aby byl terminál aktivován také pro Přístupový Profil služebních partnerů, tak jako je pro „domácího“ poskytovatele služeb.

Předpokládá se, že poskytovatelé služeb nabídnou zákazníkovi podporu, která jejich zákazníkům sdělí, jakým způsobem lze službu rozšířit, aby umožňovala dešifrování zpráv RDS-TMC v případě cestování do zahraničí. Při předem provedené aktivaci, jak je popsáno výše v 2.3, bude nutné, aby zákazník zadal nový kód PIN, který aktivuje Přístupové Profily v rámci svého terminálu – předpokládá se, že poskytovatel služby bude schopen nabídnout konečnému uživateli pomoc získat požadovaný kód PIN tak, že jej poskytne nebo sdělí.

5.2 Přenos

Pro podporu terminálu k nalezení služby TMC provozované služebním partnerem jsou poskytovatelé služeb vybídnuti k přenesení služby Ladění varianty 9, která udává tyto podrobnosti:

- Geografický předmět zprávy (MGS)
- Identifikátor služby (SID) a
- Číslo lokalizační databáze (LTN) pro jinou službu, odkazovanou kódem Identifikace Programu (PI).

Je pozoruhodné, že v kontextu šifrované služby musí být odkazovaná hodnota LTN Číslem lokalizační databáze před šifrováním (LTNBE) služebního partnera (tj. NE „0“).

Poskytovatel služby se může odkazovat na maximálně 31 jiných služebních partnerů použitím varianty 9. Míra opakování variant služby Ladění může být velmi pomalá – jedna varianta za 120 vteřin – takže se předpokládá, že terminály uloží poskytovanou informaci ve variantě v okamžiku jejího obdržení, pro možné pozdější použití.

Když je varianta uložena v paměti, je hledání služebního partnera RDS-TMC služeb, pro které byl terminál aktivován, pomocí vyhledávání kódů PI, relativně rychlé, jako u všech přenosů RDS je kód PI přenášen rychlostí nejméně 11,4krát za vteřinu.

Historie dokumentu

Historie dokumentu		
Verze	Datum	Milník
1.0	12.3. 2001	první návrh (nevydaný) – většina jeho obsahu byla převedena do nové specifikace
2.0	21.5. 2001	Nový Návrh včetně začlenění kódu PIN výrobce
	17.7. 2002	změny: přidání odkazů, zkratek, a vypuštění mnoha duplicitních informací