ISO/TS 21719-2 - **Elektronický výběr poplatků (EFC) – Personalizace palubního zařízení (OBE) – Část 2: Užití vyhrazené komunikace krátkého dosahu**

Aplikační oblast: Elektronický výběr poplatků (EFC)

Rok vydání normy a počet stran: Vydána 2019, 39 stran

Rok zpracování extraktu: 2020

Skupina témat: Interoperabilita

Téma normy: Rozhraní komunikační služby

Charakteristika tématu: Definice transakce mezi OBU a RSE za účelem personalizace palubní jednotky.

Úvod, vysvětlení východisek
Seznam podkladových norem.
Popis architektury, hierarchie, rolí a vztahů objektů
Definice protokolového zásobníku.
Popis procesu / funkce / způsobu použití
Specifikace transakčních primitiv a jejich sekvenčního řazení. Definice použitého protokolového zásobníku.
Popis rozhraní / API / struktury systému
Požadavky na nižší služby. Jména API funkcí a parametry. Definice transakčních primitiv, jejich sekvenčního řazení .
Definice protokolu / algoritmu / výpočtu
Definice výpočtů v rámci autentikačních protokolů.
Definice reprezentace dat / fyzikálního významu
Reprezentace datových struktur v ASN.1.
Definice konstant / rozsahů / omezení

Úvod

Tato technická norma (dále rovněž “popisovaný dokument”) se zabývá definicí aplikačního profilu využívajícího personalizační funkce popsané technickou normou ISO/TS 21719-1. Jsou zde rovněž definovány požadavky na palubní zařízení a personalizační zařízení, a to z pohledu podporovaných DSRC technologií, personalizačních funkcí a bezpečnostní funkcionality.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Užití

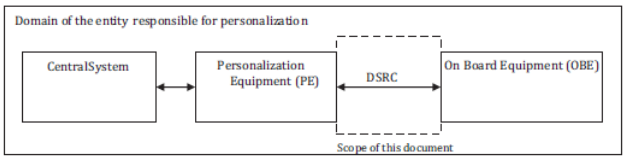
Popisovaný dokument definuje aplikační profil pro personalizaci palubního zařízení využitím vyhrazené komunikace krátkého dosahu (DSRC). Dokument je tak určen zejména výrobcům palubního zařízení a personalizačního zařízení, provozovatelům mýtného systému nebo poskytovatelům mýtných služeb.

1. Předmět normy

Popisovaný dokument specifikuje:

- rozhraní pro personalizaci využívající komunikační službu definovanou dle ISO 14906,
- fyzický systém – palubní zařízení a personalizační zařízení,
- požadavky na DSRC spojení,
- personalizační funkce EFC podle ISO/TS 21719-1,
- bezpečnostní datové prvky a mechanismy používané v DSRC rozhraní.

Předmětem popisovaného dokumentu je DSRC rozhraní mezi personalizačním zařízením (PE) a palubním zařízením (OBE), viz Obrázek 1. Dokument nedefinuje postup posouzení shody, nespecifikuje testy, neustanovuje organizační role ani neřeší právní otázky.



Obrázek 1 – Oblast předmětu technické normy, vyznačeno čárkovaně (obr. 1 normy)

2. Souvisící normy

Popisovaný dokument se odkazuje na následující technické normy:

ISO/IEC 9797-1, Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MAC) — Část 1: Mechanismy používající blokovou šifru

ISO/IEC 10116, Informační technologie – Bezpečnostní techniky – Módy činnosti pro algoritmus n-bitové blokové šifry

ISO 14906, Elektronický výběr mýtného – Stanovení aplikačního rozhraní pro vyhrazenou komunikaci krátkého dosahu

ISO 15628, Inteligentní dopravní systémy — Vyhrazené spojení krátkého dosahu (DSRC) – Aplikační vrstva

ISO/IEC 18033-3, Informační technologie – Bezpečnostní techniky – Kódovací algoritmy — Část 3: Bloková šifra

EN 12834, Dopravní telematika – Vyhrazené spojení krátkého dosahu (DSRC) – Aplikační vrstva

EN 15509, Elektronický výběr poplatků – Aplikační profil interoperability pro DSRC

3. Termíny a definice

Tato kapitola obsahuje 20 termínů a definic souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou následující:
přístupové klíče (access credentials) – důvěryhodné ověření požadované identity objektu nebo aplikace
autentizace (authentication) – schválený proces ověřování bezpečnostních pověření
palubní zařízení (on-board equipment) – zařízení instalované ve vozidle podporující výměnu informací se zařízením na infrastruktuře
personalizace palubního zařízení (OBE personalization) – proces přenosu personalizačních údajů do palubního zařízení
personalizační údaje (personalization assets) – specifická data uložená v palubním zařízení identifikující uživatele a vozidlo
personalizační zařízení (personalization equipment) – zařízení pro přenos personalizačních údajů do palubního zařízení

transakce (transaction) – kompletní výměna informací mezi dvěma fyzicky oddělenými komunikačními zařízeními

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology.

4. Symboly a zkratky

Tato kapitola obsahuje 27 zkratek souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou následující:

DSRC vyhrazená komunikace krátkého dosahu (dedicated short-range communications)

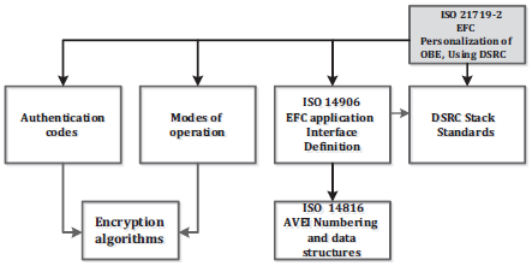
OBE palubní zařízení (on-board equipment)

PE personalizační zařízení (personalization equipment)

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

5 Shoda

Tato kapitola v rozsahu 1 stránky obecně uvádí do kontextu vztah mezi základními technickými normami a aplikačním profilem, který je definovaný v popisovaném dokumentu, viz Obrázek 2. Tato kapitola dále informuje o rozdělení požadavků do dvou oblastí, a to na palubní zařízení a personalizační zařízení.



Obrázek 2 – Vztah mezi základními technickými normami a ISO/TS 21719-2 (obr. 3 normy)

6 Základní informace o personalizaci

Tato kapitola v rozsahu 1 stránky s odkazem na technickou normu ISO/TS 21719-1 uvádí personalizační proces a systémovou architekturu.

7 Požadavky na OBE

Tato kapitola v rozsahu 5 stránek popisuje normativní požadavky na ověření shody palubního zařízení s profilem definovaným popisovaným dokumentem.

Nejdříve jsou v této kapitole shrnuty DSRC technologie podporované popisovaným dokumentem.

DSRC stack	Application layer	Lower layers	Detailed specifications
CEN-DSRC	ISO 15628 EN 12834	EN 12795 EN 12253	Specification in 7.2.2
Italian DSRC	ETSI/ES 200 674–1 (Clause 11 and Annex C)	ETSI/ES 200 674–1 (Clauses 7 to 10 and Annex C)	Specification and implementation example in Annex C
Japanese DSRC	ARIB STD-T75	ARIB STD-T75	
Wave DSRC	IEEE1609.11	IEEE802.11p IEEE1609.3/4	

Tabulka 1 – Podporované DSRC technologie (tab. 1 normy)

Dále jsou v této kapitole popsány požadavky na personalizační funkce, které má palubní zařízení podporovat, konkrétně:

- inicializace komunikace, tj. vytvoření komunikačního spojení s palubním zařízením,
- přenos identifikátorů palubního zařízení,
- zápis dat, tj. aktualizaci údajů v palubním zařízení s využitím funkce SET_SECURE definované technickou normou ISO 14906.

Na závěr této kapitoly jsou popsány požadavky na bezpečnostní funkcionalitu a personalizační transakci.

8 Požadavky na personalizační zařízení

Tato kapitola v rozsahu 2 stránek popisuje normativní požadavky na ověření shody personalizačního zařízení s profilem definovaným popisovaným dokumentem. Podporovány jsou stejné DRSC technologie jako v případě palubního zařízení.

Dále jsou v této kapitole popsány požadavky na bezpečnostní funkcionalitu a personalizační transakci.

Příloha A (normativní) – Bezpečnostní výpočty

Příloha A v rozsahu 5 stran definuje požadavky na výpočty bezpečnostních klíčů na straně palubního zařízení a personalizačního zařízení, konkrétně je zde popsán:

- výpočet přístupového klíče (AC_CR) z odvozeného personalizačního klíče MPAck(k) a náhodného čísla RndOBE, kdy výpočet je založen na využití kódovacího algoritmu blokové šifry, padding metody 4, pro autentizaci zpráv a kódovacího algoritmu AES128 blokové šifry,
- výpočet odvozeného personalizačního klíče PAcK(k) z hlavního personalizačního klíče MPAck(k) a referenčního přístupového klíče (AC_CRKeyReference), kdy výpočet je založen na využití kódovacího algoritmu AES256 blokové šifry,
- výpočet klíče pro kódování atributů z náhodného čísla RndOBE a referenčního klíče (KeyRefEnc), kdy výpočet je založen na využití kódovacího algoritmu blokové šifry, padding metody 2, pro autentizaci zpráv a kódovacího algoritmu AES128 blokové šifry,
- výpočet referenčního autentizačního klíče KeyRefAuthReq, KeyRefAuthRes z náhodného čísla RndOBE, kdy výpočet je založen na využití kódovacího algoritmu blokové šifry, padding metody 4, pro autentizaci zpráv a kódovacího algoritmu AES128 blokové šifry,
- výpočet odvozeného autentizačního klíče AuthK(k) z hlavního autentizačního klíče MAuth(k) a unikátního identifikátoru palubního zařízení, kdy výpočet je založen na využití kódovacího algoritmu AES256 blokové šifry.

Příloha B (normativní) – PICS

Příloha B v rozsahu 5 stran obsahuje formulář PICS za účelem posouzení shody dané implementace s požadavky uvedenými v popisovaném dokumentu.

Příloha C (normativní) – Personalizace OBE ve shodě s ES 200 674-1

Příloha C v rozsahu 5 stran popisuje personalizační proces pro palubní zařízení, které je ve shodě s technickou normou ETSI ES 200 674-1. Jsou zde rozebrány personalizační funkce, jejich zprávy protokolu a souslednost jednotlivých kroků, konkrétně:

- funkce inicializace (Initialization) používána pro vytvoření komunikačního spojení s palubním zařízením,
- funkce zápisu dat (Writing of data) používána pro aktualizaci údajů v palubním zařízení,
- funkce zápisu klíčů (Writing of keys) používána pro modifikaci přístupových, autentizačních a personalizačních klíčů,
- funkce ukončení (Termination) realizována prostřednictvím protokolárních zprávy.

Tato příloha dále definuje protokolární zprávy a jejich parametry:

- ConfigSet-Rq určenou pro zápis parametrů do paměti palubního zařízení v rámci funkce zápisu dat,
- ConfigKey-Set-Rq určenou pro zápis klíčů do paměti palubního zařízení v rámci funkce zápisu klíčů,
- ConfigSet-Rs určenou pro odpověď na výše zmíněné zprávy.

Příloha D (informativní) – Příklad transakce

Příloha D v rozsahu 5 stran uvádí příklad personalizační transakce, tj. přenosu personalizačních údajů mezi palubním zařízením a personalizačním zařízením. Příklad je uveden pro personalizační funkci zápisu dat. Na úrovni jednotlivých oktetů a bitů je zde detailněji popsána funkce SET_SECURE.

Příloha E (informativní) – Příklad bezpečnostních výpočtů

Příloha E v rozsahu 4 stran uvádí příklad bezpečnostních výpočtů, které jsou definovány v příloze A. Je zde uveden příklad pro výpočet přístupového klíče, výpočet odvozeného personalizačního klíče, výpočet klíče pro kódování atributů, výpočet autentizačního klíče a výpočet odvozeného autentizačního klíče.