EXTRAKT z technické specifikace

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

Elektronický výběr poplatků (EFC) – Personalizace palubního zařízení (OBE) – Část 2: Použití vyhrazeného spojení krátkého dosahu

CEN/TS 21719-2

01 8369

Vydána 2018, 41 stran

Úvod

Technická specifikace CEN/TS 21719-2 (dále jen "popisovaný dokument") se zaměřuje na definici aplikačního profilu pro funkci personalizace palubního zařízení za užití DSRC coby komunikační vrstvy (jedná se tedy o funkci personalizace prostřednictvím DSRC) a definici rozhraní pro aplikační vrstvu na základě definice aplikačního rozhraní z ISO 14906.

Poznámka: Extrakt přejímá původní číslování kapitol.

Užití

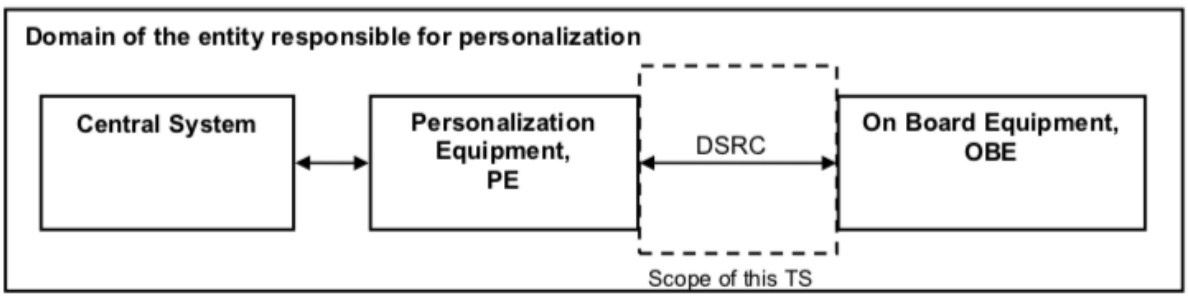
Cílem popisovaného dokumentu je definice jednotného procesu komunikace v rámci personalizačního procesu OBE za účelem uložení dat v OBE. Tyto data jsou potřebná pro výpočet mýtného a souvisí s uživatelem a vozidlem, v němž je daná OBE nainstalována (proto je termín „personalizace" vhodnější než „konfigurace", jež může zahrnovat i data, která s vozidlem či uživatelem nesouvisí). Tato specifikace je určena zejména **výrobcům palubního zařízení**. Normalizace procesu personalizace umožňuje zápis a čtení dat v rámci spektra různých poskytovatelů služeb (nikoliv pouze jednoho).

1 Předmět normy

Popisovaný dokument tvoří druhou část normy 21719, přičemž první část se týká rámcových definic procesu personalizace. Předmětem této části je detailní definice komunikačních a datových prvků v rámci personalizačního procesu. Jedná se zejména o následující:

- Popis personalizačního rozhraní (DSRC)
- Požadavky pro zařízení zúčastněná v procesu (OBE a zařízení pro personalizaci)
- Požadavky týkající se nižších vrstev DSRC
- Požadavky týkající se zabezpečení během procesu personalizace

Následující obrázek prezentuje rozsah této popisovaného dokumentu.



Obrázek 1 – Rozsah technické specifikace (obrázek 1 normy)

2 Souvisící normy (výběr)

Norma uvádí 6 norem, mimo jiné následující souvisící normy:

ČSN EN ISO 14906:2011/Amd1:2015, Elektronický výběr mýtného (EFC) - Stanovení aplikačního rozhraní pro vyhrazené spojení krátkého dosahu

ČSN EN 15509:2014, Elektronický výběr poplatků (EFC) - Aplikační profil interoperability pro DSRC
ETS ES 200 674-1

3 Termíny a definice

V této normě je uvedeno 20 termínů. Mezi ty nejpodstatnější lze zařadit následující:

integrita data *(data integrity)* – vlastnost dat zaručující, že data nebyla poškozena nebo změněna neautorizovaným způsobem

personalizace OBE (*OBE personalization*) – přenos personalizačních (nebo také konfiguračních) datových entit do palubního zařízení (OBE)

personalizační datová entita (*personalization asset*) – specifická data (datový atribut či element) uložená v OBE, jež se vztahují k uživateli a vozidlu

zařízení pro personalizaci (*personalisation equipment*) – zařízení určené pro přenos personalizačních (konfiguračních) datových entit do OBE

4 Symboly a zkratky

V této kapitole je uvedeno 27 symbolů a zkratek, z nichž nejdůležitější jsou následující:

BST tabulka služeb vysílače *(Beacon Service Table)*

EID identifikátor prvku *(Element Identifier)*

MAC řízení přístupu k médiu *(Media Access Control)*

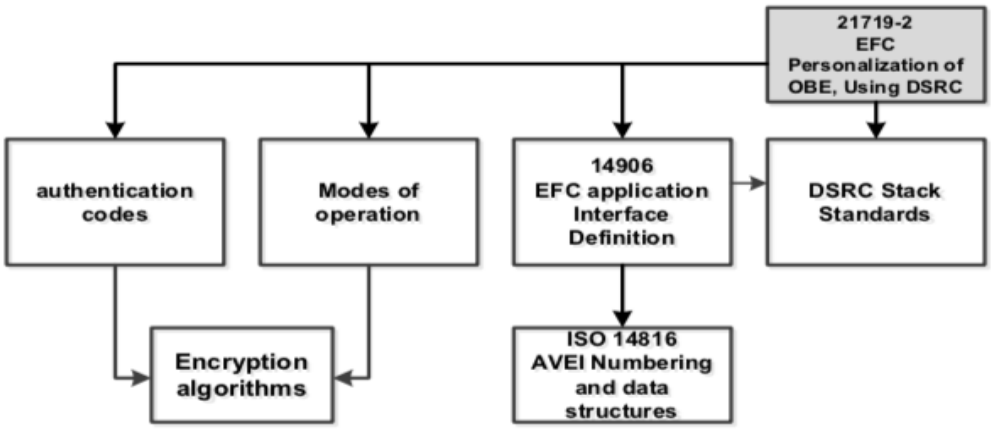
PE zařízení pro personalizaci *(Personalisation Equipment)*

VST tabulka služeb vozidla *(Vehicle Service Table)*

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

5 Shoda

Tato kapitola popisuje význam shody s profilem definovaným v rámci popisovaného dokumentu. Odkazuje se na základní normy, jež jsou v rámci procesu personalizace použity. Jedná se zejména o normy zabývající se zabezpečením, definicí aplikačního rozhraní a komunikačním modelem DSRC (viz Obrázek č. 2).



Obrázek č. 2 – Základní normy a jejich vzájemné závislosti v rámci personalizace OBU (obrázek 3 normy)

Požadavky definované v rámci popisovaného dokumentu jsou rozlišeny na požadavky pro palubní zařízení a zařízení pro personalizaci.

6 Přehled procesu personalizace

Tato kapitola obsahuje odkazy na normy definující základní důležité aspekty související s procesem personalizace, např. popis procesu personalizace či celkovou systémovou architekturu (oboje definované v rámci ISO 21719-1:2017).

7 Požadavky pro OBE

Tato kapitola obsahuje definici normativních požadavků pro palubní zařízení OBE. Tyto požadavky se týkají zejména následujících oblastí:

- Nižší komunikační vrstvy DSRC – jedná se o seznam norem, jimž musí nižší komunikační vrstvy OBE vyhovovat.
- Personalizační funkce OBE – jedná se o popis funkcí, jež musí OBE podporovat za účelem procesu personalizace (např. inicializaci komunikace, přenos identifikátorů z OBE do zařízení pro personalizaci, zápis dat a ukončení komunikace). Norma definuje jednotlivé příkazy a jejich použití (viz příklad níže – příkaz pro zabezpečený zápis dat do OBE).

Tabulka 1 – Popis příkazu SET_SECURE.request (tabulka 2 normy)

parameter name	ASN.1 type	Value	Remark / Constraints
Element Identifier EID	Dsrc-EID	1-127	
ActionType	INTEGER(0..127,...)	3	
AccessCredentials	OCTET STRING		**PRESENT, Length = 8 octets**
ActionParameter	OCTET STRING		**Content; See Table 3**
Mode	BOOLEAN	**TRUE**	**Confirmed mode**

- Požadavky týkající se zabezpečení – jedná se o definice šifrovacích algoritmů, výpočtů přístupových kódů apod.
- Požadavky týkající se mechanismu komunikace – tj. transakce – při procesu personalizace.

8 Požadavky na zařízení pro personalizaci

Tato kapitola obsahuje definici požadavků na zařízení pro personalizaci. Jedná se o následující okruhy požadavků:

- Nižší komunikační vrstvy DSRC - shoda s odpovídajícími normami
- Personalizační funkce zařízení - podpora palubních jednotek splňující požadavky uvedené v kapitole 7
- Bezpečnostní požadavky - např. podpora bezpečnostních datových elementů

Tabulka 2 – Datové elementy týkající se bezpečnosti (tabulka 7 normy)

Name	Length (in octets)	Remarks
PersonalizationAccessKey	**16**	AccessKey used for computation of AccessCredentials that allows for writing attributes received in the AttributeList into the EFC application.
AccessCredentials	**8**	AccessCredentials that allows for writing attributes received in the AttributeList into the EFC application
AC_CR-KeyReference	**2**	Reference to the key generation and the diversifier for the computation of PersonalizationAccessKey
RndOBE	**8**	Random number received from the OBE in the initialization phase of the personalization transaction and used for computation of access credentials. If RndOBE received from the OBE is 4 octets, it shall be padded to eight octets. By using the Padding method 2 according to ISO/IEC 9797-1.
RndOBE2	**8**	Random number generated by the OBE and used in the calculation of the Authenticator_Response.
EncryptionKey	**16**	Encryption Key used to encrypt/decrypt the AttributeList.
KeyRefEnc	**1**	Reference to EncryptionKey used to encrypt the AttributeList The reference corresponds to the Attribute ID where the key is stored.
RndPE	**16**	Random number, from PE used as Start Vector for encryption of the AttributeList and for the computation of the Authenticator_Response.
AuthenticationReqKey	**16**	AuthenticationKey used for the computation of Authenticator_Request calculated over the ApplicationList (or AttributeListEncrypted) that shall be written.
AuthenticationResKey	**16**	AuthenticationKey used for the computation of Authenticator_Response calculated by the OBE over the ApplicationList when it has been written.
Authenticator_Request	**8**	Authenticator calculated over the ApplicationList (or AttributeListEncrypted) that shall be written.
Authenticator_Response	**8**	Authenticator calculated by the OBE over the ApplicationList when it has been written.
KeyRefAuthReq	**1**	Reference to AuthenticationKey used for the computation of Authenticator_Request calculated over the ApplicationList (or AttributeListEncrypted) that shall be written. The reference corresponds to the Attribute ID where the key is stored.
KeyRefAuthRes	**1**	Reference to AuthenticationKey used for the computation of Authenticator_Response calculated by the OBE over the ApplicationList when it has been written. The reference corresponds to the Attribute ID where the key is stored.

- Transakční požadavky -

Příloha A (normativní) **– Výpočty související se zabezpečením**

Příloha A obsahuje detailní popis požadovaných bezpečnostních prvků a výpočtů. Jedná se zejména a popis přístupových kódů (tzv. access credentials) a jejich výpočet, výpočet přístupových zabezpečovacích klíčů (tzv. access keys) či popis postupu pro kódování a dekódování jednotlivých datových atributů.

Příloha B (normativní) **– PICS proforma**

Příloha B obsahuje PICS šablonu pro danou implementaci za účelem kontroly shody s požadavky uvedenými v popisovaném dokumentu.

Příloha C (normativní) **– Personalizace OBE vyhovující ETSI ES 200 674-1**

Příloha C obsahuje popis procesu personalizace pro OBE vyhovující ETSI normě ETS ES 200 674-1 (jedná se zejména o vnitřní paměťové struktury a datové atributy jež musí být v souladu s normou). Proces personalizace

obsahuje popis následujících jednotlivých funkcí, jež jsou v procesu personalizace použity (v rámci inicializace, zápisu, čtení a ukončení komunikace).

Příloha D (informativní) – **Příklad transakce**

Příloha D obsahuje příklad personalizační transakce mezi zařízením pro personalizaci a OBE. Jedná se o transakci obsahující následující příkazové volání:

- GET – pro čtení dat z OBE
- SET_SECURE – pro zápis dat do OBE

Detailnější popis obsahuje následující tabulka.

Tabulka 2 – Přehled DSRC transakce (tabulka D.1 normy)

Personalization Equipment		On-board Equipment	Remarks
INITIALISATION.request (BST) AID=EFC	→		The PE is asking for information of EFC applications in not yet connected OBEs.
	←	INITIALISATION.response (VST) Application list of EFC applications EFC context mark AC_CR key reference RndOBE	The OBE sends an application list to the PE with information over available EFC applications and also security related information in order for the PE to calculate the access credentials.
GET.request AttributeIdList AC_CR	→		The PE calculates access credentials and submits a GET.request in order to retrieve information about the OBE identity.
	←	GET.response Attribute list Equipment OBU ID	The OBE answers with a GET.response that contains the requested Equipment OBU ID.
SET_SECURE.request AC_CR Attribute list encrypted Key ref enc RndPE Authenticator request Key ref auth req Key ref auth res	→		The PE can now use the Equipment OBU ID and knowledge about the master keys to calculate what keys are stored in this specific OBE. With these derived keys the attribute list can be encrypted and authenticated. The RndPE that was used in these calculations is also sent to the OBE together with references to what exact keys that were used. The PE also sends a key reference to the authenticator to be submitted by the OBE in the response
	←	SET_SECURE.response Authenticator response	When the OBE has decrypted the attribute list and checked the authenticator in the request, the attributes in the list is stored in the OBE. The OBE calculates an authenticator over the attributes and returns it to the PE.
EVENT_REPORT.request (RELEASE)	→		The PE terminates the session and the OBE disconnects.

Příloha E (informativní) – **Příklad výpočtu souvisejícího se zabezpečením**

Příloha E prezentuje příklad výpočtu přístupových kódů souvisejících s ověřením práva čtení či zápisu v rámci zařízení pro personalizaci nebo výpočet pro kódování/dekódování jednotlivých datových atributů.