

ISO TS 21719-3 - Elektronický výběr poplatků (EFC) - Personalizace palubního zařízení (OBE) - Část 3: Použití karet s integrovanými obvody

Aplikační oblast: [Elektronický výběr poplatků \(EFC\)](#)

Rok vydání normy a počet stran: Vydána 2023, 24 stran

Rok zpracování extraktu: 2025

Téma normy: Perzonalizace palubního zařízení

Charakteristika tématu: Definice aplikačního profilu pro perzonalizaci palubního zařízení pomocí karet s integrovanými obvody.

Úvod, vysvětlení východisek
Popis architektury, hierarchie, rolí a vztahů objektů
Popis procesu / funkce / způsobu použití
Popis procesu perzonalizace.
Popis rozhraní / API / struktury systému
Definice protokolu / algoritmu / výpočtu
Definice reprezentace dat / fyzikálního významu
Definice konstant / rozsahů / omezení

Úvod

Tato technická norma (dále rovněž “popisovaný dokument”) je součástí souboru norem ISO/TS 21719, které se zabývají personalizací palubních zařízení (OBE) v systémech elektronického výběru mýtného (EFC). Tato skupina norem stanovuje rámec, architekturu a technické požadavky na proces přizpůsobení palubních jednotek (OBE) konkrétnímu uživateli nebo vozidlu, včetně přenosu personalizačních dat a bezpečnostních prvků.

Tento popisovaný dokument se konkrétně zabývá personalizací palubních zařízení (OBE) pomocí karet s integrovanými obvody (ICC). Definuje aplikační profil, který určuje, jak má probíhat přenos personalizačních dat mezi personalizačním zařízením (PE), palubním zařízením (OBE) a kartou ICC. Popisuje rozhraní používaná při personalizaci, role jednotlivých fyzických komponent a stanovuje požadavky na podobu dat, jejich strukturu i základní bezpečnostní mechanismy.

Hlavním cílem popisovaného dokumentu je zajistit kompatibilitu a jednotný postup personalizace napříč výrobci a provozovateli mýtných systémů.

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

Užití

Popisovaný dokument definuje aplikační profil pro personalizaci palubního zařízení (OBE) využitím karet s integračními moduly (ICC). Dokument je tak určen zejména výrobcům palubního zařízení (OBE), výrobcům personalizačního zařízení (PE), provozovatelům mýtného systému nebo poskytovatelům mýtných služeb.

1. Předmět normy

Popisovaný dokument stanovuje:

- rozhraní pro personalizaci,
- fyzický systém – palubní zařízení (OBE), personalizační zařízení (PE), kartu s integrovanými obvody (ICC),
- personalizační funkce EFC podle ISO/TS 21719-1,
- bezpečnostní datové prvky a mechanismy.

Do rozsahu popisovaného dokumentu naopak nepatří zkušební a certifikační postupy, právní rámec ani detailní specifikace příkazů či bezpečnostních algoritmů uvedených v ISO/IEC 7816-4.

2. Související normy

Popisovaný dokument se odkazuje na následující technické normy:

ISO/IEC 7816-3 – Identifikační karty – Karty s integrovanými obvody – Část 3: Karty s kontakty – Elektrické rozhraní a protokoly přenosu

ISO/IEC 7816-4 – Identifikační karty – Karty s integrovanými obvody – Část 4: Organizace, bezpečnost a příkazy pro výměnu dat

ISO/IEC 14443-3 – Bezkontaktní karty s integrovanými obvody – Karty s vazbou na blízko – Část 3: Inicializace a antikolize

ISO/IEC 14443-4 – Bezkontaktní karty s integrovanými obvody – Karty s vazbou na blízko – Část 4: Protokol přenosu

3. Termíny a definice

Tato kapitola obsahuje 11 termínů a definic souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou:

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 12 zkratk souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou následující:

ICC karet s integrovanými obvody (integrated circuits card)

EFC elektronický výběr mýtného (electronic fee collection)

OBE palubní zařízení (on-board equipment)

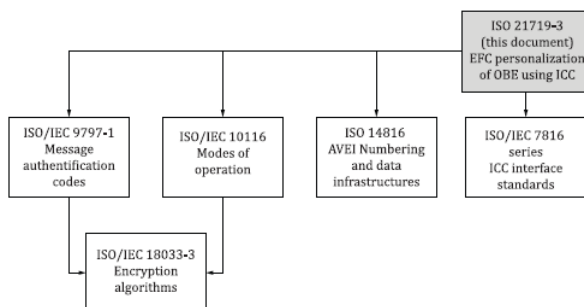
PE personalizační zařízení (personalization equipment)

PICS prohlášení o shodě implementace protokolu (protocol implementation conformance statement)

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

5 Shoda

Tato kapitola v rozsahu 1 strany 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 1 - Vztah mezi základními technickými normami a ISO/TS 21719-3 (obr. 3 normy)

6 Základní informace o personalizaci

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

7 Požadavky na palubní zařízení

Tato kapitola v rozsahu 4 stran popisuje normativní požadavky na ověření shody palubního zařízení (OBE) s profilem definovaným popisovaným dokumentem.

Palubní zařízení (OBE) musí být schopno provést kompletní personalizační transakci zahrnující inicializaci, čtení, zápis, ověření a potvrzení výsledku. Musí podporovat alespoň jedno standardizované rozhraní ICC, ať už kontaktní dle ISO/IEC 7816-3/4 nebo bezkontaktní podle ISO/IEC 14443 či ISO/IEC 15693, a být schopno inicializovat komunikaci s kartou, číst i zapisovat potřebná data a po dokončení komunikaci ukončit. Hlavním úkolem palubního zařízení (OBE) je načíst personalizační parametry uložené na kartě ICC personalizačním zařízením (PE), ověřit shodu svého identifikátoru s identifikátorem na kartě a následně zapsat zpět informaci o úspěchu nebo neúspěchu personalizace. Personalizační data mají formu atributů definovaných technickou normou ISO 14906 a mohou zahrnovat aplikační údaje i bezpečnostní klíče. Bezpečnostní požadavky vycházejí z technické normy ISO 19299 a používají mechanismy definované v ISO/IEC 7816-4, přičemž konkrétní algoritmy popisovaný dokument nestanovuje.

8 Požadavky na personalizační zařízení

Tato kapitola v rozsahu 1 strany popisuje normativní požadavky na ověření shody personalizačního zařízení (PE) s profilem definovaným popisovaným dokumentem.

Personalizační zařízení (PE) musí podporovat stejné rozhraní ICC jako palubního zařízení (OBE), tedy kontaktní podle ISO/IEC 7816 nebo bezkontaktní podle ISO/IEC 14443 či ISO/IEC 15693, a být schopno inicializovat kartu, vytvořit personalizační parametry, uložit je ve správné datové struktuře a zajistit jejich bezpečný zápis. Po dokončení personalizace na straně palubního zařízení (OBE) musí být schopno znovu přečíst kartu, zkontrolovat hodnotu informaci, která potvrzuje úspěch nebo neúspěch personalizace.

Příloha A (normativní) - PICS

Příloha A v rozsahu 4 stran obsahuje formulář PICS za účelem posouzení shody dané implementace s požadavky uvedenými v popisovaném dokumentu.

Tato příloha popisuje pravidla pro vyplňování formuláře, vysvětluje označení povinných, volitelných a podmíněných požadavků a obsahuje samostatné tabulky pro palubní zařízení (OBE) i personalizační zařízení (PE). Součástí jsou

identifikační údaje o zařízení a výrobci, přehled podporovaných ICC rozhraní a potvrzení implementace klíčových personalizačních funkcí, jako je inicializace, čtení a zápis dat.

Tato příloha tedy představuje formální a standardizovaný rámec pro posuzování a prohlášení shody palubní zařízení (OBE) i personalizační zařízení (PE) s popisovaným dokumentem.

Příloha B (informativní) - Příklad transakce

Příloha B v rozsahu 2 stran uvádí příklad personalizační transakce. Slouží k ilustraci toho, jak probíhá personalizační proces, v němž jsou data přenášena z personalizačního zařízení (PE) do palubního zařízení (OBE) prostřednictvím čipové karty ICC.