**STRUKTURA BEZKONTAKTNÍ ČIPOVÉ KARTY IREDO**

**dále jen „Struktura BČK IREDO“**

**platnost od:** bude doplněno před podpisem smlouvy

**Integrovaná regionální doprava**

****

**Struktura BČK IREDO**

**Verze 38 ze 17.4.2015**

**Obsah**

[1. Úvod 6](#_Toc525563149)

[1.1 Shoda návrhu se standardy 6](#_Toc525563150)

[1.2 Popis návrhu Struktury BČK IREDO 7](#_Toc525563151)

[1.3 Definice zkratek a pojmů 7](#_Toc525563152)

[2. Specifikace použitých datových typů 9](#_Toc525563153)

[3. Struktura popisovaných aplikací 10](#_Toc525563154)

[4. Aplikace na BČK IREDO 12](#_Toc525563155)

[4.1 Personalizační aplikace - 002D 12](#_Toc525563156)

[4.1.1 Struktura souboru Informace o BČK IREDO 12](#_Toc525563157)

[4.1.2 Struktura souboru Informace o držiteli 13](#_Toc525563158)

[4.1.3 Klíče 15](#_Toc525563159)

[4.2 Aplikace Průkazy/Benefity - 5412 16](#_Toc525563160)

[4.2.1 Soubor Průkaz/Benefit 16](#_Toc525563161)

[4.2.2 Klíče 17](#_Toc525563162)

[4.3 Aplikace IDS jízdenky - 1206 18](#_Toc525563163)

[4.3.1 Soubor Jízdenka 18](#_Toc525563164)

[4.3.2 Soubor Kontrola jízdenky 25](#_Toc525563165)

[4.3.3 Soubor Místenka 26](#_Toc525563166)

[4.3.4 Klíče 27](#_Toc525563167)

[4.4 Aplikace Elektronická peněženka (EP) – 88AD 29](#_Toc525563168)

[4.4.1 Soubor Nastavení EP 29](#_Toc525563169)

[4.4.2 Soubor Osobní nastavení EP 30](#_Toc525563170)

[4.4.3 Hodnota EP 31](#_Toc525563171)

[4.4.4 Log EP 31](#_Toc525563172)

[4.4.5 Klíče 32](#_Toc525563173)

[4.5 Rezerva 1 - 0743 34](#_Toc525563174)

[4.5.1 Struktura 34](#_Toc525563175)

[4.5.2 Klíče 34](#_Toc525563176)

[4.6 Rezerva 2 - 1207 34](#_Toc525563177)

[4.6.1 Struktura 34](#_Toc525563178)

[4.6.2 Klíče 34](#_Toc525563179)

[4.7 Rezerva 3 - 0744 34](#_Toc525563180)

[4.7.1 Struktura 34](#_Toc525563181)

[4.7.2 Klíče 35](#_Toc525563182)

[4.8 Rezerva 4 – 100B - DOPR 35](#_Toc525563183)

[4.8.1 Struktura 35](#_Toc525563184)

[4.8.2 Klíče 35](#_Toc525563185)

[4.9 Rezerva 5 – 0004 - PA 35](#_Toc525563186)

[4.9.1 Struktura 35](#_Toc525563187)

[4.9.2 Klíče 35](#_Toc525563188)

[4.10 Rezerva 6 – 883D - MEP 36](#_Toc525563189)

[4.10.1 Struktura 36](#_Toc525563190)

[4.10.2 Klíče 36](#_Toc525563191)

[*5.* Použité normativní dokumenty 37](#_Toc525563192)

**Historie změn:**

| **Verze** | **Datum** | **Jméno** | **Důvod vydání** |
| --- | --- | --- | --- |
| 32 | 27.03.2012 | Holešovský | Změna v číslování kupónů, doplnění povinných položek |
| 33 | 6.6.2012 | Holešovský | Změna v číslování kupónů , Zrušeno RFU a přidáno číslo souboru |
| 34 | 9.7.2012 | Holešovský | Změna významu položky RestrictDayOfWeek na DayOfWeek a contractPaymentMeans na výklad dle EN 1545-2 |
| 35 | 10.7.2012 | Holešovský | Změna v hodnotě publisherProviderID |
| 36 | 3.10.2012 | Holešovský | Doplnění významu položky contract-id a zpřesnění významu fileNumber |
| 37 | 25.8.2014 | Škapa | Doplnění položky couponsPrepaidTransaction a změna položky walletPersDevice na walletPersCreditTransaction |
| 38 | 17.4.2015 | Nenka | Změna loga OREDO |

# Úvod

Dokument obsahuje informace o Struktuře BČK IREDO týkající se:

* struktury aplikací/souborů a jejích formátů

Popisované struktury aplikací se týkají BČK IREDO standardu Mifare DESFire. BČK IREDO pro IDS IREDO je tzv. multi-aplikační BČK IREDO, což znamená, že na jedné BČK IREDO mohou být nahrány jak aplikace vydavatele BČK IREDO, tak i aplikace jiných poskytovatelů aplikací. Aplikace vydavatele BČK jsou obecně známé ostatním poskytovatelům aplikací či subjektům akceptujícím BČK IREDO.

Z důvodů mnoha subjektů, pracujících s BČK IREDO, jsou všechny použité datové typy co nejlépe dokumentované a zejména pak jsou převzaty z normativních dokumentů, jejichž seznam je součástí tohoto dokumentu jako kapitola 5 – Použité normativní dokumenty. Návrh je také v souladu s připravovanou vyhláškou ustanovující standardy platby a odbavení cestujících ve veřejné dopravě s využitím bezkontaktních čipových technologií.

Architektura je navržena tak, aby mohla být použita metoda postupného budování infrastruktury a využívání BČK IREDO, kde v první části (fázi) bude budována dopravní aplikace, tj. využití BČK IREDO jako nositele elektronického jízdného.

Každá aplikace má přiděleno jedno AID dle specifikace NXP pro Mifare DESFire – celkem 3 byty.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| MIFARE DESFire AID Byte 0 | | MIFARE DESFire AID Byte 1 | | MIFARE DESFire AID Byte 2 | |
| Nibble 0 | Nibble 1 | Nibble 2 | Nibble 3 | Nibble 4 | Nibble 5 |
| 0xF | MIFARE classic AID | | | | 0x0 |

## Shoda návrhu se standardy

* komunikace je řešena ve shodě s ISO 14443 A, definující bezkontaktní interface, čímž výsledné řešení zajistí technologickou interoperabilitu plošně skrze všechny uživatele,
* operační systém navržené BČK IREDO odděluje ve své paměti datové prostory tak, aby BČK IREDO umožnila práci s nezávislými aplikacemi,
* přístup k odděleným datovým prostorům je řízen podle typu operací,
* operační systém navržené BČK IREDO a autentizační mechanismy BČK IREDO umožňují jednomu subjektu vykonávat správu obsahu BČK IREDO bez možnosti přístupu k datům a klíčům uvnitř jednotlivých aplikací, tj. nahrávat dopravní aplikace jejich správu i vymazání takovým způsobem, že neoprávněné subjekty nejsou schopny zjistit ani ovlivnit jejich obsah,
* návrh BČK IREDO umožňuje multifunkční použití, tj. paralelní umístění, užívání a správu aplikací různých subjektů,
* návrh BČK IREDO nabízí kromě standardní bezpečnosti karet Mifare DESFire i vlastní nativní bezpečnostní prvky - šifrování obsahu, podpis obsahu pomocí symetrických i asymetrických kryptografických mechanismů,
* návrh BČK IREDO umožňuje zavedení dodatečné bezpečnostní vrstvy prostředky, které jsou na nativních bezpečnostních mechanismech BČK IREDO nezávislé,
* BČK IREDO umožňuje obnovovat bezpečným způsobem kryptografické klíče použité pro ochranu BČK IREDO a jejich aplikací,
* návrh BČK IREDO umožňuje bezpečným způsobem zapisovat na BČK IREDO nové aplikace, popř. je vymazávat,
* datové struktury jsou navržené na základě standardu pro běžně používané technologie,
* použité číselníky odpovídají stávajícím používaným číselníkům u ostatních IDS,
* návrh BČK IREDO umožňuje nahrávat strukturu také na NFC mobilní telefony podporující v Secure Elementu karty Mifare DESFire.

## Popis návrhu Struktury BČK IREDO

Návrh obsahuje 4 kompletní aplikace a 4 rezervní aplikace pro případné další doplnění Struktury BČK IREDO.

Kompletní aplikace:

* Personalizační, tvořená 2 soubory:
  + Informace o BČK IREDO:
    - Podrobněji viz Struktura souboru Informace o BČK IREDO.
  + Informace o držiteli:
    - Umožnuje identifikaci držitele, podporuje ale i anonymní BČK IREDO.
    - Podrobněji viz Struktura souboru Informace o držiteli.
* Průkazy/Benefity:
  + Obecná aplikace tvořená 5 stejnými soubory s různými právy na zápis do jednotlivých souborů
  + Možné využití aplikace například pro:
    - Parkování.
    - Slevová karta.
    - Rezervační systém.
    - Stravovací systém.
    - Docházkový systém.
    - Knihovní systém.
    - Portál úředníka.
    - Dopravní aplikace ČD.
  + Podrobněji viz Soubor Průkaz/Benefit.
* IDS jízdenky:
  + Aplikace podporující jak dlouhodobé časové kupóny, tak i jednorázové jízdenky.
  + Pro každou jízdenku podporuje záznam o kontrole, včetně záznamu o nástupu do vozidla.
  + Tvořená 10 soubory pro časový kupón/jednorázovou jízdenku.
  + Tvořená 5 soubory o záznamu o kontrole.
  + Tvořená 2 soubory pro podporu místenek ke kupónům.
  + Návrh podporuje použití ve všech dopravních prostředcích.
  + Podrobněji viz Aplikace IDS jízdenky.
* Elektronická peněženka (EP):
  + Obsahuje 4 soubory včetně souboru s transakčním logem pro kontrolu stavu EP.
  + Podporuje až 4 měny.
  + Podrobněji viz Aplikace Elektronická peněženka (EP).

## Definice zkratek a pojmů

| ***Zkratka/Pojem*** | ***Definice*** |
| --- | --- |
| AID | Identifikátor aplikace Application Identifier ISO/IEC 7816-5:2004 |
| BČK IREDO | Bezkontaktní čipová karta IREDO |
| contract-id | jednoznačná identifikace prodaného kontraktu (el.jízdenky) v rámci BČK IREDO v hexadecimálním tvaru  **contract-id = fileNumber(4 bity) + contractSerialNumber (8 bit)**  Používá se v komunikaci s clearingovým systémem Cards Exchange   * dopravci by ji měly tisknout na doklady – pro případné reklamace, * dopravci by ji měly ukládat do svých back office systémů pro pozdější zpracování (např. reklamace), * odbavovací zařízení by tuto proměnnou mělo být schopné zobrazit (např. v info režimu BČK IREDO), * back office systémy pracující s BČK IREDO (POS, různé „diagnostické“ nástroje pracující se Strukturou BČK IREDO) by ji měly zobrazovat |
| ČD | České dráhy, a.s. |
| DD | Odbavovací zařízení, která mají charakter odbavení zákazníka (například odbavení kupónu nebo EP na validátoru (strojku), obecná platba EP,...). DD operace s BČK IREDO jsou obecně považovány za časté a méně spolehlivé s ohledem na zápis dat na BČK IREDO |
| EP | Elektronická peněženka |
| KC | Kartové centrum, provádí grafickou a datovou personalizaci |
| HW | Hardware |
| IDS IREDO | Integrovaný dopravní systém IREDO |
| Lsb | Least Significant Bit, nejméně významný bit |
| LSB | Least Significant Byte, nejméně významný bajt |
| MHD | Městská hromadná doprava |
| Msb | Most Significant Bit, nejvíce významný bit |
| MSB | Most Significant Byte, nejvíce významný bajt |
| N/A | Not Available, není k dispozici |
| MKA | Master klíč aplikace |
| MKK | Master klíč karty |
| ORE\_CMK | Master klíč karty OREDO |
| PAD | Příměstská autobusová doprava |
| POS | Point Of Sale - zařízení, která mají charakter POS (dobití kupónu či EP na KC nebo v automatu nebo u řidiče). POS operace s BČK IREDO jsou obecně považovány za méně časté a více spolehlivé s ohledem na zápis dat na BČK IREDO |
| RFU | Reserved for Future Use, rezervováno pro budoucí použití |
| Secure Element | čip bezpečně emulující kartu Mifare a JavaCard na NFC zařízeních |
| SAM | Secure Application Module |
| SW | Software |

# Specifikace použitých datových typů

|  |  |  |
| --- | --- | --- |
| ***Název*** | ***Byte*** | ***Popis*** |
| INT1 | 1 | INTEGER (0..255) |
| INT2 | 2 | INTEGER (0..65535) |
| INT3 | 3 | INTEGER (0..16777215) |
| INT4 | 4 | INTEGER (0..4294967295) |
| BCDString |  | Sekvence BCD číslic (BCDString). Každý byte obsahuje dvě 4-bitové BCD číslice, zakódované v horní a dolní polovině bytu.  Příklad: desítkové číslo 123456 bude ve tvaru BCD uloženo jako sekvence byte 0x12, 0x34, 0x56. |
| UTF8String |  | Řetězec znaků v kódování UTF-8. U každého výskytu UTF8String musí být v tomto dokumentu specifikována jeho maximální délka v bajtech (nikoli znacích). Je-li řetězec kratší než jeho maximální délka, bude zprava doplněn byty o hodnotě 0x00. |
| Datef | 4 | Dle EN 1545 |
| DateStamp | 1,6 | Počet dní od 1.1.1997. Rozsah 1.1.1997 až 9.11.2041. |
| TimeStamp | 1,4 | Počet minut po půlnoci, půlnoc je 0 |
| OCTET STRING (L) | L × 8 | Řetězec byte (oktetů) o maximální specifikované délce (tzv. bytové pole). Řetězec je vždy zarovnán na celé byte. Je-li zapisané pole byte kratší než specifikovaná délka, bude zprava vyplněno byty v hodnotě 0x00. |

# Struktura popisovaných aplikací

Všechny soubory ve všech aplikacích v tomto návrhu BČK IREDO mají jednotnou strukturu a jednotný formát popisu (s drobnou odchylkou u typu souboru „Value File“).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***#Num*** | ***FileName*** | | | ***FileType*** |
| ***Název*** | | ***Bitů*** | ***Typ*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 |
| Status souboru | | 8 | cancelled (5)  ok (7)  pre-allocated (16)  disabled (88) |
| Typ podpisu | | 4 |  |
| Typ šifrování | | 4 |  |
| Proměnné 1 | | 32 | Typ 1 |
| Proměnné 2 | | X | Typ 2 | Potenciálně šifrovaná oblast souboru (u tohoto souboru nemá šifrování význam) |
| Podpis | | 64 |  |
| Využito | |  |  | |
| RFU | | x |  | |
| Celkem B | |  | (= X × 32 B) | |

***Význam:***

*#Num*: Pořadové číslo souboru v aplikaci

*FileName*: Jméno souboru (pouze mnemotechnická pomůcka, není uloženo na BČK IREDO)

*FileType*: Typ souboru dle speficikace DESFire

*Verze*: Verze záznamu (inkrementální počítadlo od 0). Nula znamená, že soubor existuje, neobsahuje ale žádná data. Všechny zde prezentované datové formáty jsou ve verzi 1.

*Podpis*: Digitální podpis (nebo jeho ekvivalent) dle položky Typ podpisu

*Typ podpisu*:

|  |  |
| --- | --- |
| 0 | nepodepsáno |
| 1 | privátní algoritmus poskytovatele aplikace |
| 2 | bloková šifra DES-CBC-MAC8 |
| 3 | bloková šifra 3DES-CBC-MAC8 |
| 4 | hash funkce MD5 |
| 5 | hash funkce SHA-1 |
| 6 | hash funkce SHA-2 |
| 7 | hash funkce HMAC |
| 8 | eliptická křivka SECT193R1 |
| 9 - 12 | RFU |
| 13 - 15 | specifický pro danou síť |
|  |  |

*Typ šifrování*:

|  |  |
| --- | --- |
| 0 | Nekryptováno |
| 1 | privátní algoritmus poskytovatele aplikace |
| 2 | symetrický algoritmus DES-CBC, padding Method 0 |
| 3 | symetrický algoritmus 3DES-CBC, padding Method 0 |
| 4 | symetrický algoritmus AES128 |
| 5 | symetrický algoritmus AES256 |
| 6 - 12 | RFU |
| 13 - 15 | specifický pro danou síť |

*Proměnné 1*: 4 byte k dispozici v nešifrované velikosti souboru, může být definováno nebo RFU

*Proměnné 2*: 16 + n × 32 byte šifrovaného obsahu souboru. Zaokrouhlení na 32 byte je z důvodu omezení vnitřní fragmentace souborů DESFire BČK IREDO. Z důvodu zvýšení přehlednosti je vlastní obsah souboru obvykle vypsán ve zvláštní tabulce, popsané pod popisem souboru.

Tento princip umožňuje snadnou znovupoužitelnost a jednotný pohled na struktury, jak na různých BČK IREDO, tak i v různých aplikací stejné BČK IREDO.

# Aplikace na BČK IREDO

Návrh aplikací, souborů a typů položek souborů se řídí těmito pravidly:

* režim komunikace souborů bude nastaven na Encrypted,
* RFU bude vyplněno nulami,
* vícebajtové číselné datové typy (INT2, INT3, INT4, DateStemp, TimeStamp) jsou uloženy v bajtovém kódování LittleEndian.

## Personalizační aplikace - 002D

* AID aplikace – 002D,
* obsahuje 2 soubory,
* zahrnuje identifikační znaky vydavatele, podpis UID, informace o BČK IREDO a o držiteli BČK IREDO.

### Struktura souboru Informace o BČK IREDO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***0*** | ***cardInfoFile*** | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Typ*** | ***Typ editace*** | ***Hodnota (popis)*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 |
| Status souboru | | 8 |  | KC | 7 (Ok) |
| Typ podpisu | | 4 |  | KC | 0 (nepodepsáno) |
| Typ šifrování | | 4 |  | KC | 0 (nekryptováno) |
| RFU | | 40 |  |  | volné místo vyplněné '0'B |
| cardInfo | | 640 | Datová struktura cardInfo |  | Kód definující datovou strukturu cardInfo (viz 4.1.1.1). | Potenciálně šifrovaná oblast souboru  (u tohoto souboru nemá šifrování význam) |
| Podpis | | 64 |  | KC | volné místo vyplněné '0'B |
| Využito | | 768 |  | | |
| RFU | | 0 |  | | |
| Celkem B | | 96 | (= 3 × 32 B) | | |

#### Datová struktura cardInfo

| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- |
| publisherProviderID | Identifikace vydavatele BČK IREDO dle číselníku dle Číselníku NetworkID & ProviderID | INT3 | 24 | KC | 124 |
| publisherNetworkID | Identifikace transportní sítě do které patří vydavatel BČK IREDO | INT3 | 24 | KC | 203522 |
| signatureVersion | verze klíče ECDSA | INT1 | 8 | KC | 1 |
| signatureUID | privátním klíčem ECDSA podepsané UID BČK IREDO – typ 8 | OCTET STRING (56) | 448 | KC | ORE\_002D\_ECC\_P |
| cardNumber | Logické číslo BČK IREDO – dle ISO7812 |  | 72 | KC |  |
| appStartDate | Počátek platnosti BČK IREDO | DateStamp | 14 | KC | datum výroby BČK IREDO |
| appEndDate | Konec platnosti BČK IREDO | DateStamp | 14 | KC | datum výroby BČK IREDO + 6 let |
| couponsPrepaidTransaction | Číslo předplacené transakce kuponu | INT4 | 32 | POS DD | Ekvivalent položky walletPersCreditTransaction ve struktuře EP, zde však používaný pro kupony. |
| RFU |  |  | 4 | KC | volné místo vyplněné '0'B |
| **Celkem bitů** | | | **640** |  |  |
| **Celkem byte** | | | **80** |  |  |

### Struktura souboru Informace o držiteli

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***1*** | ***cardHolderInfoFile*** | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Název*** | ***Typ editace*** | ***Hodnota (popis)*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 |
| Status souboru | | 8 |  | KC | 7 (Ok) |
| Typ podpisu | | 4 |  | POS | 0 (nepodepsáno) |
| Typ šifrování | | 4 |  | POS | 0 (nekryptováno) |
| Typ držitele | | 8 | INT1 | POS | druh BČK IREDO dle držitele a způsobu použití - viz níže |
| RFU | | 32 |  | N/A | volné místo vyplněné '0'B |
| cardHolderInfo | | 896 | Datová struktura cardHolderInfo |  | Kód definující datovou strukturu cardHolderInfo  (viz 4.1.2.1). | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | POS | 0 |
| Využito | | 1024 |  | | |
| RFU | | 0 |  | | |
| Celkem B | | 128 | (= 4 × 32 B) | | |

#### Datová struktura cardHolderInfo

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| holderBirth |  | Datum narození (nebo jiný datumový údaj) | Datef | 32 | KC  POS | RFU |
| holderSex |  | Pohlaví držitele dle ČSN ISO/IEC 5218 |  | 4 | KC  POS | RFU |
| holderID |  | Bezvýznamový identifikátor držitele, např. identifikátor MPSV, případně RFU | BCDString | 80 | KC  POS | RFU |
| holderName |  | Identifikace držitele (75 B, tedy 37 až 75 znaků) | UTF8String | 600 | KC  POS | RFU |
| holderProfile1 | + | Profil1 držitele BČK IREDO dle EN 1545 | ProfileCodeIOP | 6 | KC  POS |  |
| profile1StartDate | + | Platnost profilu1 od | DateStamp | 14 | KC  POS |  |
| profile1EndDate | + | Platnost profilu1 do | DateStamp | 14 | KC  KC  POS |  |
| holderProfile2 |  | Profil2 držitele BČK IREDO dle EN 1545 | ProfileCodeIOP | 6 | KC  POS |  |
| profile2StartDate |  | Platnost profilu2 od | DateStamp | 14 | KC  POS |  |
| profile2EndDate |  | Platnost profilu2 do | DateStamp | 14 | KC  POS |  |
| RFU |  |  |  | 112 | KC | volné místo vyplněné '0'B |
| **Celkem bitů** | | **896** |
| **Celkem byte** | | **112** |

Poznámky ke struktuře:

* *Typ držitele* je jeden z následujících:
  + 0: **Anonymní BČK IREDO** (položky holderBirth a holderName jsou vyplněny nulami; položka holderSex je nastavena v souladu s normou na 9).
  + 1: **Personalizovaná BČK IREDO** (položky holderBirth a holderSex jsou vyplněny; holderName obsahuje jméno a příjmení držitele, toto může být případně zkrácené na celé znaky).
  + 2: **Přenosná BČK IREDO** (položka holderBirth je vyplněna nulami; holderSex obsahuje 9 a holderName je jménem organizace vlastnící přenosnou BČK IREDO, holderID obsahuje identifikátor organizace).
  + 3: **Nepřenosná nepersonalizovaná BČK IREDO** (holderID může obsahovat identifikaci držitele, holderName není vyplněno, položky holderBirth a holderSex jsou vyplněny).
  + 4: **Graficky personalizovaná BČK IREDO** (položky holderBirth a holderName jsou vyplněny nulami; položka holderSex je nastavena v souladu s normou na 9).
  + 5: **Náhradní karta** (položky holderBirth a holderName jsou vyplněny nulami; položka holderSex je nastavena v souladu s normou na 9).
  + 6: **Zaměstnanecká graficky personalizovaná BČK IREDO** (položky holderBirth a holderName jsou vyplněny nulami; položka holderSex je nastavena v souladu s normou na 9).
* *Pohlaví držitele* norma ČSN ISO/IEC 5218 udává jako:
  + 0: není známo,
  + 1: mužské,
  + 2: ženské,
  + 9: není aplikováno (nemá význam).

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_002D\_0 | Master – klíč aplikace |
| #1 | ORE\_002D\_1 | Čtení souboru informace o BČK IREDO |
| #2 | ORE\_002D\_2 | Čtení/zápis souboru informace o BČK IREDO |
| #3 | ORE\_002D\_3 | Čtení souboru informace o držiteli |
| #4 | ORE\_002D\_4 | Čtení/zápis souboru informace o držiteli |
| #5 | RFU |  |

#### Přístupová práva souborů

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Soubor*** | ***Název*** | ***Read*** | ***Write*** | ***Read & Write*** | ***Change***  ***Access Rights*** |
| 0 | Informace o BČK IREDO | #1 (nebo bez klíče) | #0 | #2 | #0 |
| 1 | Informace o držiteli | #3 (nebo bez klíče) | #0 | #4 | #0 |

## Aplikace Průkazy/Benefity - 5412

* AID aplikace – 5412,
* obsahuje 5 souborů,
* možné použít pro:
  + slevovou kartu,
  + turistickou „City/Region Card“,
  + průkaz, opravňující ke vstupu či k nějaké činnosti,
  + průkaz, ověřující vlastnost držitele (žákovský průkaz, zaměstnanecký průkaz),
  + permanentní vstupenka (s nebo bez možnosti počítání vstupů na kartě),
  + dopravní aplikaci ČD.

### Soubor Průkaz/Benefit

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***0 - 4*** | ***benefitFile*** | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Název*** | ***Typ editace*** | ***Hodnota (popis)*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 |
| Status souboru | | 8 |  | KC | 7 (Ok) |
| Typ podpisu | | 4 |  | KC | 0 (nepodepsáno) |
| Typ šifrování | | 4 |  | KC | 0 (nekryptováno) |
| benefitProvider | | 32 | INT4 Kód vydavatele/příjemce průkazu dle číselníku | KC | volné místo vyplněné '0'B |
| RFU | | 8 |  | N/A | volné místo vyplněné '0'B |
| Benefit | | 128 | Datová struktura benefitInfo | KC | Kód definující datovou strukturu benefitInfo  (viz 4.2.1.1). | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | KC | 0 |
| Využito | | 256 |  | | |
| Celkem B | | 32 |  | | |
| Využito | | 256 | (= 1 × 32 B) | | |

#### Datová struktura benefitInfo

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| benefitValidityStart | Datum platnosti od | DateStamp | 14 | POS |  |
| benefitValidityEnd | Datum platnosti do | DateStamp | 14 | POS |  |
| RFU |  |  | 4 | POS | volné místo vyplněné '0'B |
| benefitType | Data průkazu (strukturu stanovuje každá aplikace sama) | OCTET STRING (8) | 96 | POS |  |
| **Celkem bitů** | | | **128** |
| **Celkem byte** | | | **16** |

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_5412\_0 | Master – klíč aplikace |
| #1 | ORE\_5412\_1 | Čtení souboru 1 – 5 |
| #2 | ORE\_5412\_2 | Čtení/zápis souboru 1 |
| #3 | ORE\_5412\_3 | Čtení/zápis souboru 2 |
| #4 | ORE\_5412\_4 | Čtení/zápis souboru 3 |
| #5 | ORE\_5412\_5 | Čtení/zápis souboru 4 |
| #6 | ORE\_5412\_6 | Čtení/zápis souboru 5 |
| #7 | ORE\_5412\_7 | RFU |

#### Přístupová práva souborů

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Soubor*** | ***Název*** | ***Read*** | ***Write*** | ***Read & Write*** | ***Change***  ***Access Rights*** |
| 0 | Soubor 1 | #1 | #0 | #2 | #0 |
| 1 | Soubor 2 | #1 | #0 | #3 | #0 |
| 2 | Soubor 3 | #1 | #0 | #4 | #0 |
| 3 | Soubor 4 | #1 | #0 | #5 | #0 |
| 4 | Soubor 5 | #1 | #0 | #6 | #0 |

## Aplikace IDS jízdenky - 1206

* AID aplikace - 1206,
* obsahuje 10 souborů jízdenek, 5 souborů pro kontrolu jízdenky a 2 soubory místenek,
* v datových strukturách v této aplikaci jsou na rozdíl od zbytku dokumentu použity datové typy dle norem ČSN EN 1545-1 a ČSN EN 15320.

### Soubor Jízdenka

Filozofie souboru: Soubor Jízdenka umožňuje výdej libovolného dokladu (jednorázového nebo časového) platného v IDS IREDO. Umožňuje i nahrání většiny jízdních dokladů dopravců mimo IDS IREDO. Vlastnosti:

* Na jeden jízdní doklad lze odbavit až 4 × 15 cestujících, v libovolné kombinaci „dospělých“, „slev“ a „zavazadel/psů“.
* Jízdenka platí v čase, který je na ní uveden při prodeji, lze určit platnost „od prvního označení“.
* Trasu lze definovat:
  + definicí sítě,
  + výčtem zón platnosti,
  + relačně.
* Pro zjednodušení prodejních a kontrolních operací jsou všechny záznamy pevné délky (nedojde tak k situaci, že by sice v souboru s jízdenkami bylo dostatek místa, ale díky vnitřní fragmentaci by nebylo možné novou jízdenku zapsat).
* Časovou platnost dokladu lze nastavit v podstatě libovolně.
* Je počítáno s tím, že k jízdnímu dokladu je možné vydat doplatek nebo doklad refundovat cestujícícmu i na zařízení, které je off-line (umožňují-li to tarifní a jiné administrativní podmínky).
* Hlavní zásadou při tvorbě dokladu je *minimalizace dat*, zapisovaných na BČK IREDO a vyměňovaných mezi jednotlivými (dopravními) subjekty. Proto nejsou na BČK IREDO zejména žádné údaje, které se vytvářejí/ověřují pouze při zpracování BČK IREDO oproti centrálním systémům. Typicky není potřeba na BČK IREDO nahrávat přesné názvy tarifních dokladů. Tedy například *jednodenní, pětidenní, týdenní, měsíční, čtvrtletní, desetiměsíční a roční jízdenku* je pro kontrolu ve vozidle možné vést pouze jako *jízdenku časovou.* Navíc je pro potřeby kontroly ve voze obecně jedno, zda-li se jedná o jízdenku občanskou, pro dárce krve nebo jinou. Je třeba pouze odlišit různé typy dokladů, které vyžadují *při kontrole ve vozidle, nikoli při prodeji* různé dodatečné ověření způsobem, který neumožňuje přímo BČK IREDO jako datový nosič (například předložení jiného průkazu).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***0 - 9*** | ***seasonTicketFile*** | | | | | ***Backup Data File*** |
| ***Název*** | | ***Bitů*** | ***Název*** | ***Typ editace*** | ***Hodnota (popis)*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 |
| Status souboru | | 8 |  | KC | cancelled (5)  ok (7)  pre-allocated (16) |
| Typ podpisu | | 4 |  | POS/DD | 3 (3DES-CBC-MAC8) |
| Typ šifrování | | 4 |  | POS/DD | 0 (nekryptováno) |
| RFU | | 24 |  |  | volné místo vyplněné '0'B |
| seasonTicket | | 656 | Datová struktura seasonTicketInfo |  | Kód definující datovou strukturu seasonTicketInfo  (viz 4.3.1.1). | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | POS/DD | Struktura od Verze po seasonTicket + **UID + 0x00** podepsán klíčem ORE\_1206\_SIGN |
| Využito | | 768 |  | | |
| Celkem B | | 0 |  | | |
| Využito | | 96 | (= 3 × 32 B) | | |

#### Datová struktura seasonTicketInfo

| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- | --- |
| contractNetwork | + | Identifikace transportní sítě, do které patří provozovatel uvedený v proměnné contractProvider. Dle číselníku NetworkID & ProviderID | NetworkId | 24 | POS  DD | 203522 |
| contractProvider | + | Kód provozovatele, který prodal či dobil kupón | ProviderID | 8 | POS  DD | Dle číselníku NetworkID & ProviderID pro IREDO |
| couponType | + | Typ kupónu  0 – časový kupón  1 – krátkodobá jízdenka  2 – kilometrické jízdné  3 – jednotlivé jízdné  4 .. – RFU |  | 6 | POS  DD |  |
| contractSaleAgent | + | Pokladník, který doklad prodal | INT3 | 24 | POS  DD |  |
| contractSaleDevice | + | Číslo prodejního místa (terminálu) | INT4 | 32 | POS  DD |  |
| contractSerialNumber | + | Číslo kupónu (v datech pro clearing se odlišuje číslem souboru na BČK IREDO) | INT1 | 8 | POS  DD | Inkrementuje se při prodeji v rámci souboru (po 255 následuje 0) |
| contractSaleSerialNumber | + | Jedinečné číslo kupónu pro prodejní místo(terminál, eshop) | INT3 | 24 | POS  DD | Inkrementuje se při prodeji |
| contractValidityStartDate | + | Počátek platnosti – datum | DateStamp | 14 | POS  DD |  |
| contractValidityStartTime | + | Počátek platnosti – čas | TimeStamp | 11 | POS  DD |  |
| contractValidityEndDate | + | Konec platnosti – datum | DateStamp | 14 | POS  DD |  |
| contractValidityEndTime | + | Konec platnosti – čas | TimeStamp | 11 | POS  DD |  |
| contractValidityRestrictDay | + | Omezení platnosti na dny (vhodné např. pro žákovské jízdenky).  bity: 0 – 6 = Po až Ne, bit 7 = ‚h’. Nastavený bit = doklad platí. Standardně tedy bude vyplněno hodnotou 0x7F (7 bitů) | Days of Week | 8 | POS  DD | 0x7F |
| contractValidityRestrictCode |  | Omezení platnosti dle číselníku, uplatňuje se, pokud je nastaven nejvyšší bit ‚h‘ položky *contractValidityRestrictDays*. Číselník bude vytvořen později. | INT1 | 8 | POS  DD | 0x00 |
| contract1 | + | Informace o prvním profilu cestujícího. | seasonTicketContract (viz 4.3.1.2) | 32 | POS  DD |  |
| contract2 | + | Informace o druhém profilu cestujícího. | seasonTicketContract (viz 4.3.1.2) | 32 | POS  DD |  |
| contract3 | + | Informace o třetím profilu cestujícího. | seasonTicketContract (viz 4.3.1.2) | 32 | POS  DD |  |
| contract4 | + | Informace o čtvrtém profilu cestujícího. | seasonTicketContract (viz 4.3.1.2) | 32 | POS  DD |  |
| seatReservationFile |  | Číslo souboru s místenkou  0 – bez místenky,  1 – soubor místenka 1 (číslo souboru 10),  2 – soubor místenka 2 (číslo souboru 11) |  | 3 | POS  DD | 0x00 |
| contractTransportMeansRestriction |  | Bitové pole povolených dopravních prostředků. Více pod tabulkou. |  | 16 | POS  DD | 0x00 |
| contractVehicleClassCodeRestriction |  | Povolená vozová třída (v závislosti na dopravním prostředku) 0: bez omezení  1: 1. třída nebo její ekvivalent  2: 1. i 2. třída nebo jejich ekvivalent  3: RFU |  | 2 | POS  DD | 0x00 |
| contractHasJourney | + | **0: Doklad nemá trasu (síťová jízdenka)**  **1: Doklad je dán relací (Z, Do, Přes)**  **2: Doklad je dán výčtem zón**  3: Doklad je dán číslem trasy  **4: Doklad je dán intervalem zón**  5-7: RFU |  | 3 | POS  DD |  |
| contractPaymentMeans |  | Typ prodejní transakce dle EN1545-2. | Payment Means | 8 | POS  DD | 0x00 |
| contractPriceUnit | + | Měna a násobek ceny jízdenky  1000b – CZK v haléřích  1001b – EUR v centech | PayUnitMap | 4 | POS  DD | 1000b |
| contractPrice | + | Cena jízdenky dle contractPriceUnit | Amount (167 77 215) | 24 |  |  |
| fileNumber | + | Číslo souboru |  | 4 | POS  DD | 0 – nultý soubor  1 – první soubor  2 - …  9 - … |
| variantPart | + | Variantní část jízdenky dle *contractHasJourney*, právě jedna ze struktur   * *seasonTicketNetworkInfo* * *seasonTicketRelationInfo* * *seasonTicketZonesInfo* * *seasonTicketTraceInfo* |  | 256 |  |  |
| samNumber |  | Číslo SAM, který provedl záznam |  | 16 | POS  DD | Zapisuje pouze SAM |
| **Celkem bitů** | | | | **656** |  |  |
| **Celkem byte** | | | | **82** |  |  |

*contractTransportMeansRestriction*:

Nastavený bit 1 až 15 při nastaveném bitu 0 znamená, že v daném prostředku je jízdenka platná.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Bit*** | ***Omezení*** |  | ***Bit*** | ***Omezení*** |
| 0 | 0: Bez omezení  1: Omezení aplikováno |  | 8 | Tramvaj |
| 1 | Vlak Os, Sp, Ex |  | 9 | Trolejbus |
| 2 | Vlak R |  | 10 | RFU |
| 3 | Vlak EC, IC |  | 11 |
| 4 | Vlak SC |  | 12 |
| 5 | Lanovka |  | 13 |
| 6 | Bus |  | 14 |
| 7 | Loď |  | 15 |

V případě některých *contractPaymentMeans* nemusí mít cestující nárok na vrácení jízdného.

Vzájemné refundace mezi subjekty musí řešit následné systémy, není předmětem Struktur BČK IREDO.

#### Datová struktura seasonTicketContract

| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- | --- |
| contractFlags |  | Příznaky upřesňující typ dokladu (zjednodušení číselníků). Viz komentář pod tabulkou. | INT2 | 16 | POS  DD | 0x00 |
| contractAmount | + | Počet cestujících (zavazadel atp.) zde popsaného tarifu, profilu a příznaku. | Amount (15) | 4 | POS  DD |  |
| contractTariffProfile | + | Kód určující tarif kupónu relativně v rámci daného profilu zákazníka a transportní sítě. |  | 6 | POS  DD |  |
| contractCustomerProfile | + | Kód klasifikující kupón dle určitých kritérií. Profil zákazníka popisuje zákazníka (např. důchodce). | ProfileCodeIOP | 6 | POS  DD |  |
| **Celkem** | | | | 32 |  |  |

Význam *contractFlags:*

|  |  |
| --- | --- |
| ***Bit*** | ***Vlastnost*** |
| 0 | 1: Jízdenka je zpáteční. Týká se všech jízdenek s *contractHasJourney = 2 a 0*. Jízdenka může být uznána i v opačném směru oproti údajům, uloženým v *seasonTicketRelationInfo*. |
| 1–5 | Číslo průkazu v aplikaci Průkazy, který je potřeba ověřit pro ověření platnosti jízdenky. Vlastní ověření je dáno aplikační logikou daného průkazu, je nad rámec specifikace elektronické jízdenky. |
| 6 | Byl zakoupen přestupní lístek |
| 7–15 | RFU |

Smyslem zavedení položky *contractFlags* je minimalizace číselníků dokladů a typů.

#### Datová struktura seasonTicketNetworkInfo– použito v IREDO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| contractNetworkID | + | Identifikace sítě, v níž je jízdenka platná | NetworkID | 24 | POS  DD | 203522 |
| RFU |  |  |  | 232 | POS  DD |  |
| **Celkem** | | | | **256** |  |  |

#### Datová struktura seasonTicketRelationInfo – použito v IREDO

***V IREDO použito pro:***

***1: Doklad je dán relací (Z, Do, Přes).***

***4: Doklad je dán intervalem zón.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| contractNetworkID | + | Identifikace sítě, k níž jsou vztaženy stanice (zóny) | NetworkID | 24 | POS  DD | 203522 |
| contractDistance |  | Počet kilometrů | Amount (255) | 8 | POS  DD |  |
| contractTransferEndDate |  | Datum, do kdy lze přestoupit na následný spoj | DateStamp | 14 | POS  DD |  |
| contractTransferEndTime |  | Čas, do kdy lze přestoupit na následný spoj | TimeStamp | 11 | POS  DD |  |
| contractJourneyViaCount |  | Počet stanic (zón) „přes“, 0 až 5 | Amount (255) | 8 | POS  DD |  |
| contractJourneyElemSize | + | Velikost jedné datové položky (reprezentace stanice, zóny) v bitech – *ElemS*, zmenšená o 1 (tedy z rozsahu 1 až 32 bitů).  Zda se jedná o stanice nebo zóny je dáno sítí (contractNetworkID) | Amount (32) | 5 | POS  DD | 01111b |
| RFU |  |  |  | 2 | POS  DD |  |
| contractjourney | + | Stanice / zóna Z, Do a pole stanic / zón přes (0 až contractJourneyViaCount), každá o velikosti *ElemS* | OCTET STRING (23) | 184 | POS  DD |  |
| **Celkem** | | | | **256** |  |  |

**Poznámky:**

Počty zón:

|  |  |  |
| --- | --- | --- |
| **Nejvyšší číslo zóny** | ***ElemSize*** | **Počet zón uložitelných do *seasonTicketZonesInfo*** |
| 127 | 7 | až 26 |
| 255 | 8 | až 23 |
| 511 | 9 | až 20 |
| 1023 | 10 | až 18 |
| 2047 | 11 | až 16 |
| 4095 | 12 | až 15 |
| … | … | … |
| **65535** | **16** | **Až 11, využito pro IREDO** |

Příklad pro IREDO:

Jízdenka platná mezi zónami 343, 581

contractJourney : ‘0000000101010111**0000001001000101**’b

#### Datová struktura seasonTicketZonesInfo – použito v IREDO

| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- | --- |
| contractNetworkID | + | Identifikace sítě, k níž jsou vztaženy zóny (od sítě se odvíjí max. velikost čísla zóny a počet uložených zón) | NetworkID | 24 | POS  DD | 203522 |
| contractDistance |  | Počet kilometrů | Amount (255) | 8 | POS  DD |  |
| contractTransferEndDate |  | Datum, do kdy lze přestoupit na následný spoj | DateStamp | 14 | POS  DD |  |
| contractTransferEndTime |  | Čas, do kdy lze přestoupit na následný spoj | TimeStamp | 11 | POS  DD |  |
| contractJourneyZonesCount | + | Počet zón v seznamu | Amount (255) | 8 | POS  DD | Udává počet zón v položce contractJourneyZones |
| contractJourneyElemSize | + | Velikost jedné datové položky (reprezentace stanice, zóny) v bitech – *ElemS*, zmenšená o 1 (tedy z rozsahu 1 až 32 bitů) | Amount (32) | 5 | POS  DD |  |
| RFU |  |  |  | 2 |  |  |
| contractJourneyZones |  | Pole Zón přes | OCTET STRING (23) | 184 | POS  DD |  |
| **Celkem** |  |  |  | **256** |  |  |

#### Datová struktura seasonTicketTraceInfo

| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- |
| contractNetworkID | Identifikace sítě, k níž jsou vztaženy zóny (od sítě se odvíjí max. velikost čísla zóny a počet uložených zón) | NetworkID | 24 | POS  DD |  |
| contractDistance | Počet kilometrů na kolik je jízdenka platná | Amount (255) | 8 | POS  DD |  |
| contractTransferEndDate | Datum, do kdy lze přestupit na následný spoj | DateStamp | 14 | POS  DD |  |
| contractTransferEndTime | Čas, do kdy lze přestupit na následný spoj | TimeStamp | 11 | POS  DD |  |
| ticketJourneyLine | Číslo linky, kde je jízdenka platná | INT4 | 32 | POS  DD |  |
| ticketJourneyConnection | Číslo spoje | INT4 | 32 | POS  DD |  |
| RFU |  |  | 135 |  |  |
| **Celkem** |  |  | **256** |  |  |

### Soubor Kontrola jízdenky

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***10 - 14*** | ***ticketPliersFile*** | | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Typ*** | ***Typ editace*** | ***Hodnota (popis)*** | | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 | |
| Status souboru | | 8 |  | KC | 7 (Ok) | |
| ticketCheck | | 240 | Struktura ticketPliersInfo |  |  | |
| Využito | | 256 |  | | |
| RFU | | 0 |  | | |
| Celkem B | | 32 | (= 1 × 32 B) | | |

#### Struktura ticketPliersInfo

| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- |
| contractNetwork | Identifikace transportní sítě do které patří provozovatel | NetworkId | 24 | DD |  |
| contractProvider | Kód provozovatele, který zkontroloval jízdenku | ProviderID | 8 | DD |  |
| ticketCheckInDevice | Číslo kontrolujícího místa (terminálu) | INT4 | 32 | DD |  |
| ticketCheckInDate | Datum provedeného označení | DateStamp | 14 | DD |  |
| ticketCheckInTime | Čas provedeného označení | TimeStamp | 11 | DD |  |
| ticketCheckInLine | Číslo linky, ve kterém došlo k označení | INT3 | 24 | DD |  |
| ticketCheckInRoute | Číslo spoje, ve kterém došlo k označení | INT3 | 24 | DD |  |
| ticketCheckInBus | Číslo vozidla, ve kterém došlo k označení | INT4 | 32 | DD |  |
| ticketCheckInZone | Číslo zóny, ve které došlo k označení | INT3 | 24 | DD |  |
| ticketCheckInStop | Číslo stanice, ve které došlo k označení | INT4 | 32 | DD |  |
| ticketCross | Počítadlo přestupů |  | 4 | DD |  |
| ticketCounter | Počítadlo jízd na jeden kupón |  | 11 | DD | 0x00 |
| **Celkem bitů** |  |  | **240** |  |  |

### Soubor Místenka

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***15 - 17*** | ***seatReservationTicketFile*** | | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Typ*** | ***Typ editace*** | ***Hodnota (popis)*** | | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 | |
| Status souboru | | 8 |  | KC | 7 (Ok) | |
| Typ podpisu | | 4 |  | KC | 0 | |
| Typ šifrování | | 4 |  | KC | 0 | |
| RFU | | 8 |  | KC | volné místo vyplněné '0'B | |
| seatReservation | | 160 | Struktura seatReservationTicketInfo |  |  | | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | KC | 0 | |
| Využito | | 256 |  | | |
| RFU | | 0 |  | | |
| Celkem B | | 32 | (= 1 × 32 B) | | |

#### Struktura seatReservationTicketInfo

| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- |
| seatValidityStartDate | Počátek platnosti – datum | DateStamp | 14 | POS  DD |  |
| seatValidityStartTime | Počátek platnosti – čas | TimeStamp | 11 | POS  DD |  |
| contractLineRestriction | Číslo linky, ve které je místenka platná (0 = bez omezení) | INT3 | 24 | POS  DD |  |
| contractRouteRestriction | Číslo spoje, ve které je místenka platná (0 = bez omezení) | INT3 | 24 | POS  DD |  |
| contractVehicleRestriction | Číslo vozu, ve kterém je místenka platná (0 bez omezení) | INT3 | 16 | POS  DD |  |
| contractVehicleClassCodeRestriction | Povolená vozová třída (v závislosti na dopravním prostředku) 0: bez omezení  1: 1. třída nebo její ekvivalent  2: 1. i 2. třída nebo jejich ekvivalent  3: RFU  Lze dokoupit i místenku na vyšší třídu než je jízdenka |  | 2 | POS  DD |  |
| contractPaymentMeans | Typ prodejní transakce. (viz výše) | Payment Means | 4 | POS  DD |  |
| contractSeatCount | Počet místenek v souboru |  | 3 | POS  DD |  |
| contractSeatPlace1Restriction | Číslo místa1 ve vozidle, na kterém je místenka platná | INT1 | 8 | POS  DD |  |
| contractSeatPlace2Restriction | Číslo místa2 ve vozidle, na kterém je místenka platná | INT1 | 8 | POS  DD |  |
| contractSeatPlace3Restriction | Číslo místa3 ve vozidle, na kterém je místenka platná | INT1 | 8 | POS  DD |  |
| contractSeatPlace4Restriction | Číslo místa4 ve vozidle, na kterém je místenka platná | INT1 | 8 | POS  DD |  |
| seatPriceUnit | Měna a násobek ceny místenky  ‘1000‘B – CZK v haléřích  ‘1001‘B – EUR v centech | PayUnitMap | 4 | POS  DD | ‘1000‘B |
| seatPrice | Cena místenky dle contractPriceUnit | Amount (167 77 215) | 24 | POS  DD |  |
| RFU |  |  | 2 |  |  |
| **Celkem bitů** |  |  | **160** |  |  |

### Klíče

| ***Klíč*** | ***Název*** | ***Význam*** |
| --- | --- | --- |
| #0 | ORE\_1206\_0 | Master – klíč aplikace |
| #1 | ORE\_1206\_1 | Čtení jízdenky 1 – 10, Kontroly jízdenky 1 – 5, Místenky 1 - 2 |
| #2 | ORE\_1206\_2 | Čtení/zápis jízdenky 1 – 5, Místenky 1 – 2 |
| #3 | ORE\_1206\_3 | Čtení/zápis Kontroly jízdenek 1 – 5 |
| #4 | ORE\_1206\_4 | Čtení/zápis jízdenky 6 – 10 |
| #5 | ORE\_1206\_5 | RFU |

#### Přístupová práva souborů

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Soubor*** | ***Název*** | ***Read*** | ***Write*** | ***Read & Write*** | ***Change***  ***Access Rights*** |
| 0 | Jízdenka 1 | #1 | #0 | #2 | #0 |
| 1 | Jízdenka 2 | #1 | #0 | #2 | #0 |
| 2 | Jízdenka 3 | #1 | #0 | #2 | #0 |
| 3 | Jízdenka 4 | #1 | #0 | #2 | #0 |
| 4 | Jízdenka 5 | #1 | #0 | #2 | #0 |
| 5 | Jízdenka 6 | #1 | #0 | #4 | #0 |
| 6 | Jízdenka 7 | #1 | #0 | #4 | #0 |
| 7 | Jízdenka 8 | #1 | #0 | #4 | #0 |
| 8 | Jízdenka 9 | #1 | #0 | #4 | #0 |
| 9 | Jízdenka 10 | #1 | #0 | #4 | #0 |
| 10 | Kontrola jízdenky 1 | #1 | #0 | #3 | #0 |
| 11 | Kontrola jízdenky 2 | #1 | #0 | #3 | #0 |
| 12 | Kontrola jízdenky 3 | #1 | #0 | #3 | #0 |
| 13 | Kontrola jízdenky 4 | #1 | #0 | #3 | #0 |
| 14 | Kontrola jízdenky 5 | #1 | #0 | #3 | #0 |
| 15 | Místenka 1 | #1 | #0 | #2 | #0 |
| 16 | Místenka 2 | #1 | #0 | #2 | #0 |

## Aplikace Elektronická peněženka (EP) – 88AD

* AID aplikace – 88AD,
* obsahuje 4 soubory,
* v tomto dokumentu jsou popsány pouze struktury EP na BČK IREDO. Operacemi prováděnými s EP se zabývá zvláštní dokument.

### Soubor Nastavení EP

Soubor popisuje základní vlastnosti EP, dané typicky legislativou.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***0*** | ***walletSettingsFile*** | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Typ*** | ***Typ editace*** | ***Hodnota (popis)*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | KC | 1 |
| Status souboru | | 8 |  | KC | 7 – status EP OK |
| Typ podpisu | | 4 |  | KC | 0 |
| Typ šifrování | | 4 |  | KC | 0 |
| logVersion | | 4 | Verze souboru logů | KC | 1 |
| RFU | | 36 |  | KC | volné místo vyplněné '0'B |
| walletInfo | | 384 | Struktura walletSettingsInfo |  |  | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | KC | 0 |
| Využito | | 512 |  | |
| RFU | | 0 |  | |
| Celkem B | | 64 | (= 2 × 32 B) | |

#### Struktura walletSettingsInfo

| ***Proměnná*** | ***P*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- | --- |
| contractNetwork | + | Identifikace transportní sítě do které patří vydavatel EP | NetworkId | 24 | POS | 203522 |
| contractProvider | + | Kód vydavatele EP | ProviderID | 8 | POS | 124 |
| maxValueEP | + | Maximální hodnota EP  Pro CZK s exponentem 2 nastaveno na 450 000 | INT4 | 32 | KC | 450 000 |
| minValueEP | + | Minimální hodnota EP  Nastaveno na 0 | INT4 | 32 | KC | 0 |
| maxDebet | + | Maximální výše povoleného debetu | INT4 | 32 | KC | 0 – neomezeno |
| maxOnePay | + | Maximální výše dobití | INT4 | 32 | KC | 0 – bez limitu |
| expirationDate | + | Datum expirace platnosti EP | DateStamp | 14 | POS | Nastaveno dle platnosti BČK IREDO |
| allowedDebet | + | Povolený debet  ‘00‘B – debet povolen  ‘01‘B – debet zakázán |  | 2 | KC  POS | ‘00’B |
| baseCurrencyEP | + | Měna EP dle EN 1545  ‘1000‘B – CZK v haléřích | PayUnitMap | 4 | KC | ‘1000’B |
| RFU |  |  |  | 204 |  |  |
| **Celkem bitů** | | | | **384** |
| **Celkem byte** | | | | **48** |

### Soubor Osobní nastavení EP

Soubor popisuje aktuální uživatelské nastavení EP.

Se souborem se v návrhu nepracuje, slouží pro případné budoucí využití.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***1*** | ***walletPersonalSettingsFile*** | | | | | | ***Standard Data File*** |
| ***Název*** | | ***Bitů*** | ***Typ*** | | ***Typ editace*** | ***Hodnota (popis)*** | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | | KC | 1 |
| Status souboru | | 8 |  | | KC | 7 |
| Typ podpisu | | 4 |  | | KC | 0 |
| Typ šifrování | | 4 |  | | KC | 0 |
| RFU | | 40 |  | | KC | volné místo vyplněné '0'B |
| walletInfo | | 128 | Struktura walletPersonalSettingsInfo | |  |  | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | | POS  DD |  |
| Využito | | 256 |  |
| RFU | | 0 |  |
| Celkem B | | 32 | (= 1 × 32 B) |

#### Struktura walletPersonalSettingsInfo

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| walletPersNetwork | Identifikace transportní sítě, do které patří společnost, která záznam provedla | NetworkId | 24 | POS  DD | 203522 |
| walletPersProvider | Společnost, která záznam provedla | ProviderID | 8 | POS  DD |  |
| walletPersCreditTransaction | Číslo transakce kreditu předplacené transakce | INT4 | 32 | POS  DD |  |
| walletPersDate | Datum zápisu souboru | DateStamp | 14 | POS  DD |  |
| walletPersTime | Čas zápisu souboru | TimeStamp | 11 | POS  DD |  |
| walletStatus | Status EP dle ČSN EN 1546-1 |  | 8 | POS | 7 |
| RFU |  |  | 31 |  |  |
| **Celkem bitů** | | | **128** |
| **Celkem byte** | | | **16** |

### Hodnota EP

Hodnotový soubor bude vytvořen bez horního limitu.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***2*** | ***valueEPFile*** | | | ***Value File*** |
| ***Název*** | | ***Bitů*** | ***Typ*** |  |
| valueEP | | 32 | INT32 - Aktuální hodnota EP |
| Využito | | 32 |  |  |
| Nevyužitelné | | 224 |  | |
| Celkem B | | 32 | (= 1 × 32 B) | |

### Log EP

Počet níže popsaných záznamů v souboru je 6, počet posledních uchovávaných transakcí je 5. Soubor typu CRF.

| ***3*** | ***logEPFile*** | | | | | | ***Cyclic Record File*** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Název*** | | ***Bitů*** | ***Typ*** | ***Typ editace*** | ***Hodnota (popis)*** | | Nešifrovaná oblast souboru |
| Verze | | 8 | INT1 | POS  DD | 1 | |
| Status souboru | | 8 |  | POS  DD | 7 | |
| Typ podpisu | | 4 |  | POS  DD | 3 (3DES-CBC-MAC8) | |
| Typ šifrování | | 4 |  | POS  DD | 0 | |
| RFU | | 0 |  | POS  DD |  | |
| Log | | 168 | Struktura logEPInfo |  |  | | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | POS  DD | Struktura od Verze po Log + **UID + 0x00** podepsána klíčem ORE\_88AD\_SIGN | |
| Využito 1 záznam | | 256 |  | | |
| Nevyužito v souboru | | 0 |  | | |
| Celkem soubor B | | 224 | (= 7 × 32 B) | | |

#### Struktura logEPInfo

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| counterEP | Pořadové číslo transakce v rámci EP na konkrétní BČK IREDO. | INT3 | 24 | POS  DD |  |
| prevValueEP | Hodnota EP před transakcí | INT4 | 32 | POS  DD |  |
| changeEP | Hodnota transakce | INT4 | 32 | POS  DD |  |
| changeDevice | Číslo zařízení, které provedlo záznam | INT4 | 32 | POS  DD |  |
| samNumber | Číslo SAM, který provedl záznam |  | 16 | POS  DD | Zapisuje SAM |
| dateEP | Datum transakce EP | DateStamp | 14 | POS  DD |  |
| timeEP | Čas transakce EP | TimeStamp | 11 | POS  DD |  |
| typeEP | Typ operace 0 – inicializováno 1 – Debet 2 – Credit 3 – Limited credit |  | 4 | POS  DD |  |
| RFU |  |  | 3 |  |  |
|  |  |  |  |  |  |
| **Celkem bitů** | | | **168** |  |  |
| **Celkem byte** | | | **21** |  |  |

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_88AD\_0 | Master – klíč aplikace |
| #1 | ORE\_88AD\_1 | Čtení souboru nastavení EP a osobní nastavení EP, Log EP |
| #2 | ORE\_88AD\_2 | Zápis souboru nastavení EP |
| #3 | ORE\_88AD\_3 | Čtení, debet (dekrementace) a limited credit souboru hodnota EP, zápis Log EP |
| #4 | ORE\_88AD\_4 | Kredit (inkrementace) souboru hodnota EP |
| #5 | ORE\_88AD\_5 | Zápis souboru osobního nastavení |

#### Přístupová práva souborů

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Soubor*** | ***Název*** | ***Read*** | ***Write*** | ***Read & Write*** | ***Change***  ***Access Rights*** |
| 0 | Nastavení EP | #1 | #0 | #2 | #0 |
| 1 | Osobní nastavení EP | #1 | #0 | #5 | #0 |
| 2 | Hodnota EP | #3 | #3 | #4 | #0 |
| 3 | Log EP | #1 | #0 | #3 | #0 |

## Rezerva 1 - 0743

Aplikace „Rezerva 1“:

* AID aplikace – 0743,
* neobsahuje žádné soubory,
* slouží jako rezervní aplikace.

### Struktura

* Není definována

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_0743\_0 | Master – klíč aplikace |
| #1 | ORE\_0743\_1 | RFU |
| #2 | ORE\_0743\_2 | RFU |
| #3 | ORE\_0743\_3 | RFU |
| #4 | ORE\_0743\_4 | RFU |
| #5 | ORE\_0743\_5 | RFU |

## Rezerva 2 - 1207

Aplikace „Rezerva 2“:

* AID aplikace – 1207,
* neobsahuje žádné soubory,
* slouží jako rezervní aplikace.

### Struktura

* Není definována

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_1207\_0 | Master – klíč aplikace |
| #1 | ORE\_1207\_1 | RFU |
| #2 | ORE\_1207\_2 | RFU |
| #3 | ORE\_1207\_3 | RFU |
| #4 | ORE\_1207\_4 | RFU |
| #5 | ORE\_1207\_5 | RFU |

## Rezerva 3 - 0744

Aplikace „Rezerva 3“:

* AID aplikace – 0744,
* neobsahuje žádné soubory,
* slouží jako rezervní aplikace.

### Struktura

* Není definována

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_0744\_0 | Master – klíč aplikace |
| #1 | ORE\_0744\_1 | RFU |
| #2 | ORE\_0744\_2 | RFU |
| #3 | ORE\_0744\_3 | RFU |

## Rezerva 4 – 100B - DOPR

Aplikace „Rezerva 4“:

* AID aplikace – **00100B,**
* neobsahuje žádné soubory,
* slouží jako rezervní aplikace.

### Struktura

* Není definována

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_100B\_0 | Master – klíč aplikace |
| #1 | ORE\_100B\_1 | RFU |
| #2 | ORE\_100B\_2 | RFU |
| #3 | ORE\_100B\_3 | RFU |

## Rezerva 5 – 0004 - PA

Aplikace „Rezerva 5“:

* AID aplikace – **000004,**
* neobsahuje žádné soubory,
* slouží jako rezervní aplikace.

### Struktura

* Není definována

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_0004\_0 | Master – klíč aplikace |
| #1 | ORE\_0004\_1 | RFU |
| #2 | ORE\_0004\_2 | RFU |
| #3 | ORE\_0004\_3 | RFU |
| #4 | ORE\_0004\_4 | RFU |
| #5 | ORE\_0004\_5 | RFU |
| #6 | ORE\_0004\_6 | RFU |
| #7 | ORE\_0004\_7 | RFU |
| #8 | ORE\_0004\_8 | RFU |
| #9 | ORE\_0004\_9 | RFU |

## Rezerva 6 – 883D - MEP

Aplikace „Rezerva 6“:

* AID aplikace – **00883D,**
* neobsahuje žádné soubory,
* slouží jako rezervní aplikace.

### Struktura

* Není definována

### Klíče

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | ORE\_883D\_0 | Master – klíč aplikace |
| #1 | ORE\_883D\_1 | RFU |
| #2 | ORE\_883D\_2 | RFU |
| #3 | ORE\_883D\_3 | RFU |
| #4 | ORE\_883D\_4 | RFU |
| #5 | ORE\_883D\_5 | RFU |

# Použité normativní dokumenty

*ČSN EN 1545–1 : Systémy identifikačních karet – Aplikace pro povrchovou dopravu – Část 1: Základní datové typy, všeobecný seznam kódů a datových prvků*. Praha : Český normalizační institut, 2006. 98 s.

*ČSN EN 15320 : Systémy s identifikačními kartami – Rozhraní přepravy – Interoperabilita veřejné přepravy osob – Struktura (IOPTA)*. Praha : Český normalizační institut, 2008. 152 s.

*ČSN EN ISO 24014–1 : Interoperabilní systém managementu jízdného – Část 1: Architektura*. Praha : Český normalizační institut, 2007. 76 s.

*ČSN EN 1546–1 : Systémy s identifikačními kartami – Mezioborová elektronická peněženka – Část 1: Definice, pojmy a struktury*. Praha : Český normalizační institut, 1999. 36 s.

*ČSN EN 1546–2 : Systémy s identifikačními kartami – Mezioborová elektronická peněženka – Část 2: Bezpečnostní architektura*. Praha : Český normalizační institut, 2000. 106 s.

*ČSN EN 1546–3 : Systémy s identifikačními kartami – Mezioborová elektronická peněženka – Část 3: Datové prvky a výměny*. Praha : Český normalizační institut, 2000. 72 s.

*ČSN EN 1546–4 : Systémy s identifikačními kartami – Mezioborová elektronická peněženka – Část 4: Datové objekty*. Praha : Český normalizační institut, 2000. 36s.

*ČSN ISO/IEC 5218 : Informační technologie – Kódy pro prezentaci lidského pohlaví*. Praha : Český normalizační institut, 2006. 24s.

*ČSN ISO 4217 : Kódy pro měny a fondy*. Praha : Český normalizační institut, 2002. 20s.

*ČSN ISO/IEC 11770–1 : Informační technologie – Bezpečnostní techniky – Správa klíčů – Část 1: Struktura*. Praha : Český normalizační institut, 1998. 28s.

*ČSN ISO/IEC 11770–2 : Informační technologie – Bezpečnostní techniky – Správa klíčů – Část 2: Mechanismy používající symetrické techniky*. Praha : Český normalizační institut, 1999. 24s.

*ČSN ISO/IEC 11770–3 : Informační technologie – Bezpečnostní techniky – Správa klíčů – Část 3: Mechanismy používající asymetrické techniky*. Praha : Český normalizační institut, 2002. 44s.

*ČSN ISO/IEC 15946–1 : Informační technologie – Bezpečnostní techniky – Kryptografické techniky založené na eliptických křivkách – Část 1: Všeobecně*. Praha : Český normalizační institut, 2005. 32s.

*ČSN ISO/IEC 15946–2 : Informační technologie – Bezpečnostní techniky – Kryptografické techniky založené na eliptických křivkách – Část 2: Digitální podpisy*. Praha : Český normalizační institut, 2006. 32s.

*ČSN ISO/IEC 7816–5 : Identifikační karty – Karty s integrovanými obvody – Část 5: Registrace poskytovatelů aplikací*. Praha : Český normalizační institut, 2005. 12s.

*ČSN ISO/IEC 7816–6 : Identifikační karty – Karty s integrovanými obvody – Část 6: Mezioborové datové prvky pro výměnu*. Praha : Český normalizační institut, 2005. 24s.

*AN10787 MIFARE Application Directory (MAD) Rev. 04 — 5 March 2009*