|  |  |  |
| --- | --- | --- |
|  | | |
| Karta IDS ZK | | |
| Příloha č. 5 Smlouvy o přistoupení k IDS ZK | | |
|  | | |
|  | | |
|  | | |
| **Zlín, červen 2020** |  |

OBSAH

[1 Základní Povinnosti Dopravce 2](#_Toc50566985)

[1.1 Linkový Dopravce je v souvislosti s Kartou IDS ZK povinen zejména: 2](#_Toc50566986)

[1.2 Drážní Dopravce je v souvislosti s Kartou IDS ZK povinen zejména: 2](#_Toc50566987)

[2 Výroba karet 2](#_Toc50566988)

[3 Nosič elektronického jízdného a elektronických peněz 2](#_Toc50566989)

[3.1 Povinnosti Linkového Dopravce při vydávání Karet IDS ZK 3](#_Toc50566990)

[3.2 Povinnosti Drážního Dopravce při vydávání Karet IDS ZK 5](#_Toc50566991)

[4 KartA IDS ZK 7](#_Toc50566992)

[4.1 Definice zkratek a pojmů použitých v této kapitole 7](#_Toc50566993)

[4.2 Specifikace použitých datových typů 7](#_Toc50566994)

[4.3 Struktura popisovaných aplikací 8](#_Toc50566995)

[4.4 Struktura Karty IDS ZK 9](#_Toc50566996)

# Základní Povinnosti Dopravce

## Linkový Dopravce je v souvislosti s Kartou IDS ZK povinen zejména:

1. na své vlastní náklady zajistit změnu profilu cestujícího v datech na čipu. Dodání Karet IDS ZK a elektronickou personalizaci, tedy vytvoření struktury na kartě zajistí KOVED. Tato struktura karty je uvedena v kapitole 5, tohoto dokumentu. SW pro správu karet dodá KOVED,
2. zajistit proces zpracování objednávky (žádost cestujícího), prodej a distribuci Karet IDS ZK v Informačních kancelářích dopravce,
3. Plnit všechny povinnosti uvedené v kapitole 3.1 „Povinnosti Linkového Dopravce při vydávání Karet IDS ZK“.

Další povinnosti Dopravce jsou uvedeny ve zbývajících kapitolách tohoto dokumentu. Dopravce je povinen dodržovat veškeré povinnosti, postupy a parametry stanovené Koordinátorem v tomto dokumentu.

## Drážní Dopravce je v souvislosti s Kartou IDS ZK povinen zejména:

1. Zajistit proces příjmu žádosti o vydání nové Karty IDS ZK v Informačních kancelářích Dopravce a následné dodání těchto žádostí na KOVED.
2. Plnit všechny povinnosti uvedené v kapitole 3.2 „Povinnosti Drážního Dopravce při vydávání Karet IDS ZK“.

Další povinnosti Dopravce jsou uvedeny ve zbývajících kapitolách tohoto dokumentu. Dopravce je povinen dodržovat veškeré povinnosti, postupy a parametry stanovené Koordinátorem v tomto dokumentu.

# Výroba karet

Výrobu Karet IDS ZK bude zajišťovat KOVED na své vlastní náklady.

# Nosič elektronického jízdného a elektronických peněz

Základním nosičem elektronických jízdních dokladů a základním platebním prostředkem umožňujícím odbavení cestujících odbavovacím zařízením je Karta IDS ZK, jejíž vydávání cestujícím zajišťuje Dopravce přes Informační kanceláře a KOVED přes E-shop.

Karta IDS ZK je plně kompatibilní (absolutně kompatibilní bez jakýchkoliv výjimek) s bezkontaktní čipovou kartou MIFARE DESFire EV1 a MIFARE DESFire EV3, velikost paměti 8 kB. V rámci mezikrajské spolupráce je struktura karty ODISka a Karty IDS ZK totožná a plně kompatibilní. Jediný rozdíl je v číslu sítě a číslu vydavetele.

**Typy vydávaných Karet IDS ZK**

**Varianty Karet IDS ZK**

KOVED bude vydávat karty ve variantách:

1. **Přenosná karta**

Přenosná karta je určena pro libovolného cestujícího a její vydání ani používání není podmíněno zpracováním osobních údajů cestujícího žádajícího o vydání karty nebo Uživatele karty. Jediným evidovaným identifikátorem této karty je identifikační číslo karty. Ke každé kartě bude držiteli vydán tzv. protokol o převzetí karty, který bude určen k prokázání vlastnictví konkrétní čipové karty. Rovněž tento certifikát neobsahuje žádné osobní údaje Uživatele karty.

V případě nutnosti řešení procesů životního cyklu karty, jako je například blokace, zrušení, převod elektronických peněz zpět na hotovost atp. musí být předložen vydaný protokol o převzetí karty. Bez něj nebude provedení jakéhokoliv procesu s kartou možné.

1. **Osobní karta**

Osobní karta je určena pro konkrétního cestujícího a její vydání je podmíněno souhlasem se zpracováním osobních údajů žádajícího cestujícího o její vydání, které se budou zpracovávat pouze za účelem výroby karty. Karta obsahuje kromě evidenčního čísla také další osobní údaje, jako jsou fotografie, jméno, příjmení a datum narození Uživatele karty.

Analogicky k přenosné kartě bude také k osobní kartě vydáván protokol o převzetí karty, kterým bude Uživatel karty při řešení procesů životního cyklu karty prokazovat vlastnictví konkrétní karty.

## Povinnosti Linkového Dopravce při vydávání Karet IDS ZK

1. Dopravce je povinen provozovat definovaný počet Informačních kanceláří tak, jak určuje dokument „Technické a provozní standardy“, který tvoří přílohu č. 5 Smlouvy o veřejných službách. Tato prodejní místa budou zajišťovat příjem žádostí o vydání čipové karty, distribuce čipové karty, jakož i další procesy související s životním cyklem čipové karty.
2. Při vydávání Karet IDS ZK je Dopravce povinen pracovat s osobními údaji žadatele v co nejmenším rozsahu nutném pro vydání osobní Karty IDS ZK, a to pouze po dobu potřebnou pro vydání Karty IDS ZK. Procesy musí splňovat požadavky zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění.
3. Dopravce nesmí vést žádnou nepovolenou evidenci osobních údajů držitelů Karet IDS ZK ve smyslu zákona o ochraně osobních údajů.
4. Procesy odbavení, odbavovací zařízení a procesy evidence údajů z odbavovacích zařízení musí splňovat požadavky zákona o ochraně osobních údajů (odbavovací systém Dopravce bude zpracovávat osobní údaje Uživatelů karet jiných vydavatelů).
5. Ke každé Kartě IDS ZK musí být současně vydán protokol o převzetí karty, prokazující Uživateli karty práva k příslušné čipové kartě.
6. Pro případ ztráty Karty IDS ZK, jejího odcizení či jiné situace vyžadující znemožnění použití karty k tomu neoprávněnou třetí osobou bude KOVED vydávat a aktualizovat Blacklist.
7. Doba platnosti Karet IDS ZK bude vydavatelem nastavena na dobu šesti (6) let od data výroby konkrétní Karty IDS ZK.
8. Dopravce je povinen vydávat Karty IDS ZK a poskytovat další služby související s celým životním cyklem karet za ceny, které nepřesáhnou maximální ceny, které stanovuje Koordinátor. Ceník pro vydání Karet IDS ZK a související služby tvoří přílohu č. 7 Smlouvy. Dopravce bude povinen po přijetí žádosti o vydání Karty IDS ZK vydat Uživateli karty plně funkční Kartu IDS ZK ve lhůtě, která nepřesáhne o více než 7 dnů lhůtu, v níž bude KOVED garantovat Dopravci dodání Karty IDS ZK.
9. Dopravce je v souvislosti s vydáváním Karty IDS ZK povinen naplňovat veškeré podmínky zákona č. 139/2011 Sb. kterým se mění zákon č. 284/2009 Sb., o platebním styku, ve znění zákona č. 156/2010 Sb., a některé další zákony platné pro vydavatele elektronických peněž a dodržovat veškeré zákonné povinnosti s vydáváním elektronických peněz související. V souvislosti s EP platí, že:

* užíváním elektronického peněžního prostředku nahraného na Kartu IDS ZK se rozumí bezhotovostní platby jízdenek a nabíjení elektronických peněženek na Kartu IDS ZK v dopravních prostředcích, Informačních kancelářích dopravce, příjemců nebo osoby, která je smluvně oprávněna nabíjet tyto elektronické peněžní prostředky.

1. Dopravce je podle zákona o platebním styku povinen provádět zpětnou výměnu elektronických peněz uložených na Kartách IDS ZK podle Smlouvy jejím Uživatelům. Porušením této povinnosti vznikne Uživateli karty vůči Dopravci peněžní pohledávka z této Smlouvy odpovídající výši částky zpětně nevyměněných elektronických peněz.
2. Dopravce je povinen vést veškeré údaje o Kartách IDS ZK vydávaných dle Smlouvy odděleně od údajů ostatních jím případně vydávaných karet.
3. Dopravce je povinen ukládat hotovost ve výši celkového zůstatku elektronických platebních prostředků vložených na Kartách IDS ZK vydávaných dle Smlouvy odděleně od hotovosti vložené do ostatních jím případně vydávaných karet (tedy na zvláštním účtu); Dopravce je v této souvislosti povinen zasílat Koordinátorovi pravidelné měsíční výpisy o zůstatku na tomto zvláštním účtu.
4. Majitelem vydávané Karty IDS ZK je KOVED.
5. V případě předčasného ukončení Smlouvy (před koncem doby plnění) je Dopravce povinen zejména:

* předat Koordinátorovi veškeré informace o Kartách IDS ZK,
* předat Koordinátorovi veškeré zůstatky z EP

## Povinnosti Drážního Dopravce při vydávání Karet IDS ZK

1. Dopravce je povinen provozovat definovaný počet Informačních kanceláří tak, jak určuje dokument „Technické a provozní standardy“, který tvoří přílohu č. 2 Smlouvy o veřejných službách. Tato prodejní místa budou zajišťovat příjem žádostí o vydání čipové karty prodej a reklamace jízdného IDZK a EP Karty IDS ZK. Nebudou zajišťovat distribuci čipových karet.
2. Dopravce nesmí vést žádnou nepovolenou evidenci osobních údajů držitelů Karet IDS ZK ve smyslu zákona o ochraně osobních údajů.
3. Procesy odbavení, odbavovací zařízení a procesy evidence údajů z odbavovacích zařízení musí splňovat požadavky zákona o ochraně osobních údajů (odbavovací systém Dopravce bude zpracovávat osobní údaje Uživatelů karet jiných vydavatelů).
4. Pro případ ztráty Karty IDS ZK, jejího odcizení či jiné situace vyžadující znemožnění použití karty k tomu neoprávněnou třetí osobou bude KOVED vydávat a aktualizovat Blacklist.
5. Doba platnosti Karet IDS ZK bude vydavatelem nastavena na dobu šesti (6) let od data výroby konkrétní Karty IDS ZK.
6. Dopravce je povinen přijímat žádosti o vydání Karty IDS ZK a v případě poskytování dalších služeb souvisejících s celým životním cyklem karet za ceny, které nepřesáhnou maximální ceny, které stanovuje Koordinátor. Ceník pro vydání Karet IDS ZK a související služby tvoří přílohu č. 7 Smlouvy. Dopravce bude povinen po přijetí žádosti o vydání Karty IDS ZK odeslat žádost na KOVED, kde bude zpracována.
7. Dopravce je povinen vést veškeré údaje o Kartách IDS ZK vydávaných dle Smlouvy odděleně od údajů ostatních jím případně vydávaných karet.
8. Dopravce je povinen ukládat hotovost ve výši celkového zůstatku elektronických platebních prostředků vložených na Kartách IDS ZK vydávaných dle Smlouvy odděleně od hotovosti vložené do ostatních jím případně vydávaných karet (tedy na zvláštním účtu); Dopravce je v této souvislosti povinen zasílat Koordinátorovi pravidelné měsíční výpisy o zůstatku na tomto zvláštním účtu.
9. Majitelem vydávané Karty IDS ZK je KOVED.
10. V případě předčasného ukončení Smlouvy (před koncem doby plnění) je Dopravce povinen zejména:

* předat Koordinátorovi veškeré informace o Kartách IDS ZK,
* předat Koordinátorovi veškeré zůstatky z EP

# KartA IDS ZK

## Definice zkratek a pojmů použitých v této kapitole

| ***Pojem*** | ***Definice*** |
| --- | --- |
| AID | Identifikátor aplikace Application Identifier ISO/IEC 7816-5:2004 |
| ČK | Čipová karta |
| ČD | České dráhy |
| DD | Odbavovací zařízení, které mají charakter odbavení zákazníka (například odbavení kupónu nebo el. peněženky na validátoru (strojku), obecná platba el. peněženkou...). DD operace s ČK jsou obecně považovány za časté a méně spolehlivé s ohledem na zápis dat na ČK |
| EP | Elektronická peněženka |
| KC | Kartové centrum, provádí grafickou a datovou personalizaci |
| HW | Hardware |
| IDS | Integrovaný dopravní systém |
| 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 |
| MSK\_CMK | Master klíč MSk |
| PAD | Příměstská autobusová doprava |
| POS | Point Of Sale - zařízení, které mají charakter POS (dobití kupónu či el. peněženky na KC nebo v automatu nebo u řidiče...). POS operace s ČK jsou obecně považovány za méně časté a více spolehlivé s ohledem na zápis dat na ČK |
| 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 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 kartě)

*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 dipozici v nešifrované velikosti souboru, může být definováno nebo RFU

*Proměnné 2*: 16 + n × 32 byte šifrovaného obsahu souboru. Zaokrouhlení na 32 byte je z důvodů omezení vnitřní fragmentace souborů DESFire karet. 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 kartách, tak i v různých aplikací stejné karty.

## Struktura Karty IDS ZK

V následujících kapitolách a článcích jsou obsaženy informace o Kartě IDS ZK týkající se:

* struktury aplikací/souborů a jejích formátů

Popisované struktury aplikací se týkají standardu Mifare DESFire. Karta IDS ZK je tzv. multi-aplikační bezkontaktní čipová karta, což znamená, že na jedné takovéto kartě mohou být nahrány jak aplikace vydavatele karty, tak i aplikace jiných poskytovatelů aplikací. Aplikace vydavatele jsou obecně známé ostatním poskytovatelům aplikací či subjektům akceptujícím bezkontaktní čipové karty.

Z důvodů mnoha subjektů, pracujících s kartou, jsou všechny použité datové typy co nejlépe dokumentované a zejména pak jsou převzaty z normativních dokumentů, jejichž seznam je součástí tohoto dokumentu jako kapitola 7 – Dotčené normy. Návrh je také v souladu s připravovanou vyhláškou ustanovující standardy platby a odbavení cestujících ve veřejné dopravě s využitím bezkonatktních čipových technologií.

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 Karty IDS ZK odděluje ve své paměti datové prostory tak, aby karta umožnila práci s nezávislými aplikacemi.
* Přístup k odděleným datovým prostorům je řízen podle typu operací.
* Operační systém a autentizační mechanismy Karty IDS ZK umožňují jednomu subjektu vykonávat správu obsahu karty 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.
* Karta IDS ZK umožňuje multifunkční použití, tj. paralelní umístění, užívání a správu aplikací různých subjektů.
* Karta IDS ZK nabízí kromě standardní bezpečnosti karet Mifare DESFire i vlastní nativní bezpečnostní prvky - šifrování obsahu, podpis obsahu pomocí symetrických i asymetrických kryptografických mechanismů.
* Karta IDS ZK umožňuje zavedení dodatečné bezpečnostní vrstvy prostředky, které jsou na nativních bezpečnostních mechanismech karty nezávislé.
* Karta IDS ZK umožňuje obnovovat bezpečným způsobem kryptografické klíče použité pro ochranu karty a jejich aplikací.
* Karta IDS ZK umožňuje bezpečným způsobem zapisovat na kartu nové aplikace, popř. je vymazávat.
* Datové struktury jsou navržené na základě standardu pro běžně používané technologie.
* Použité číselníky odpovídají stávajícím používaným číselníkům u ostatních Integrovaných dopravních systémů (IDS).
* Karta IDS ZK umožňuje nahrávat strukturu také na NFC mobilní telefony podporující v Secure Elementu karty Mifare DESFire

**Popis struktury Karty IDS ZK**

Struktura obsahuje 4 kompletní aplikace a 4 rezervní aplikace pro případné další dopnění struktury Karty IDS ZK.

Kompletní aplikace:

* Personalizační, tvořená 2 soubory:
  + Informace o kartě
    - Podrobněji viz. Struktura souboru Informace o kartě
  + Informace o držiteli
    - Umožnuje identifikaci držitele, podporuje ale i anonymní karty
    - Podrobněji viz. Struktura souboru Informace o držiteli
* Průkazy/Benefity
  + Obecná aplikace tvořená 5 stejným soubory s různými právy na zápis do jednotlivých souborů
  + Možné využití aplikace například pro:
    - Parkování
    - Slevová karta
    - Rezervační systém
    - Stravovací systém (SS)
    - Docházkový systém
    - Knihovní systém
    - Portál úředníka (PÚ)
    - Dopravní aplikace Českých drah
  + 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 5 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 peněženky
  + Podporuje až 4 měny
  + Podrobněji viz. Aplikace elektronická peněženka (EP)
* **Aplikace na Kartě IDS ZK**

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**

* AID aplikace – 0027
* obsahuje 2 soubory
* zahrnuje identifikační znaky vydavatele, podpis UID, informace o kartě a o držiteli karty

**Struktura souboru Informace o kartě**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***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 | 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 karty dle číselníku XXX | INT3 | 24 | KC | 179 – vydavatel KOVED |
| publisherNetworkID | Identifikace transportní sítě do které patří vydavatel karty | INT3 | 24 | KC | 203721 (dle Číselníku NetworkID & ProviderID) |
| signatureVersion | verze klíče ECDSA | INT1 | 8 | KC | 1 |
| signatureUID | privátním klíčem ECDSA podepsané UID karty – typ 8 | OCTET STRING (56) | 448 | KC | Karta IDS ZK\_0027\_ECC\_P |
| cardNumber | Logické číslo karty – dle ISO7812 |  | 72 | KC |  |
| appStartDate | Počátek platnosti karty | DateStamp | 14 | KC | datum výroby karty |
| appEndDate | Konec platnosti karty | DateStamp | 14 | KC | datum výroby karty + 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 karty 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 | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | POS | 0 |
| Využito | | 1024 |  | | |
| RFU | | 0 |  | | |
| Celkem B | | 128 | (= 4 × 32 B) | | |

**Datová struktura cardHolderInfo**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***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 Možnost využití pro identifikaci zaměstnavatele pro účely zaměstnaneckého jízdného. | BCDString | 80 | KC  POS | RFU |
| holderName | Identifikace držitele (75 B, tedy 37 až 75 znaků) | UTF8String | 600 | KC  POS | RFU |
| holderProfile1 | Profil1 držitele ČK 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 ČK 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 karta** (položky holderBirth a holderName jsou vyplněny nulami; položka holderSex je nastavena v souladu s normou na 9).
  + 1: **Personalizovaná karta** (položky holderBirth a holderSex jsou vyplněny; holderName obsahuje jméno a příjmení držitele, toto může být případně zkrácené na celé znaky).
  + 2: **Přenosná karta** (položka holderBirth je vyplněna nulami; holderSex obsahuje 9 a holderName je jménem organizace, vlastnící přenosnou kartu, holderID obsahuje identifikátor organizace).
  + 3: **Nepřenosná nepersonalizovaná karta** (holderID může obsahovat identifikaci držitele, holderName není vyplněno, položky holderBirth a holderSex jsou vyplněny).
  + 4: **Graficky personalizovaná karta** (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 karta** (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 | MSK\_0027\_0 | Master – klíč aplikace |
| #1 | MSK\_0027\_1 | Čtení souboru informace o kartě |
| #2 | MSK\_0027\_2 | Čtení/zápis souboru informace o kartě |
| #3 | MSK\_0027\_3 | Čtení souboru informace o držiteli |
| #4 | MSK\_0027\_4 | Čtení/zápis souboru informace o držiteli |
| #5 | RFU |  |

**Přístupová práva souborů**

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

**Aplikace Průkazy/Benefity**

* AID aplikace – 5346
* 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) |
| benefitNetwork | | 24 | Kód sítě | POS | 203811 |  |
| BenefitProvider | | 8 | Kód vydavatele | POS | Doplnit dle vydavatele a číselníku |
| RFU | | 8 |  | N/A | volné místo vyplněné '0'B |
| Benefit | | 128 | Datová struktura benefitInfo, Datová struktura benefitCheckInCheckOut, Datová struktura benefitBusAccess případně jiná struktura | KC | Kód definující datovou strukturu benefitu. | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | KC | 0 |
| Využito | | 256 |  | | |
| Celkem B | | 32 |  | | |
| Využito | | 256 | (= 1 × 32 B) | | |

**Datová struktura benefitInfo**

Obecná datová struktura vhodná pro použití v souboru Průkazy/Benefity, může být však nahrazena libovolnou jinou strukturou.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***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 | MSK\_5346\_0 | Master – klíč aplikace |
| #1 | MSK\_5346\_1 | Čtení souboru 1 – 5 |
| #2 | MSK\_5346\_2 | Čtení/zápis souboru 1 |
| #3 | MSK\_5346\_3 | Čtení/zápis souboru 2 |
| #4 | MSK\_5346\_4 | Čtení/zápis souboru 3 |
| #5 | MSK\_5346\_5 | Čtení/zápis souboru 4 |
| #6 | MSK\_5346\_6 | Čtení/zápis souboru 5 |
| #7 | MSK\_5346\_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 v jednotlivých souborech Průkaz/Benefit**

**Soubor 1 – CheckIn/CheckOut pro DPO**

Datová struktura benefitCheckInCheckOut

Datová struktura pro uchování kontraktů pro ChechIn CheckOut odbavení v rámci DPO. Jedná se o tři další dokupované jízdenky k lístku držitele uloženém ve struktuře seasonTicketInfo (proměnná contract1) v souboru seasonTicketFile. Zde uvedená struktura je uložena v souboru benefitFile (proměnná Benefit).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| benefitValidityEndDate | Datum platnosti do | DateStamp | 14 | POS |  |
| benefitValidityEndTime | Čas platnosti do | TimeStamp | 11 | POS |  |
| RFU |  |  | 7 | POS | volné místo vyplněné '0'B |
| contract1 | Informace o prvním profilu cestujícího. | seasonTicketContract | 32 | POS |  |
| contract2 | Informace o druhém profilu cestujícího. | seasonTicketContract | 32 | POS |  |
| contract3 | Informace o třetím profilu cestujícího. | seasonTicketContract | 32 | POS |  |
| **Celkem bitů** | | | **128** |
| **Celkem byte** | | | **16** |

**Soubor 2**

Soubor prozatím není využíván.

**Soubor 3**

Soubor prozatím není využíván.

**Soubor 4**

Soubor prozatím není využíván.

**Soubor 5 – Přístup ke strojkům v autobusech (odemykací karta)**

Datová struktura benefitBusAccess

Datová struktura pro uchování bezpečnostních informací (PIN) pro odemykání strojků v autobusech pomocí přístupové karty. Zde uvedená struktura je uložena v souboru benefitFile (proměnná Benefit).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| BenefitPIN | Hodnota PIN šifrována algoritmem ALG\_DES\_CBC\_NOPAD |  | 64 | POS |  |
| RFU |  |  | 64 |  |  |
| **Celkem bitů** | | | **128** |
| **Celkem byte** | | | **16** |

**Aplikace IDS jízdenky**

* AID aplikace - 1201
* obsahuje 5 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 slouží umožňuje výdej libovolného dokladu (jednorázového nebo časového) platného v IDS. Umožňuje i nahrání většiny jízdních dokladů dopravců mimo IDS. 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 kartu a vyměňovaných mezi jednotlivými (dopravními) subjekty. Proto nejsou na kartě zejména žádné údaje, které se vytvářejí/ověřují pouze při zpracování karty oproti centrálním systémům. Typicky není potřeba na kartu 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 Kartu IDS ZK jako datový nosič (například předložení jiného průkazu).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***0 - 4*** | ***seasonTicketFile*** | | | | | ***Backup 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/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 | Potenciálně šifrovaná oblast souboru |
| Podpis | | 64 |  | POS/DD | Struktura od Verze po seasonTicket podepsán klíčem MSK\_1201\_SIGN |
| Využito | | 768 |  | | |
| Celkem B | | 0 |  | | |
| Využito | | 96 | (= 3 × 32 B) | | |

**Datová struktura seasonTicketInfo**

| ***Proměnná*** | ***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 | 203811 |
| contractProvider | Kód provozovatele, který prodal kupón | ProviderID | 8 | POS  DD |  |
| RFU |  |  | 3 |  |  |
| couponType | Typ kupónu  0 – časový kupón  1 – krátkodobá jízdenka  2 – kilometrické jízdné  3 – jednotlivé jízdné  4 – zaměstnanecký kupón  5 .. 6 - RFU  7 - pro použití vydavatele karty |  | 3 | POS  DD |  |
| contractSaleAgent | Pokladník, který doklad prodal | INT3 | 24 | POS  DD |  |
| contractSaleDevice | Číslo prodejního místa (terminálu) | INT4 | 32 | POS  DD |  |
| contractSerialNumber | Číslo kupónu rozdělené pro kupóny(soubory 0..3) a jízdenku(soubor 4) | INT1 | 8 | POS  DD | Inkrementuje se při prodeji |
| 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) | Restrict 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 | 32 | POS  DD |  |
| contract2 | Informace o druhém profilu cestujícího. | seasonTicketContract | 32 | POS  DD |  |
| contract3 | Informace o třetím profilu cestujícího. | seasonTicketContract | 32 | POS  DD |  |
| contract4 | Informace o čtvrtém profilu cestujícího. | seasonTicketContract | 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  4-7: RFU |  | 3 | POS  DD |  |
| contractPaymentMeans | Typ prodejní transakce. Číselník pod tabulkou.  Určuje, zda je možné provést vrácení peněz při offline anulaci nebo check-out. | 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 |  |  |
| RFU |  |  | 4 |  |  |
| 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** |  |  |

*contractPaymentMeans* je jedno z nebo kombinace:

* '0000' Nespecifikováno;
* '0001' Hotovost;
* '0010' Šek;
* '0011' Kreditní/Debetní karta;
* '0100' IEP (Internet Payment);
* '0101' CTA;
* '0110' Direct Debit (elektronická peněženka);
* '0111' Fakturováno/úvěr;
* '1000' Stored Travel Rights;
* '1001' Loyalty redemption;
* '1010' Token;
* '1100' Členská výhoda;
* '1101' Automatické obnovení/prodloužení;
* '1110' Poukázka;
* '1111' Voucher;
* '00010010' Kombinace hotovost – šek;

*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 na kartě.

**Datová struktura seasonTicketContract**

| ***Proměnná*** | ***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. Číselník dle TarifProfile z „struktura\_tarifu\_KOVED\_xxx.xlsx“ |  | 6 | POS  DD |  |
| contractCustomerProfile | Kód klasifikující kupón dle určitých kritérií. Profil zákazníka popisuje zákazníka (např. důchodce). Číselník dle CustomerProfile z „struktura\_tarifu\_KOVED\_xxx.xlsx“ | 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**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| contractNetworkID | Identifikace sítě, v níž je jízdenka platná | NetworkID | 24 | POS  DD | 203811 |
| RFU |  |  | 232 | POS  DD |  |
| **Celkem** |  |  | **256** |  |  |

**Datová struktura seasonTicketRelationInfo**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| contractNetworkID | Identifikace sítě, k níž jsou vztaženy stanice (zóny) | NetworkID | 24 | POS  DD | 203811 |
| contractDistance | Počet kilometrů | Amount (255) | 8 | POS  DD |  |
| contractTransferEndDate | Datum do kdy lze přestoupit na následný spoj – pro ČD | DateStamp | 14 | POS  DD |  |
| contractTransferEndTime | Čas do kdy lze přestoupit na následný spoj – pro ČD | 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 |  |
| 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** |  |  |

**Datová struktura seasonTicketZonesInfo**

| ***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 | 203811 |
| 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 | 01000b |
| RFU |  |  | 2 |  |  |
| contractJourneyZones | Pole Zón přes | OCTET STRING (23) | 184 | POS  DD |  |
| **Celkem** |  |  | **256** |  |  |

Poznámky:

contractJourneyZonesCount je maximálně 10, jinak je contractHasJourney = 0)

U karet se zapisuje do struktury ContractJourneyElemSize vždy hodnota 8, což tedy znamená že bitová délka jedné zóny je 9bitů.

Hodnoty zón jsou fyzicky na kartě uloženy jako Big-Endian

Počty zón:

|  |  |  |
| --- | --- | --- |
| **Nejvyšší číslo zóny** | ***ElemSize*** | **Počet zón uložitelných do *seasonTicketZonesInfo*** |
| 127 | 7 | až 26 |
| 255 | 8 | až 23 |
| **511** | **9** | **až 20 – využito pro Moravskoslezskou kartu (ODISKa)** |
| 1023 | 10 | až 18 |
| 2047 | 11 | až 16 |
| 4095 | 12 | až 15 |
| … | … | … |

Příklad :

Jízdenka platná v zónách 22,230,300

contractJourneyZonesCount : 0x03

ContractJourneyZones: 0x162EB00400

Vysvětlení

0x162EB00400 se interpretuje v Big-Endian jako následující sekvence po sobě jdoucích bitů (rozděleno po oktetech, tedy po 8bitech):

* **00010110** = 0x16
* **00101110** = 0x2E
* **10110000** = 0xB0
* **00000100** = 0x04
* **00000000** = 0x00
* ....

Výše jsou barevně odděleny jednotlivé hodnoty zón, takže když spojíme jejich významově vyšší části (následující oktet) s jejich významově nižšími částmi (předchozí oktet), tak v následujících 9bitových hodnotách dostaneme zapsaná čísla zón:

* **0 00010110** = 0x016 =  **22**
* **00 0010111** = 0x017 =  **23**
* **100 101100 =** 0x12C = **300**

**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 | 203811 |
| 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 |  |
| contractJourneyZonesCount | Počet zón/zastávek v seznamu | Amount (255) | 8 | POS  DD | Udává počet zón/zastávek v položce contractJourneyZones  00000010b |
| 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 | 01000b pro zónu  11111b pro zastávku |
| contractJourneyZones | Od zóny/Do zóny  resp.  Od Zastávky/ Do zastávky | OCTET STRING (23) | 122 | POS  DD |  |
| **Celkem** |  |  | **256** |  |  |

**Soubor Kontrola jízdenky**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***5 - 9*** | ***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 | 203811 |
| 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**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***10 - 11*** | ***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 | |
| structureType | | 8 |  | KC, POS, DD | 0 – viz Struktura seatReservationTicketInfo  1 – viz Struktura FirstClassTicketInfo | |
| seatReservation | | 160 | Struktura seatReservationTicketInfo  nebo  Struktura FirstClassTicketInfo |  |  | | 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** |  |  |

**Struktura FirstClassTicketInfo**

Poznámky:

* Struktura se týká pouze souboru 11
  + Na kartě mohou být 2 místenky nebo místenka + doplatek
* Položky contractSeatPlace*X*Restriction (*X* = 1 až 4) jsou nahrazeny koncem platnosti doplatku
* Čas konce platnosti bude nastaven na půlnoc (00:00), pro doplatek platící *D* dnů by tedy poslední den platnosti měl být *D* + 1 od počátku.
* Položka contractVehicleClassCodeRestriction bude nastavena na „1“ (doplatek do 1. třídy)
* Ukládání ceny je u doplatku není nutné

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Proměnná*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| seatValidityStartDate | Počátek platnosti – datum | DateStamp | 14 | POS DD | První den, kdy doplatek platí |
| seatValidityStartTime | Počátek platnosti – čas | TimeStamp | 11 | POS DD | Pokud doplatek platí více než jeden den, pak uložena 0, jinak počátek platnosti |
| contractLineRestriction | Číslo linky, ve které je místenka platná (0 = bez omezení) | INT3 | 24 | POS DD | 0, nyní nevyužito |
| contractRouteRestriction | Číslo spoje, ve které je místenka platná (0 = bez omezení) | INT3 | 24 | POS DD | 0, nyní nevyužito |
| contractVehicleRestriction | Číslo vozu, ve kterém je místenka platná (0 bez omezení) | INT3 | 16 | POS DD | 0, nyní nevyužito |
| 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 | Dle vozové třídy doplatku (doplatek do 1. třídy tedy má uloženo 1) |
| contractPaymentMeans | Typ prodejní transakce. (viz. výše) | Payment Means | 4 | POS DD |  |
| contractSeatCount | Počet místenek v souboru |  | 3 | POS DD | Vždy 0. |
| seatValidityEndDate | Konec platnosti – datum | DateStamp | 14 | POS DD | Pokud je platnost doplatku vyjádřena v celých dnech (či delším období), pak první den, kdy již doplatek **ne**platí, jinak poslední den platnosti doplatku. |
| seatValidityEndTime | Konec platnosti – čas | TimeStamp | 11 | POS DD | Pokud je platnost doplatku vyjádřena v celých dnech (či delším období), pak 0, jinak čas konce platnosti doplatku. |
| RFU |  |  | 7 | POS DD | 0 |
| 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 | MSK\_1201\_0 | Master – klíč aplikace |
| #1 | MSK\_1201\_1 | Čtení jízdenky 1 – 5, Kontroly jízdenky 1 – 5, Místenky 1 - 2 |
| #2 | MSK\_1201\_2 | Čtení/zápis jízdenky 1 – 5, Místenky 1 – 2 |
| #3 | MSK\_1201\_3 | Čtení/zápis Kontroly jízdenek 1 – 5 |
| #4 | MSK\_1201\_4 | RFU |
| #5 | MSK\_1201\_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 | Kontrola jízdenky 1 | #1 | #0 | #3 | #0 |
| 6 | Kontrola jízdenky 2 | #1 | #0 | #3 | #0 |
| 7 | Kontrola jízdenky 3 | #1 | #0 | #3 | #0 |
| 8 | Kontrola jízdenky 4 | #1 | #0 | #3 | #0 |
| 9 | Kontrola jízdenky 5 | #1 | #0 | #3 | #0 |
| 10 | Místenka 1 | #1 | #0 | #2 | #0 |
| 11 | Místenka 2 | #1 | #0 | #2 | #0 |

**Aplikace elektronická peněženka (EP)**

* AID aplikace - 8895
* obsahuje 4 soubory
* V tomto dokumentu jsou popsány pouze struktury EP na kartě. Operacemi prováděnými s EP se zabývá zvláštní dokument.

**Soubor Nastavení EP**

Soubor popisuje základní vlastnosti elektronické peněženky, 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*** | ***Popis*** | ***Datový typ*** | ***Bit*** | ***Typ editace*** | ***Hodnota (popis)*** |
| --- | --- | --- | --- | --- | --- |
| contractNetwork | Identifikace transportní sítě do které patří vydavatel EP | NetworkId | 24 | POS |  |
| contractProvider | Kód vydavatele EP | ProviderID | 8 | POS |  |
| 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 karty |
| 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  na Kartě IDS ZK 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 |  |
| 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 |  |
| 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 podepsána klíčem MSK\_8895\_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 elektronické peněženky na konkrétní kartě. | 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 | čísloSAM, 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 | MSK\_8895\_0 | Master – klíč aplikace |
| #1 | MSK\_8895\_1 | Čtení souboru nastavení EP a osobní nastavení EP, Log EP |
| #2 | MSK\_8895\_2 | Zápis souboru nastavení EP |
| #3 | MSK\_8895\_3 | Čtení, debet (dekrementace) a limited credit souboru hodnota EP, zápis Log EP |
| #4 | MSK\_8895\_4 | Kredit (inkrementace) souboru hodnota EP |
| #5 | MSK\_8895\_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**

Aplikace „Rezerva 1“

* AID aplikace – 1202
* neobsahuje žádné soubory
* slouží jako rezervní aplikace

**Struktura**

* Není definována

**Klíče**

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | MSK\_1202\_0 | Master – klíč aplikace |
| #1 | MSK\_1202\_1 | RFU |
| #2 | MSK\_1202\_2 | RFU |
| #3 | MSK\_1202\_3 | RFU |
| #4 | MSK\_1202\_4 | RFU |
| #5 | MSK\_1202\_5 | RFU |

**Rezerva 2**

Aplikace „Rezerva 2“

* AID aplikace – 1108
* neobsahuje žádné soubory
* slouží jako rezervní aplikace

**Struktura**

* Není definována

**Klíče**

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | MSK\_1108\_0 | Master – klíč aplikace |
| #1 | MSK\_1108\_1 | RFU |
| #2 | MSK\_1108\_2 | RFU |
| #3 | MSK\_1108\_3 | RFU |
| #4 | MSK\_1108\_4 | RFU |
| #5 | MSK\_1108\_5 | RFU |

**Rezerva 3**

Aplikace „Rezerva 3“

* AID aplikace – 111A
* neobsahuje žádné soubory
* slouží jako rezervní aplikace

**Struktura**

* Není definována

**Klíče**

|  |  |  |
| --- | --- | --- |
| ***Klíč*** | ***Název*** | ***Význam*** |
| #0 | MSK\_111A\_0 | Master – klíč aplikace |
| #1 | MSK\_111A\_1 | RFU |
| #2 | MSK\_111A\_2 | RFU |
| #3 | MSK\_111A\_3 | RFU |

**Rezerva 4**

Aplikace „Rezerva 4“

* AID aplikace – 100B
* neobsahuje žádné soubory
* slouží jako rezervní aplikace

**Struktura**

* Není definována

**Klíče**

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

**Dotčené normy**

*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, 19988. 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*