Struktura BČK Moravskoslezské karty

Verze 33

21. 3. 2014

Obsah

Historie změn:

<table>
<tr><th>Verze</th><th>Datum</th><th>Jméno</th><th>Důvod vydání</th></tr>
<tr><td>27</td><td>20.03.2012</td><td>Holešovský</td><td>Změna v číslování kupónů a typu</td></tr>
<tr><td>28</td><td>26.03.2012</td><td>Matoušek
Holešovský</td><td>Doplatek do 1. třídy v souboru místenka</td></tr>
<tr><td>29</td><td>25.9. 2012</td><td>Holešovský</td><td>Dobití EP + doplnění významu publisherProviderID, úprava v couponType</td></tr>
<tr><td>29a</td><td>28.11.2013</td><td>Koštuřík</td><td>Úprava pro CheckIn CheckOut v rámci MHD Ostrava. Přidána struktura nového benefitu, viz kapitola 6.2.2 Klíče
<table>
<tr><th>Klíč</th><th>Název</th><th>Význam</th></tr>
<tr><td>#0</td><td>MSK_5346_0</td><td>Master – klíč aplikace</td></tr>
<tr><td>#1</td><td>MSK_5346_1</td><td>Čtení souboru 1 – 5</td></tr>
<tr><td>#2</td><td>MSK_5346_2</td><td>Čtení/zápis souboru 1</td></tr>
<tr><td>#3</td><td>MSK_5346_3</td><td>Čtení/zápis souboru 2</td></tr>
<tr><td>#4</td><td>MSK_5346_4</td><td>Čtení/zápis souboru 3</td></tr>
<tr><td>#5</td><td>MSK_5346_5</td><td>Čtení/zápis souboru 4</td></tr>
<tr><td>#6</td><td>MSK_5346_6</td><td>Čtení/zápis souboru 5</td></tr>
<tr><td>#7</td><td>MSK_5346_7</td><td>RFU</td></tr>
</table>
1.1.1.1 Přístupová práva souborů
<table>
<tr><th>Soubor</th><th>Název</th><th>Read</th><th>Write</th><th>Read & Write</th><th>Change Access Rights</th></tr>
<tr><td>0</td><td>Soubor 1</td><td>#1</td><td>#0</td><td>#2</td><td>#0</td></tr>
<tr><td>1</td><td>Soubor 2</td><td>#1</td><td>#0</td><td>#3</td><td>#0</td></tr>
<tr><td>2</td><td>Soubor 3</td><td>#1</td><td>#0</td><td>#4</td><td>#0</td></tr>
<tr><td>3</td><td>Soubor 4</td><td>#1</td><td>#0</td><td>#5</td><td>#0</td></tr>
<tr><td>4</td><td>Soubor 5</td><td>#1</td><td>#0</td><td>#6</td><td>#0</td></tr>
</table>
1.1.2 Aplikace v jednotlivých souborech Průkaz/Benefit
1.1.2.1 Soubor 1 – CheckIn/CheckOut pro DPO
Datová struktura benefitCheckInCheckOut.</td></tr>
<tr><td>29b</td><td>3.12. 2013</td><td>Koštuřík</td><td>Přidána kapitola 6.2.3 Aplikace v jednotlivých souborech Průkaz/Benefit</td></tr>
<tr><td>30</td><td>10.2. 2014</td><td>Koštuřík</td><td>Přidána položka couponsPrepaidTransaction viz kapitola 6.1.1.1 Datová struktura cardInfo.</td></tr>
<tr><td>31</td><td>21.3. 2014</td><td>Škapa</td><td>Změna struktury datum u Benefitu
viz kapitola 6.1.1.1.1 Datová struktura cardInfo</td></tr>
<tr><td>32</td><td>14.10.2014</td><td>Nenka</td><td>Úprava kapitoly 2</td></tr>
<tr><td>33</td><td>10. 9‘. 2019</td><td>Nenka</td><td>Doplnění popisu položky HolderID v cardHolderInfo</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Verze	Datum	Jméno	Důvod vydání

2. Požadavky na funkčnost odbavovacího zařízení

Odbavovací zařízení musí zajistit bezproblémový proces odbavení cestujících na bázi bezkontaktní čipové karty typu MIFAREDESFireEV1 8 kB (dále BČK). Musí umožnit prodej cestovního dokladu (jak papírového, tak na platformě BČK) podle platného tarifu ODIS.. Zařízení musí splňovat požadavky Bezpečnostní politiky BČK Moravskoslezské karty (bezpečné úložiště klíčů v odbavovacím zařízení – SAM modul, bezpečná komunikace odbavovacího zařízení s bezkontaktní čipovou kartou, atd.). Komunikace zařízení s kartou musí trvat krátkou dobu – za jakékoliv situace a při jakékoliv tarifní kombinaci do 3 sekund od přiložení karty a zadání cílové zastávky řidičem.

Odbavovací zařízení musí obecně splnit úkony - prodej papírového jízdního dokladu, plnění elektronické peněženky, nahrání jednotlivého jízdného ODIS na BČK při prodeji z elektronické peněženky, nahrání dlouhodobého časového jízdného ODIS na BČK při platbě z elektronické peněženky nebo za hotovost, nahrání dlouhodobého časového jízdného ODIS zakoupeného přes e-shop, nahrání kreditu elektronické peněženky zakoupeného přes e-shop, reklamační proces, čímž se rozumí vystornováníjakékoliv operace provedené v rámci odbavení na BČK; odbavovací zařízení musí mít dostatečnou paměťovou kapacitu pro tarif ODIS, musí zvládat zapisovat data přímo do paměti BČK, musí generovat výstupní sestavy dle požadavků clearingového centra, musí umět pracovat s jednotnými vstupními daty popisujícími Tarif ODIS, který bude spravovat Koordinátor ODIS, a který je součástí clearingového centra.

Společnost Koordinátor ODIS s.r.o. poskytne pro dopravce bezpečným způsobem klíče ke kartám a SAM modulům a SW nástroje pro nahrání datové struktury karty ODIS zejména pak Dopravní aplikace a aplikace elektronické peněženky a dále poskytne design karty pro potřeby výroby karty.

3. Úvod

Dokument obsahuje informace o BČK Moravskoslezské karty týkající se:

- struktury aplikací/souborů a jejích formátů

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

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 0 – Použité normativní dokumenty. Návrh je také v souladu s připravovanou vyhláškou ustanovující standardy platby a odbavení cestujících ve veřejné dopravě s využitím bezkonatktních čipových technologií.

Architektura je navržena tak, aby mohla být použita metoda postupného budování infrastruktury a využívání MSK, kde v první části (fázi) bude budována dopravní aplikace, tj. využití karty 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

3.1 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 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 navržené BČK a autentizační mechanismy BČK 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
- návrh BČK umožňuje multifunkční použití, tj. paralelní umístění, užívání a správu aplikací různých subjektů
- návrh BČK nabízí kromě standardní bezpečnosti karet Mifare DESFire i vlastní nativní bezpečnostní prvky - šifrování obsahu, podpis obsahu pomocí symetrických i asymetrických kryptografických mechanismů
- návrh BČK umožňuje zavedení dodatečné bezpečnostní vrstvy prostředky, které jsou na nativních bezpečnostních mechanismech karty nezávislé
- BČK umožňuje obnovovat bezpečným způsobem kryptografické klíče použité pro ochranu karty a jejich aplikací
- Návrh BČK 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 IDS
- Návrh BČK umožňuje nahrávat strukturu také na NFC mobilní telefony podporující v Secure Elementu karty Mifare DESFire

3.2 Popis návrhu struktury BČK MSK

Návrh obsahuje 4 kompletní aplikace a 4 rezervní aplikace pro případné další dopnění struktury BČK MSK.

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)

3.3 Definice zkratek a pojmů

Pojem	*Definice*
AID	Identifikátor aplikace Application Identifier ISO/IEC 7816-5:2004
BČK	Bezkontaktní 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 BČK jsou obecně považovány za časté a méně spolehlivé s ohledem na zápis dat na BČK
EP	Elektronická peněženka
KC	Kartové centrum, provádí grafickou a datovou personalizaci
HW	Hardware
IDS	Integrovaný dopravní systém Moravskoslezského kraje
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	Moravskoslezská karta
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 BČK jsou obecně považovány za méně časté a více spolehlivé s ohledem na zápis dat na BČK
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
Tarif ODIS	Filozofie tarifu pro MS kartu zpracovanou Koordinátorem ODIS s.r.o.

4. 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.

5. Struktura popisovaných aplikací

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

#Num	***FileName***		***FileType***
Název	***Bitů***	***Typ***	
Verze	8	INT1	Nešifrovaná oblast souboru
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.

6. Aplikace na MSK

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

6.1 Personalizační aplikace

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

6.1.1 Struktura souboru Informace o kartě

0	***cardInfoFile***				***Standard Data File***
Název	***Bitů***	***Typ***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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 6.1.1.1).	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)			

6.1.1.1 Datová struktura cardInfo

Proměnná	***Popis***	***Datový typ***	***Bit***	***Typ editace***	***Hodnota (popis)***
publisherProviderID	Identifikace vydavatele karty dle číselníku XXX	INT3	24	KC	0811 – vydavatel DPO u karet vydaných do 15.11. 2011 062 – vydavatel DPO
publisherNetworkID	Identifikace transportní sítě do které patří vydavatel karty	INT3	24	KC	203811 (dle Číselníku NetworkID & ProviderID)
signatureVersion	verze klíče ECDSA	INT1	8	KC	1
signatureUID	privátním klíčem ECDSA	OCTET STRING	448	KC	MSK_0027_ECC_P

Proměnná	*Popis*	*Datový typ*	*Bit*	*Typ editace*	*Hodnota (popis)*
	podepsané UID karty – typ 8	(56)			
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**		

6.1.2 Struktura souboru Informace o držiteli

1	*cardHolderInfoFile*				*Standard Data File*
Název	***Bitů***	***Název***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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 (viz 6.1.2.1).	Potenciálně šifrovaná oblast souboru
Podpis	64		POS	0	
Využito	1024				
RFU	0				
Celkem B	128	(= 4 × 32 B)			

6.1.2.1 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	BCDString	80	KC POS	RFU

	využití pro identifikaci zaměstnavatele pro účely zaměstnaneckého jízdného.				
holderName	Identifikace držitele (75 B, tedy 37 až 75 znaků)	UTF8String	600	KC POS	RFU
holderProfile1	Profil1 držitele BČK 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 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)

6.1.3 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	

6.1.3.1 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

6.2 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

6.2.1 Soubor Průkaz/Benefit

0 - 4	***benefitFile***				***Standard Data File***
Název	***Bitů***	***Název***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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)			

6.2.1.1 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**		

6.2.2 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

6.2.2.1 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

6.2.3 Aplikace v jednotlivých souborech Průkaz/Benefit

6.2.3.1 Soubor 1 – CheckIn/CheckOut pro DPO

6.2.3.1.1 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 (viz kap. 6.3.1.2)	32	POS	
contract2	Informace o	seasonTicketC	32	POS	

	druhém profilu cestujícího.	ontract (viz kap. 6.3.1.2)			
contract3	Informace o třetím profilu cestujícího.	seasonTicketContract (viz kap. 6.3.1.2)	32	POS	
Celkem bitů			**128**		
Celkem byte			**16**		

6.2.3.2 Soubor 2

Soubor prozatím není využíván.

6.2.3.3 Soubor 3

Soubor prozatím není využíván.

6.2.3.4 Soubor 4

Soubor prozatím není využíván.

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

6.2.3.5.1 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**		

6.3 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.

6.3.1 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 cestujícímu 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 MSK jako datový nosič (například předložení jiného průkazu).

0 - 4	*seasonTicketFile*				*Backup Data File*
Název	***Bitů***	***Název***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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 (viz 6.3.1.1).	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)			

6.3.1.1 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 či dobil 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
contractValiditySta	Počátek platnosti – datum	DateStamp	14	POS	

Proměnná	*Popis*	*Datový typ*	*Bit*	*Typ editace*	*Hodnota (popis)*
rtDate				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 (viz kap. 6.3.1.2)	32	POS DD	
contract2	Informace o druhém profilu cestujícího.	seasonTicketContract (viz kap. 6.3.1.2)	32	POS DD	
contract3	Informace o třetím profilu cestujícího.	seasonTicketContract (viz kap. 6.3.1.2)	32	POS DD	
contract4	Informace o čtvrtém profilu cestujícího.	seasonTicketContract (viz kap. 6.3.1.2)	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
contractHasJourne	0: Doklad nemá trasu (síťová		3	POS	

Proměnná	*Popis*	*Datový typ*	*Bit*	*Typ editace*	*Hodnota (popis)*
y	jízdenka) 1: Doklad je dán relací (Z, Do, Přes) 2: Doklad je dán výčtem zón 3: Doklad je dán číslem trasy 4-7: RFU			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***
0	0: Bez omezení 1: Omezení aplikováno
1	Vlak Os, Sp, Ex
2	Vlak R
3	Vlak EC, IC
4	Vlak SC
5	Lanovka
6	Bus
7	Loď

Bit	***Omezení***
8	Tramvaj
9	Trolejbus
10	RFU
11	
12	
13	
14	
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.

6.3.1.2 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_KODIS_xxx.xlsx“		6	POS DD	
contractCustomerProfile	Kód klasifikující kupón dle určitých kritérií. Profil zákazníka popisuje zákazníka (např. důchodce). Číselník dle CustomerProfile z „struktura_tarifu_KODIS_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.

6.3.1.3 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**		

6.3.1.4 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**		

6.3.1.5 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)

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 MSK**
1023	10	až 18
2047	11	až 16
4095	12	až 15
…	…	…

Příklad pro MSK:

Jízdenka platná v zónách **230**, 126,**125**,124,**135**

contractJourneyZonesCount : 0x05

contractJourneyZones : '**01100110**00111111**00111110**00111111**01000111**'b

6.3.1.6 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**		

6.3.2 Soubor Kontrola jízdenky

5 - 9	*ticketPliersFile*				*Standard Data File*
Název	***Bitů***	***Typ***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
Status souboru	8		KC	7 (Ok)	
ticketCheck	240	Struktura ticketPliersInfo			
Využito	256				
RFU	0				
Celkem B	32	(= 1 × 32 B)			

6.3.2.1 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**		

6.3.3 Soubor Místenka

10 - 11	*seatReservationTicketFile*				*Standard Data File*
Název	***Bitů***	***Typ***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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)			

6.3.3.1 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		2	POS DD	

Proměnná	*Popis*	*Datový typ*	*Bit*	*Typ editace*	*Hodnota (popis)*
	vyšší třídu než je jízdenka				
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**		

6.3.3.2 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	INT3	24	POS DD	0, nyní nevyužito

	omezení)				
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**		

6.3.4 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

Klíč	*Název*	*Význam*
#4	MSK_1201_4	RFU
#5	MSK_1201_5	RFU

6.3.4.1 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

6.4 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.

6.4.1 Soubor Nastavení EP

Soubor popisuje základní vlastnosti elektronické peněženky, dané typicky legislativou.

0	***walletSettingsFile***				***Standard Data File***
Název	***Bitů***	***Typ***	***Typ editace***	***Hodnota (popis)***	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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)			

6.4.1.1 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

Proměnná	*Popis*	*Datový typ*	*Bit*	*Typ editace*	*Hodnota (popis)*
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**		

6.4.2 Soubor Osobní nastavení EP

Soubor popisuje aktuální uživatelské nastavení EP.

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

1	*walletPersonalSettingsFile*				*Standard Data File*
Název	*Bitů*	*Typ*	*Typ editace*	*Hodnota (popis)*	
Verze	8	INT1	KC	1	Nešifrovaná oblast souboru
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)			

6.4.2.1 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**		

6.4.3 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)	

6.4.4 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)***	
Verze	8	INT1	POS DD	1	Nešifrovaná oblast souboru
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

3	*logEPFile*				*Cyclic Record File*
Podpis	64		POS DD	Struktura od Verze po Log podepsána klíčem MSK_8895_SIGN	šifrovaná oblast souboru

Využito 1 záznam	256	
Nevyužito v souboru	0	
Celkem soubor B	224	(= 7 × 32 B)

6.4.4.1 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**		

6.4.5 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

6.4.5.1 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

6.5 Rezerva 1

Aplikace „Rezerva 1“

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

6.5.1 Struktura

- Není definována

6.5.2 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

6.6 Rezerva 2

Aplikace „Rezerva 2“

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

6.6.1 Struktura

- Není definována

6.6.2 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

6.7 Rezerva 3

Aplikace „Rezerva 3“

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

6.7.1 Struktura

- Není definována

6.7.2 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

6.8 Rezerva 4

Aplikace „Rezerva 4“

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

6.8.1 Struktura

- Není definována

6.8.2 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

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, 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