Príloha č. 1 k metodickému usmerneniu č. 16

Zoznam položiek v dátových blokoch č. 0, 1 a 2

Dátový blok č. 0 - verejné údaje o preukaze (nešifrované)

Poradie položky	Popis položky / údaja	Formát	Max. počet znakov
1.	Druh preukazu	číslo	1
2.	Začiatok platnosti preukazu	dátum	8
3.	Koniec platnosti preukazu	dátum	8
4.	Dátum poslednej aktualizácie údajov	dátum	8
	Oddeľovacie znaky „|“ medzi položkami		3
	Spolu		28

Dátový blok č. 1 - potvrdenie o štúdiu na vysokej škole (šifrované kľúčom K1)

Poradie položky	Popis položky / údaja	Formát	Max. počet znakov
1.	Vysoká škola, fakulta, miesto štúdia - kód	číslo	9
2.	Vysoká škola, fakulta, miesto štúdia - PSČ	číslo	5
3.	Stupeň štúdia	číslo	1
4.	Pohlavie	znaky	1
5.	Tituly pred menom	text	25
6.	Meno	text	25
7.	Priezvisko	text	50
8.	Tituly za menom	text	25
	Oddeľovacie znaky „|“ medzi položkami		7
	Spolu		148

Dátový blok č. 2 - osobné údaje držiteľa preukazu (šifrované kľúčom K2)

Poradie položky	Popis položky / údaja	Formát	Max. počet znakov
1.	Osobné číslo	znaky	10
2.	Dátum narodenia	dátum	8
3.	Trvalý pobyt - ulica a číslo domu	text	50
4.	Trvalý pobyt - obec	text	30
5.	Trvalý pobyt - PSČ	znaky	10
6.	Trvalý pobyt - štát	znaky	2
7.	Prechodný pobyt - ulica a číslo domu	text	50
8.	Prechodný pobyt - obec	text	30
9.	Prechodný pobyt - PSČ	číslo	5
	Oddeľovacie znaky „|“ medzi položkami		8
	Spolu		203

Význam položiek a spôsob ich vypĺňania, prípadne kódovania

Dátový blok č. 0 - verejné údaje o preukaze

(1) **Druh preukazu**:
1 - študent dennej formy štúdia
2 - študent externej formy štúdia
3 - učiteľ VŠ
4 - iný zamestnanec VŠ
5 - iný používateľ

(2) **Začiatok platnosti preukazu** - podľa textu usmernenia

(3) **Koniec platnosti preukazu** - podľa textu usmernenia

(4) **Dátum poslednej aktualizácie údajov** - dátum a čas, ku ktorému sú údaje platné

Dátový blok č. 1 - potvrdenie o štúdiu na vysokej škole

(1) **Vysoká škola, fakulta, miesto štúdia - kód** - podľa katalógu CRŠ

(2) **Vysoká škola, fakulta, miesto štúdia - PSČ** - na dopravné zľavy

(3) **Stupeň štúdia**:
1 - študijný program prvého stupňa na VŠ
2 - študijný program druhého stupňa na VŠ
3 - študijný program tretieho stupňa na VŠ

(4) **Pohlavie**:
„M“ - muž - Male
„F“ - žena - Female

(5) **Tituly pred menom** - akademické tituly, vedecko-pedagogické tituly a umelecko-pedagogické tituly pred menom

(6) **Meno** - krstné meno alebo niekoľko mien - oddelené medzerami

(7) **Priezvisko** - priezvisko alebo niekoľko priezvisk - vrátane rodného priezviska

(8) **Tituly za menom** - akademické tituly a vedecké hodnosti za menom

Dátový blok č. 2 - osobné údaje držiteľa preukazu

(1) **Osobné číslo** - jednoznačný identifikátor držiteľa preukazu určený vydavateľom preukazu. Môže obsahovať ľubovoľné alfanumerické znaky bez slovenskej diakritiky. Vo funkcii osobného čísla nemožno použiť všeobecne použiteľné identifikátory osoby podľa osobitného predpisu o ochrane osobných údajov.

(2) **Dátum narodenia** - osobný údaj

(3) **Trvalý pobyt - ulica a číslo domu**

(4) **Trvalý pobyt - obec**

(5) **Trvalý pobyt - PSČ**

(6) **Trvalý pobyt - štát** - podľa normy ISO na 2 znaky, napr. „SK“

(7) **Prechodný pobyt - ulica a číslo domu** - miesto pobytu na území Slovenskej republiky

(8) **Prechodný pobyt - obec**

(9) **Prechodný pobyt - PSČ**

Príloha č. 2 k metodickému usmerneniu č. 16

Použitie algoritmov na šifrovanie a elektronický podpis údajov v preukaze študenta

Táto príloha obsahuje príklad zostavenia dátového záznamu v pamäti preukazu študenta na základe vzorových údajov o fiktívnej osobe.

Vysvetlivky k ďalšiemu textu:

- Neproporcionálnym písmom sú označené hodnoty bajtov alebo bajtových polí v šestnástkovej číselnej sústave (hexadecimálne, hexa) - napr. **3D 25 F9**.
- Bežným písmom sú označené číselné údaje v desiatkovej číselnej sústave - napr. 123.
- Tučným písmom v úvodzovkách sú označené znakové reťazce - napr. „**František“**.

Vstupné údaje

K1, K2 - tajné kľúče na šifrovanie a dešifrovanie dátových blokov č. 1 a 2 v pamäti preukazu, ktoré určí ministerstvo podľa čl. 12, ods. 1 usmernenia. Tieto kľúče sú spoločné pre všetkých vydavateľov preukazov a poskytovateľov služieb, ktoré si vyžadujú použitie údajov v pamäti preukazu. Kľúče sú dlhé 16 bajtov a v nasledujúcom príklade majú hodnotu:

- **00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF** - K1
- **FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00** - K2

Privátny a verejný kľúč - slúžia na vytvorenie a overenie elektronického podpisu vydavateľa preukazu. V nasledujúcom príklade majú hodnotu:

- **1F 18 AA E9 D3 BD 93 70 A0 59 28 D6 C3 A1 E6 A1 5B 1B B3 EB 39 16 99 F1** - privátny kľúč - 24 bajtov
- **04 D2 DB A4 D1 6F 27 D9 A9 C2 F6 26 C2 93 89 6F C5 52 29 5F 8C CA 82 0E 44 49 7C 30 EB 9A A1 1A D0 31 3B 07 BC 20 BC 3B 42 16 65 48 54 78 B7 CD 23** - verejný kľúč - 49 bajtov

UID - unikátny identifikátor bezkontaktného čipu Mifare v preukaze, ktorý je dlhý 7 bajtov na preukaze s čipom DESFire a 4 bajty na preukaze s čipom Classic. Používa sa na vytvorenie a overenie elektronického podpisu vydavateľa preukazu. V nasledujúcom príklade sa používa dlhšia hodnota pre preukaz s čipom DESFire:

- 6 2694 8164 5966 6450 - dekadicky
- **12 34 56 78 9A BC DE** - hexa, little-endian

Dátový blok č. 0 - verejné údaje o preukaze, nešifrované

Poradie	Položka	Príklad
1.	Druh preukazu	1
2.	Začiatok platnosti preukazu	01.09.2013
3.	Koniec platnosti preukazu	30.09.2014
4.	Dátum poslednej aktualizácie údajov	24.03.2014

- „**1|20130901|20140930|20140324“** - 28 znakov
- `31 7C 32 30 31 33 30 39 30 31 7C 32 30 31 34 30` - 28 bajtov + zarovnanie
  `39 33 30 7C 32 30 31 34 30 33 32 34 00 00 00 00`

Podľa čl. 9 usmernenia dátový blok obsahuje súvislý reťazec znakov zostavený z položiek vo formáte CSV s oddeľovacím znakom „|“. Je kódovaný podľa normy UTF-8 a zarovnaný na násobok 16 bajtov.

Dátový blok č. 1 - potvrdenie o štúdiu na vysokej škole, šifrované kľúčom K1

Poradie	Položka	Príklad
1.	Škola, fakulta, miesto štúdia - kód	710010100
2.	Škola, fakulta, miesto štúdia - PSČ	83106
3.	Stupeň štúdia	2
4.	Pohlavie	M
5.	Tituly pred menom	Bc.
6.	Meno	František
7.	Priezvisko	Ľúbezný
8.	Tituly za menom	

- „**710010100|83106|2|M|Bc.|František|Ľúbezný**|“ - 42 znakov
- `37 31 30 30 31 30 31 30 30 7C 38 33 31 30 36 7C` - 46 bajtov + zarovnanie + CRC
  `32 7C 4D 7C 42 63 2E 7C 46 72 61 6E 74 69 C5 A1`
  `65 6B 7C C4 BD C3 BA 62 65 7A 6E C3 BD 7C 00 00`
  `00 00 00 00 00 00 00 00 00 00 00 00 FB E9 91 A3`
- `69 92 B0 38 6F C5 03 FE C1 75 6F 5F 45 7B ED 48` - šifrovaný
  `C8 B5 B2 83 83 06 0D 63 E5 C2 F9 E6 84 81 0C 22`
  `28 A1 68 9A B1 6E F3 AB 26 CC A9 1E E6 46 2C 5D`
  `2E 93 70 66 FB 01 F1 08 37 6D 4E 8D 7C 47 FA 0E`

Meno študenta v príklade je zvolené tak, aby sa preukázal vplyv kódovania UTF-8 na znaky so slovenskými diakritickými znamienkami. Vďaka tomuto kódovaniu reťazec v binárnej forme zaberá viac bajtov ako obsahuje znakov. Oddeľovač „|“ na konci záznamu je prítomný preto, že posledná položka „Tituly za menom“ je prázdna.

Podľa čl. 9, ods. 5 usmernenia sa šifruje celý dátový blok algoritmom AES-128 s parametrami Mode = CBC, Padding = None, IV = 0. Do posledných 4 bajtov bloku sa predtým vloží kontrolný súčet bloku podľa štandardu Mifare CRC-32.

Dátový blok č. 2 - osobné údaje držiteľa preukazu, šifrované kľúčom K2

Poradie	Položka	Príklad
1.	Osobné číslo	120735
2.	Dátum narodenia	11.03.1995
3.	Trvalý pobyt - ulica a číslo domu	M. R. Štefánika 78/A
4.	Trvalý pobyt - obec	Čadca
5.	Trvalý pobyt - PSČ	02201
6.	Trvalý pobyt - štát	SK
7.	Prechodný pobyt - ulica a číslo domu	Staré Záhrady 35
8.	Prechodný pobyt - obec	Bratislava
9.	Prechodný pobyt - PSČ	82105

- „**120735|19950311|M. R. Štefánika 78/A|Čadca|02201|SK|Staré Záhrady 35|Bratislava|82105**“ - 85 znakov
- `31 32 30 37 33 35 7C 31 39 39 35 30 33 31 31 7C` - 90 bajtov + zarovnanie + CRC
  `4D 2E 20 52 2E 20 C5 A0 74 65 66 C3 A1 6E 69 6B`
  `61 20 37 38 2F 41 7C C4 8C 61 64 63 61 7C 30 32`
  `32 30 31 7C 53 4B 7C 53 74 61 72 C3 A9 20 5A C3`
  `A1 68 72 61 64 79 20 33 35 7C 42 72 61 74 69 73`
  `6C 61 76 61 7C 38 32 31 30 35 00 00 44 68 90 3C`
- `BE 69 CE 36 CC 33 91 5A 62 A6 3A 88 39 C2 8E AD` - šifrovaný
  `BC C3 CB E8 63 BE 1B 4C 32 46 1B BA CD 2A 3D 64`
  `F1 A4 6B 49 73 A2 A9 43 E1 A5 56 7A 75 39 D3 7E`
  `D5 A9 62 F8 F8 92 66 06 4B 6F 8A 29 2D D3 88 F4`
  `E0 B0 BE 42 D1 77 AD 1D D2 2D F9 0A 38 D3 95 1D`
  `7D 34 DE DF 07 6E E1 AA 8B C5 A2 90 09 AD 2B E3`

Elektronický podpis vydavateľa preukazu

Podľa čl. 10 usmernenia elektronický podpis údajov sa vytvára pomocou algoritmov SHA-1 a ECDSA s krivkou NIST P-192, ktorá je známa aj pod označením X9.62 prime192v1 alebo secp192r1. Do jeho výpočtu vstupuje obsah celého záznamu a UID preukazu. Výsledný podpis sa vkladá za posledný dátový blok.

- `05 01 01 1B 1C 00 2E 00 5A 00 00 00 00 00 00 00` - hlavička záznamu
- `31 7C 32 30 31 33 30 39 30 31 7C 32 30 31 34 30` - dátový blok č. 0
  `39 33 30 7C 32 30 31 34 30 33 32 34 00 00 00 00`
- `69 92 B0 38 6F C5 03 FE C1 75 6F 5F 45 7B ED 48` - dátový blok č. 1
  `C8 B5 B2 83 83 06 0D 63 E5 C2 F9 E6 84 81 0C 22`
  `28 A1 68 9A B1 6E F3 AB 26 CC A9 1E E6 46 2C 5D`
  `2E 93 70 66 FB 01 F1 08 37 6D 4E 8D 7C 47 FA 0E`
- `BE 69 CE 36 CC 33 91 5A 62 A6 3A 88 39 C2 8E AD` - dátový blok č. 2
  `BC C3 CB E8 63 BE 1B 4C 32 46 1B BA CD 2A 3D 64`
  `F1 A4 6B 49 73 A2 A9 43 E1 A5 56 7A 75 39 D3 7E`
  `D5 A9 62 F8 F8 92 66 06 4B 6F 8A 29 2D D3 88 F4`
  `E0 B0 BE 42 D1 77 AD 1D D2 2D F9 0A 38 D3 95 1D`
  `7D 34 DE DF 07 6E E1 AA 8B C5 A2 90 09 AD 2B E3`
- `12 34 56 78 9A BC DE` - UID preukazu
- `89 B9 39 82 A2 48 80 BE 40 75 D4 8F 34 00 97 BF` - kontrolný súčet - 20 bajtov
  `3E 14 82 CD`

- 86 B0 E7 0D BF 10 AB 2C F4 F3 AA 80 56 DB A8 D9 - elektronický podpis - 48 bajtov
  C2 E0 7F 5E 62 3B F4 33 E0 61 F4 CE EF D0 7F 2C
  8E FB 01 D6 43 A9 5C B9 4A CB 68 3C D6 11 80 73

Podpis tvoria dve veľké celé čísla bez znamienka, ktoré sa v kryptografii ECDSA označujú ako R a S. Každé z nich je dlhé 24 bajtov (192 bitov) a je uložené v tvare "big-endian". Poznamenávame, že pre rovnaké vstupné údaje, t.j. kontrolný súčet a verejný kľuč, algoritmus vygeneruje vždy iný podpis.

Výsledný dátový záznam

Podľa čl. 7 usmernenia dátový záznam tvorí hlavička, tri dátové bloky a elektronický podpis vydavateľa preukazu.

- 05 - verzia záznamu - 16 bajtov - hlavička
- 01 - verzia kľúča K1
- 01 - verzia kľúča K2
- 1B - registračné číslo kľúča elektronického podpisu (príklad)
- 1C 00 - dĺžka dát v bloku č. 0
- 2E 00 - dĺžka dát v bloku č. 1
- 5A 00 - dĺžka dát v bloku č. 2
- 00 00 00 00 00 00 - zarovnanie

- 31 7C 32 30 31 33 30 39 30 31 7C 32 30 31 34 30 - 32 bajtov - dátový blok č. 0
  39 33 30 7C 32 30 31 34 30 33 32 34 00 00 00 00

- 69 92 B0 38 6F C5 03 FE C1 75 6F 5F 45 7B ED 48 - 64 bajtov - dátový blok č. 1
  C8 B5 B2 83 83 06 0D 63 E5 C2 F9 E6 84 81 0C 22
  28 A1 68 9A B1 6E F3 AB 26 CC A9 1E E6 46 2C 5D
  2E 93 70 66 FB 01 F1 08 37 6D 4E 8D 7C 47 FA 0E

- BE 69 CE 36 CC 33 91 5A 62 A6 3A 88 39 C2 8E AD - 96 bajtov - dátový blok č. 2
  BC C3 CB E8 63 BE 1B 4C 32 46 1B BA CD 2A 3D 64
  F1 A4 6B 49 73 A2 A9 43 E1 A5 56 7A 75 39 D3 7E
  D5 A9 62 F8 F8 92 66 06 4B 6F 8A 29 2D D3 88 F4
  E0 B0 BE 42 D1 77 AD 1D D2 2D F9 0A 38 D3 95 1D
  7D 34 DE DF 07 6E E1 AA 8B C5 A2 90 09 AD 2B E3

- 86 B0 E7 0D BF 10 AB 2C F4 F3 AA 80 56 DB A8 D9 - 48 bajtov - elektronický podpis
  C2 E0 7F 5E 62 3B F4 33 E0 61 F4 CE EF D0 7F 2C
  8E FB 01 D6 43 A9 5C B9 4A CB 68 3C D6 11 80 73

Celková dĺžka dátového záznamu v tomto prípade je 256 bajtov. Ak by presiahla 480 bajtov, museli by sa skrátiť textové položky v dátových blokoch.

Registračné číslo kľúča elektronického podpisu uvedené v hlavičke záznamu slúži na vyhľadanie verejného kľúča vydavateľa preukazu, ktorým možno overiť platnosť podpisu.

Príloha č. 3 k metodickému usmerneniu č. 16

Použité technologické a informatické skratky

Skratka	Vysvetlenie skratky
AES	Advanced Encryption Standard - schválený štandard amerického úradu pre štandardizáciu založený na symetrickej blokovej šifre Rijndael
AID	Aplication IDentifier (pre karty Mifare)
APDU	Application Protocol Data Unit (komunikačný protokol definovaný a popísaný v norme ISO 7816-4)
API	Application Programing Interface
ASCII	American Standard Code for Information Interchange (kódová stránka)
CBC	Cipher Block Chaining (spôsob/mód použitia šifrovacieho algoritmu)
CC EAL	Common Criteria Evaluation Assurance Level (požadovaná úroveň záruk podľa medzinárodných noriem)
CNG	Cryptographic API Next Generation (nová architektúra kryptografických služieb operačných systémov Microsoft Windows)
CSP	Cryptographic Service Provider (základný poskytovateľ kryptografických služieb systémov na báze MS Windows)
CSV	Comma-separated values (jednoduchý formát na zápis alebo prenos tabuľkových údajov vo forme čistého textu, kde hodnoty jednotlivých položiek v riadku sú navzájom oddelené dohodnutým oddeľovacím znakom)
DES	Data Encryption Standard (symetrický šifrovací algoritmus)
ECDSA	Elliptic Curve Digital Signature Algorithm (variant podpisovej schémy digitálneho podpisovacieho algoritmu založený na algebrickej štruktúre eliptických kriviek nad konečnými poľami)
EEPROM	Electricalle Erasable Programmable Read Only Memory (elektronická súčiastka, pamäť)
FIPS	Federal Information Processing Standard (bezpečnostná certifikácia vlády USA)
GUID	Globally Unique Identifier (jedinečný identifikátor)
ISIC	International Students Identity Card (medzinárodná identifikačná karta študenta)
ITIC	Internation Teacher Identification Card (medzinárodná identifikačná karta učiteľa)
KSP	Key Storage Provider (základný poskytovateľ pre bezpečné uloženie a používanie súkromných kľúčov)
MAC	Message Authentication Code
MAD	Mifare Application Directory (adresár pre karty Mifare)
PICC	Proximity Integrated Circuit Card (bezkontaktná karta)
PIN	Personal Identification Number (osobné identifikačné číslo)
PKCS	Public Key Cryptography Standard (štandardy pre kryptografiu s verejným kľúčom)
PKCS#11	štandard, definujúci multi platformné rozhranie pre kryptografické zariadenia
PKI	Public Key Infrastructure (Infraštruktúra verejného kľúča)
PUK	Pin Unlock Key (odblokovací kód pre PIN)
RSA	Rivest, Shamir, Adleman (druh kryptografického algoritmu)
SAM	Secure Access Module (HW modul pre bezpečné kryptografické operácie)
SHA	Secure Hash Algorithm (bezpečný abstrakčný algoritmus)
SNR	Serial NumbeR (výrobné číslo karty pre karty Mifare Standard)
SSCD	Ignature Creation Device (prostriedok pre bezpečné vytváranie elektronického podpisu)
UID	Unique IDdentifier (výrobné číslo karty pre čipové karty)
UTF8	8-bit Unicode Transformation Format (bezstratové kódovanie s variabilnou dĺžkou určené pre Unicode znaky)