

Príloha č. 2 Použitie algoritmov na šifrovanie a elektronický podpis údajov v preukaze

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

Vysvetlivky

- 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. 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 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

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

- 1F 18 **AA E9** D3 BD 93 70 A0 59 28 D6 C3 **A1 E6 A1** - **súkromný** kľúč 24 bajtov
5B 1B B3 **EB** 39 16 99 **F1**
- 04 D2 DB **A4 D1 6F** 27 D9 **A9 C2 F6** 26 C2 93 89 **6F** -verejný kľúč 49 bajtov
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

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 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

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
1.	Stupeň štúdia	2
2.	Pohlavie	M
3.	Tituly pred menom	Bc.
4.	Meno	František
5.	Priezvisko	Lúbezný
6.	Tituly za menom	
7.	ESCN	1a041b0079dd103da648001227063334
8.	ESI	urn:schac:personalUniqueCode:int:esi:sk:stuba.sk:123456

131 znakov

„710010100|83106|2|M|Bc.|František|Lúbezný||1a041b0079dd103da648001227063334|urn:schac:personalUniqueCode:int:esi:sk:stuba.sk:123456“

135 bajtov + zarovnanie + crc (144 bajtov)

- 37 31 30 30 31 30 31 30 30 7C 38 33 31 30 36 7C
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 7C 31
61 30 34 31 62 30 30 37 39 64 64 31 30 33 64 61
36 34 38 30 30 31 32 32 37 30 36 33 33 33 34 7C
75 72 6E 3A 73 63 68 61 63 3A 70 65 72 73 6F 6E
61 6C 55 6E 69 71 75 65 43 6F 64 65 3A 69 6E 74
3A 65 73 69 3A 73 6B 3A 73 74 75 62 61 2E 73 6B
3A 31 32 33 34 35 36 00 00 00 00 00 AB 4B E8 88

šifrované data:

- 69 92 B0 38 6F C5 03 FE C1 75 6F 5F 45 7B ED 48
C8 B5 B2 83 83 06 0D 63 E5 C2 F9 E6 84 81 0C 22

```
03 5F 13 E8 BD 3E 13 DE 91 D6 9D CF 9C 33 15 49
11 8D 08 25 A3 81 CE 64 15 B7 43 92 22 B7 20 A1
0C DD A7 11 4F 79 A5 22 04 2A A6 3B 61 60 E2 34
CF 82 8B 58 4F E2 0B 50 FC E4 1B 63 18 33 1F F8
10 7B A5 31 CE D4 7C C9 84 5A DF C4 E0 6E CF 2A
74 1B D0 89 49 39 39 4A C7 F7 6C 1D 06 EB BE 0F
43 07 FB 66 DD EF BA 40 7F 1A 09 03 25 A0 85 B5
```

Meno a priezvisko študenta v príklade je zvolené tak, aby sa preukázal vplyv kódovania UTF-8 na znaky so slovenskými diakritickými znamienkami a v dôsledku kódovania reťazec v binárnej forme zaberá viac bajtov ako obsahuje znakov. Oddeľovač „|“ na konci záznamu je z dôvodu prázdnej poslednej položky „Tituly za menom“.

ESCN obsahuje len identifikátor, pre QR kód sa použije cesta s identifikátorom podľa špecifikácie

<https://esc-r.eu/1a041b00-79dd-103d-a648-001227063334>

Podľa čl. 9, ods. 5 písm. c) 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 Záhřady 35
8.	Prechodný pobyt - obec	Bratislava
9.	Prechodný pobyt - PSČ	82105

- „120735|19950311|M. R. Štefánika 78/A|Čadca|02201|SK|Staré Záhřady 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 sa elektronický podpis údajov vytvára pomocou algoritmov SHA-1 a ECDSA s krivkou NIST P-192 (X9.62 prime192v1 alebo secp192r1). Do 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 - 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
03 5F 13 E8 BD 3E 13 DE 91 D6 9D CF 9C 33 15 49
11 8D 08 25 A3 81 CE 64 15 B7 43 92 22 B7 20 A1
0C DD A7 11 4F 79 A5 22 04 2A A6 3B 61 60 E2 34
CF 82 8B 58 4F E2 0B 50 FC E4 1B 63 18 33 1F F8
10 7B A5 31 CE D4 7C C9 84 5A DF C4 E0 6E CF 2A
74 1B D0 89 49 39 39 4A C7 F7 6C 1D 06 EB BE 0F
43 07 FB 66 DD EF BA 40 7F 1A 09 03 25 A0 85 B5
- 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
- 5E 7B 10 D1 2A C6 72 B8 33 80 B8 BA 80 5A A4 A4 - kontrolný súčet - 20 bajtov
- 9C 88 73 F8

- 8A 81 B6 DD 3E F3 BC 79 BC 81 F5 B9 CE 34 FC 27 - elektronický podpis - 48 bajtov
- A3 8D 8E F9 CA 80 18 E8 E5 5F EA 04 0A FA DC C6
- D3 1F E7 5D D1 1A F5 BC F1 EB 5C D0 28 E5 15 CF

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 v tvare "big-endian". Pre rovnaké vstupné údaje, ktorými sú kontrolný súčet a verejný kľúč, algoritmus vygeneruje vždy iný podpis.

Výsledný dátový záznam

Podľa čl. 7 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
- 87 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 - 144 bajtov - dátový blok č. 1
C8 B5 B2 83 83 06 0D 63 E5 C2 F9 E6 84 81 0C 22
03 5F 13 E8 BD 3E 13 DE 91 D6 9D CF 9C 33 15 49
11 8D 08 25 A3 81 CE 64 15 B7 43 92 22 B7 20 A1
0C DD A7 11 4F 79 A5 22 04 2A A6 3B 61 60 E2 34
CF 82 8B 58 4F E2 0B 50 FC E4 1B 63 18 33 1F F8
10 7B A5 31 CE D4 7C C9 84 5A DF C4 E0 6E CF 2A
74 1B D0 89 49 39 39 4A C7 F7 6C 1D 06 EB BE 0F
43 07 FB 66 DD EF BA 40 7F 1A 09 03 25 A0 85 B5
- 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
- 8A 81 B6 DD 3E F3 BC 79 BC 81 F5 B9 CE 34 FC 27 - 48 bajtov - elektronický podpis
A3 8D 8E F9 CA 80 18 E8 E5 5F EA 04 0A FA DC C6
D3 1F E7 5D D1 1A F5 BC F1 EB 5C D0 28 E5 15 CF

Celková dĺžka dátového záznamu v príklade je 336 bajtov. Pri presiahnutí 480 bajtov sa skráti textové položky v dátových blokoch.

Registračným číslom kľúča elektronického podpisu uvedeným v hlavičke záznamu sa vyhľadáva verejný kľúč vydavateľa preukazu, ktorým možno overiť platnosť podpisu.