Metodické usmernenie č. 13/2010-R
zo 7. júla 2010
o štruktúre údajov a technickom vyhotovení preukazu študenta

Gestorský útvar: sekcia vysokých škôl tel.: 02/59 37 43 56 2010-8452/24813:8-071

Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky (ďalej len „ministerstvo“) v súlade s § 67 ods. 2 zákona č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) a čl. 11 Organizačného poriadku Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky vydáva toto metodické usmernenie:

Prvá časť

Čl. 1
Úvodné ustanovenia

(1) Toto metodické usmernenie určuje:

a) využitie

1. pamäťových blokov pri použití čipu Mifare Standard alebo
2. aplikácií pri použití čipu Mifare DESFire EV1,

b) identifikáciu jednotlivých aplikácií pomocou AID, a to

1. adresár MAD2 pre Mifare Standard alebo
2. adresár MAD3 pre Mifare DESFire EV1,

c) štruktúru údajov v rámci

1. pamäťových blokov pre Mifare Standard alebo
2. súborov v rámci aplikácií pre Mifare DESFire EV1,

d) technickú špecifikáciu kontaktného čipu a popis ovládačov pre použitie elektronického podpisu pri použití preukazu ako bezpečného úložiska PKI kľúčov pre použitie elektronického podpisu.

(2) Ak sa vysoká škola v Slovenskej republike (ďalej len „vydavateľ preukazu“) rozhodne vydávať svojim vysokoškolským učiteľom preukaz učiteľa, prípadne svojim iným zamestnancom preukaz zamestnanca, odporúča sa použiť toto usmernenie aj pre štruktúru údajov a technické vyhotovenie týchto preukazov.

(3) Na účely tohto usmernenia sa preukazom rozumie preukaz študenta vysokej školy, preukaz učiteľa, preukaz zamestnanca alebo iný typ preukazu vydávaný vydavateľmi preukazu.

Čl. 2
Technické vyhotovenie preukazu

(1) Preukaz je vyhotovený na báze bezkontaktnej alebo hybridnej čipovej karty. Bezkontaktná časť spĺňa normu ISO/IEC 14443A, najmenej v častiach 1 až 3. Pre zápis štruktúry údajov, určenej týmto metodickým usmernením, je použitý bezkontaktný čip Mifare Standard alebo Mifare DESFire EV1.

(2) Vzhľadom na životnosť čipových kariet garantovanú výrobcom sa odporúča bezkontaktné alebo hybridné čipové karty vydávať najviac na dobu šesť rokov.

Čl. 3
Štruktúra údajov na preukaze

(1) Na prednej strane preukazu študenta sa uvádzajú

a) nápis „Študent“ alebo „Preukaz študenta“ pre študenta v dennej forme štúdia, nápis „Externý študent“ pre študenta v externej forme štúdia,

b) názov a sídlo vydavateľa preukazu študenta,

c) názov fakulty, ak sa študijný program, na ktorého štúdium je držiteľ preukazu študenta zapísaný, uskutočňuje na fakulte,

d) meno a priezvisko držiteľa preukazu študenta spolu s akademickými titulmi, vedecko-pedagogickými titulmi a umelecko-pedagogickými titulmi a vedeckými hodnosťami,

e) údaj o dátume narodenia držiteľa preukazu študenta v tvare „Narodený/á: <dátum>“,

f) údaj o začiatku platnosti preukazu študenta v tvare „Platný od: <dátum>“,

g) jedinečné číslo preukazu študenta, ktorým je sériové číslo bezkontaktného čipu karty Mifare,

h) ak je preukaz študenta vydaný v grafickom vyhotovení ISIC, údaj o dobe platnosti licencie ISIC je v tvare „Platnosť licencie ISIC do:“ a nápis „POZRI RUB“,

i) fotografia držiteľa preukazu študenta zobrazujúca jeho aktuálnu podobu; fotografia je čierno-biela alebo farebná, minimálny rozmer 2,5 x 3,0 cm, maximálny rozmer 3,0 cm x 3,5 cm, minimálna výška tváre je 2,0 cm; tituly podľa písmena d) sa uvádzajú v takom rozsahu, aby nezasahovali do fotografie,

j) nápis „Tento preukaz je vydaný podľa zákona č. 131/2002 Z. z. a je dokladom o štúdiu jeho držiteľa na vysokej škole. Preukaz je vydaný najviac na dobu 6 rokov od dátumu začiatku platnosti preukazu.“, ak preukaz študenta nie je vydaný v grafickom vyhotovení ISIC.

(2) Ak je preukaz študenta vydaný v grafickom vyhotovení ISIC, na zadnej strane preukazu študenta sa uvádzajú

a) údaj o konci platnosti licencie ISIC v tvare „Platnosť licencie ISIC do: <09/RRRR>“, ktorý vyjadruje maximálnu dobu platnosti licencie ISIC v príslušnom akademickom roku,

b) nápis „Tento preukaz je vydaný podľa zákona č. 131/2002 Z. z. a je dokladom o štúdiu jeho držiteľa na vysokej škole. Tento preukaz je vydaný najviac na dobu 6 rokov od dátumu začiatku platnosti preukazu.“ a

c) podpisové pole a nápis „PODPIS DRŽITEĽA PREUKAZU:“.

(3) Na prednej strane preukazu učiteľa sa uvádzajú

a) nápis „Učiteľ“, alebo „Preukaz učiteľa“,

b) názov a sídlo vydavateľa preukazu učiteľa,

c) názov fakulty, ak je držiteľ preukazu učiteľa v pracovnoprávnom vzťahu organizačne zaradený na fakulte vysokej školy,

d) meno a priezvisko držiteľa preukazu učiteľa spolu s akademickými titulmi, vedecko-pedagogickými titulmi a umelecko-pedagogickými titulmi a vedeckými hodnosťami,

e) údaj o dátume narodenia držiteľa preukazu učiteľa v tvare „Narodený/á: <dátum>“,

f) údaj o začiatku platnosti preukazu učiteľa v tvare „Platný od: <dátum>“,

g) údaj o dobe platnosti licencie ITIC v tvare „Platnosť licencie ITIC do:“ a nápis „POZRI RUB“, ak je preukaz učiteľa vydaný v grafickom vyhotovení ITIC,

h) jedinečné číslo preukazu učiteľa , ktorým je sériové číslo bezkontaktného čipu karty Mifare,

i) fotografia držiteľa preukazu učiteľa zobrazujúca jeho aktuálnu podobu; fotografia je čierno-biela alebo farebná, minimálny rozmer 2,5 x 3,0 cm, maximálny rozmer 3,0 cm x 3,5 cm, minimálna výška tváre je 2,0 cm; tituly podľa písmena d) sa uvádzajú v takom rozsahu, aby nezasahovali do fotografie,

j) nápis „Tento preukaz je vydaný najviac na dobu 6 rokov od dátumu začiatku platnosti preukazu.“, ak preukaz učiteľa nie je vydaný v grafickom vyhotovení ITIC.

(4) Ak je preukaz učiteľa vydaný v grafickom vyhotovení ITIC, na zadnej strane preukazu učiteľa sa uvádzajú

a) údaj o konci platnosti licencie ITIC v tvare „Platnosť licencie ITIC do: <12/RRRR>”,

b) nápis „Tento preukaz je vydaný najviac na dobu 6 rokov od dátumu začiatku platnosti preukazu.“ a

c) podpisové pole a nápis „PODPIS DRŽITEĽA PREUKAZU:“.

(5) Na prednej strane preukazu iného zamestnanca sa uvádzajú údaje podľa odseku 3 okrem údajov podľa odseku 3 písm. a) a c).

(6) Údaj o konci platnosti licencie ISIC alebo ITIC sa nachádza na prolongačnej známke, ktorá je zhotovená z holografickej samodeštrukčnej fólie. V roku vydania preukazu môže byť tento údaj vytlačený priamo na preukaze. Na prolongačnej známke môže byť aj ďalší text, nesmie však vizuálne potláčať údaj o platnosti preukazu.

(7) Dátum sa na miestach označených „<dátum>” uvádza v tvare DD/MM/RRRR alebo DD.MM.RRRR, kde DD je číselné vyjadrenie dňa, MM je číselné vyjadrenie mesiaca a RRRR je číselné vyjadrenie roku. Na miestach označených „<dátum-MR>“ sa dátum uvádza v tvare MM/RRRR alebo MM.RRRR.

(8) Údaje uvedené v odsekoch 1 až 5 sú povinné podľa príslušného typu preukazu; údaje podľa odseku 1 písm. c) a odseku 3 písm. c) a tituly podľa odseku 1 písm. d) a odseku 3 písm. d) sú nepovinné. Okrem nich môže vydavateľ preukazu umiestniť na preukaz aj ďalšie údaje tak, aby sa nenarušila čitateľnosť informácií na preukaze.

Čl. 4
Grafické vyhotovenie preukazu

(1) Pre študentov v dennej forme štúdia sa odporúča použitie grafického vyhotovenia medzinárodného študentského preukazu ISIC.

(2) Pre vysokoškolských učiteľov sa odporúča použitie grafického vyhotovenia medzinárodného preukazu učiteľa ITIC.

Čl. 5
Platnosť preukazu

(1) Začiatok platnosti preukazu študenta je určený podľa § 69 ods. 1 zákona. Koniec platnosti preukazu študenta je určený podľa § 69 ods. 2 zákona. Maximálna doba platnosti aplikácií preukazu študenta vzťahujúcich sa na štátom garantované zľavy je do 30. septembra nasledujúceho akademického roku.

(2) Ak osoba prestane byť študentom podľa § 65 alebo 66 zákona, vydavateľ preukazu zabezpečí

a) deaktiváciu nároku na štátom garantované zľavy vo všetkých aplikáciách a

b) zmenu dátumu

1. položky č. 3 v prílohe č. 1 pri použití čipu Mifare Standard alebo
2. položky č. 12 v prílohe č. 2 pri použití čipu Mifare DESFire EV1.

Druhá časť

Preukaz typu Mifare Standard

Čl. 6
Údaje uložené v pamäti bezkontaktného čipu preukazu typu Mifare Standard a ich štruktúra

(1) Štruktúru údajov v pamäti preukazu (ďalej len „záznam“) tvorí súbor s veľkosťou 256 bajtov.

(2) Záznam pozostáva z hlavičky a z tela záznamu obsahujúceho jednotlivé údajové položky záznamu (ďalej len „položka“). V každej položke je uložený jeden personalizačný údaj. Každej položke je jednoznačne priradený typ položky, ktorým je číslo z intervalu 0 až 255.

(3) Hlavička záznamu pozostáva z 2N + 5 bajtov, kde N je počet položiek záznamu. Štruktúra hlavičky je nasledovná

a) prvý bajt obsahuje počet položiek v zázname,

b) druhý bajt obsahuje číslo verzie záznamu; záznam určený týmto metodickým usmernením má číslo verzie 4,

c) tretí bajt obsahuje verziu šifrovania dát,

d) štvrtý bajt obsahuje verziu podpisu dát,

e) piaty bajt obsahuje veľkosť zašifrovaných dát,

f) šiesty bajt obsahuje typ prvej položky záznamu,

g) siedmy bajt obsahuje poradové číslo (offset) prvého bajtu prvej položky záznamu,

h) ôsmy bajt obsahuje typ druhej položky záznamu,

i) deviaty bajt obsahuje poradové číslo (offset) prvého bajtu druhej položky záznamu,

j) 2N+5 bajt obsahuje typ N-tej položky záznamu,

k) 2N+6 bajt obsahuje poradové číslo (offset) prvého bajtu N-tej položky záznamu,

l) poradové číslo (offset) prvého bajtu (prvej) položky záznamu relatívne k začiatku sektora s číslovaním od 0.

(4) Zoznam údajových položiek záznamu je v prílohe č. 1

(5) Ak celková veľkosť záznamu vrátane podpisu presiahne veľkosť 240 bajtov, dlhé položky sú skrátené proporcionálne takým spôsobom, aby žiadna skrátená položka nebola kratšia ako hodnota uvedená v stĺpci „Garantovaná veľkosť v bajtoch“ v prílohe č. 1.

(6) Záznam obsahuje všetky položky podľa odseku 4, ktoré nie sú prázdne. Okrem nich neobsahuje žiadne iné položky.

(7) Kódovanie údajov je takéto

a) „číslo“ je binárne kódované číslo,

b) „text“ je textový reťazec v kódovaní podľa normy ISO 8859-2 ukončený binárnym znakom 0,

c) „dátum“ je dátum uložený v tvare DMRR, kde D obsahuje binárne kódovaný deň v mesiaci s hodnotami 1 až 31, M binárne kódovaný mesiac s hodnotami 1 až 12 a RR binárne kódovaný rok vo formáte little-endian,

d) „ID“ je osobné číslo vo formáte textového reťazca, ktorý môže obsahovať ľubovoľné alfanumerické znaky uložené v kódovaní ASCII a je ukončený binárnym znakom 0, tak aby ním nebol všeobecne použiteľný identifikátor podľa osobitného predpisu[1)]; prideľovanie osobných čísel je v pôsobnosti vydavateľa preukazu.

(8) Položky vo formáte „číslo“ a „dátum“ majú pevnú veľkosť určenú v poslednom stĺpci tabuľky v prílohe č. 1. Položky vo formáte „text“ a „ID“ majú premenlivú veľkosť podľa skutočnej veľkosti v nich uloženého personalizačného údaja.

(9) Údaje sú zašifrované algoritmom definovaným v hlavičke záznamu. Šifrujú sa všetky údaje od šiesteho bajtu. Pred šifrovaný blok údajov sa doplní 4 bajtové SNR pri použití čipu Mifare Standard. Zarovnanie údajov je definované typom šifrovacieho algoritmu

a) 1-3DES-CBC 2KEY, padding Method 0 (podľa normy ISO 9797),

b) 2-AES-128.

(10) Integrita dát je zabezpečená MAC, ktorý nasleduje za blokom zašifrovaných údajov. Veľkosť MAC je definovaná typom podpisovacieho algoritmu

a) 1-3DES-CBC-MAC8 (podľa normy ISO 9797) M2 ALG1,

[1)] Zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov.

b) 2-3DES-CBC-MAC8 (podľa normy ISO 9797) M2 ALG3

c) 3-3DES-CBC-MAC8 (podľa normy ISO 9797) M2 ALG3 vstupné údaje SHA -2,

d) 4-asymetrický podpis ECDSA SHA-1.

(11) Ak nie je možné uložiť v zázname údaje podľa prílohy č. 1 v plnom rozsahu, niektoré položky s premenlivou veľkosťou sú skrátené tak, že príslušný personalizačný údaj v nich nebude uložený úplný.

(12) Pri určovaní veľkosti položiek záznamu ostáva pre každý údaj k dispozícii priestor nie menší, ako je uvedené v poslednom stĺpci tabuľky v prílohe č. 1.

(13) Ak sa vydavateľ preukazu rozhodne použiť pre preukazy učiteľov a preukazy iných zamestnancov, prípadne iných používateľov informačných systémov bezkontaktné čipové karty zodpovedajúce norme ISO/IEC 14443A, odporúča sa použitie štruktúry údajov podľa odsekov 3 a 4 aj pre tieto preukazy.

(14) Za správnosť a aktuálnosť údajov podľa odseku 4 v zariadení na zápis údajov zodpovedá vydavateľ preukazu. Prístupové práva k týmto údajom sú nastavené tak, že

a) zápis údajov alebo ich zmenu môže uskutočniť iba vydavateľ preukazu,

b) čítanie údajov je možné pre všetkých vydavateľov preukazu, pre ministerstvo a pre iné fyzické osoby alebo právnické osoby podľa § 73 ods. 5 zákona.

(15) Presný popis použitia algoritmov vrátane príkladov šifrovania a podpisovania sa poskytne na žiadosť podľa osobitného prepisu[1]).

Čl. 7
Technické vyhotovenie preukazu pri použití čipu Mifare Standard

(1) Presné označenie čipu je Mifare Standard (Classic) 4kB, MF1 IC S70.

(2) Pri práci s aplikačnými sektormi sa využíva adresár podľa štandardu Mifare Application Directory (MAD). Aplikácia „Preukaz študenta“ má unikátny identifikátor z medzinárodného registra aplikácií, ktorý má hodnotu 0x581C.

(3) Záznam je uložený v prvých 256 bajtoch tretieho kilobajtu pamäti preukazu, t.j. v sektore 0x20.

(4) Kód pre prístupové práva k záznamu sa nastaví na hodnotu 0x78778800.

(5) Na uloženie ďalších centrálne určených údajov v budúcnosti sa v pamäti preukazu rezervuje druhých a tretích 256 bytov tretieho kilobajtu, t.j. sektory 0x21 a 0x22 v čipe Mifare Standard 4kB.

(6) Odporúča sa vyhradiť

a) prvý kilobajt pamäte preukazu, ktorý obsahuje sektory 0x00-0x0F, pre aplikácie umožňujúce použitie preukazu na preukázanie nároku na študentskú zľavu, časový lístok prípadne na elektronickú peňaženku Železničnej spoločnosti Slovensko, dopravných spoločností SAD a podnikov mestskej hromadnej prepravy osôb a

b) priestor v pamäti preukazu pre aplikáciu „Knižničný (kultúrny) preukaz“, umožňujúcu použitie preukazov v akademických a vedeckých knižniciach, prípadne ďalších kultúrnych a vzdelávacích organizáciách v rezorte kultúry.

(7) Kľúč „KEY B“ na zápis do súboru je diverzifikovaný a pre každú kartu jedinečný. Vydavateľ preukazu je zodpovedný za jeho ochranu pred prezradením alebo stratou.

Kľúč „KEY A“ na čítanie záznamu sa oznamuje všetkým vydavateľom preukazu, prípadne iným právnickým osobám alebo fyzickým osobám podľa § 73 ods. 5 zákona. Vydavateľ preukazu zabezpečí ochranu kľúčov na čítanie pred stratou. Spôsob zabezpečenia je popísaný v bezpečnostnom projekte na základe osobitného prepisu.[1]) Všetky strany, ktoré majú prístup ku kľúčom na čítanie záznamu zabezpečia ich ochranu pred prezradením. Šifrovanie údajov a overovanie podpisov sa vykonáva bezpečným spôsobom.

(8) Údaje v čipe preukazu sú zabezpečené šifrovaním ľubovoľným algoritmom podľa Čl. 6 ods. 9 a podpísané ľubovoľným algoritmom podľa Čl. 6 ods. 10.

Tretia časť

Preukaz typu Mifare DESFire EV1

Čl. 8
Údaje uložené v pamäti bezkontaktného čipu preukazu typu Mifare DESFire EV1 a ich štruktúra

(1) Údaje o držiteľovi preukazu sa ukladajú do jednej aplikácie, pričom sú zapísané v dvoch súboroch v štruktúre podľa odsekov 2 až 5.

(2) „Súbor 0“ obsahuje údaje podľa prílohy č. 2.

(3) Pre zápis údajov o držiteľovi preukazu sa pre súbor 0 vyhradí veľkosť 192 bajtov takto

a) verzia záznamu personálnych údajov s číselnou hodnotou 1; ak sa zmení štruktúra dát v súbore 0, zmení sa verzia záznamu,

b) verzia elektronického podpisu personálnych dát s číselnou hodnotou 1; ak sa zmení šifrovane štruktúry dát v súbore 0, zmení sa verzia záznamu,

c) verzia kľúčov s číselnou hodnotou 1; ak sa zmenia šifrovacie kľúče v súbore 0, zmení sa hodnota verzie kľúčov,

d) údaj o druhu preukazu s číselnými hodnotami

1. „1“ pre študenta v dennej forme štúdia,
2. „2“ pre študenta v externej forme štúdia,
3. „3“ pre vysokoškolského učiteľa,
4. „4“ pre iného zamestnanca,
5. „5“ pre iného používateľa,

e) údaj o stupni štúdia s veľkosťou 1 bajt a číselnými hodnotami

1. „1“ pre študijný program prvého stupňa na vysokej škole,
2. „2“ pre študijný program druhého stupňa na vysokej škole,
3. „3“ pre študijný program tretieho stupňa na vysokej škole,

f) pohlavie s veľkosťou 1 bajt v textovom formáte s hodnotami „M“ alebo „F“,

g) akademické tituly, vedecko-pedagogické tituly a umelecko-pedagogické tituly pred menom v textovom formáte s vyhradenými 19 bajtmi pre zápis; textový zápis je ukončený ukončovacím znakom 0x00,

h) meno a priezvisko v textovom formáte s vyhradenými 56 bajtmi pre zápis; jednotlivé položky sú oddelené podľa RLC (Run Length Coding) kódovania a textový zápis je ukončený ukončovacím znakom 0x00,

i) akademické tituly a vedecké hodnosti za menom v textovom formáte s vyhradenými 12 bajtmi pre zápis; textový zápis je ukončený ukončovacím znakom 0x00,

j) dátum narodenia vo formáte podľa odseku 6 písm. c),

k) začiatok platnosti preukazu vo formáte podľa odseku 6 písm. c),

l) koniec platnosti aplikácií preukazu vzťahujúcich sa na štátom garantované zľavy vo formáte podľa odseku 6 písm. c),

m) názov a sídlo vydavateľa preukazu a názov fakulty v textovom formáte ako 6 bajtový textový reťazec podľa katalógu VSFAKU JUZ; textový zápis je ukončený ukončovacím znakom 0x00,

n) rezerva na zarovnanie,

o) elektronický podpis, pričom údaje budú podpísané ľubovoľným algoritmom podľa Čl. 6 ods. 10; pre podpis sa použije algoritmus s kľúčom dlhým 160 bitov, dĺžka podpisu je 40 bajtov (320 bitov) a dĺžka poľa 64 bajtov umožní budúce rozšírenie kľúča.

(4) „Súbor 1“ obsahuje údaje podľa prílohy č. 3.

(5) Pre zápis údajov o držiteľovi preukazu sa pre súbor 1 vyhradí veľkosť 192 bajtov takto

a) verzia záznamu personálnych údajov s číselnou hodnotou 1; ak sa zmení štruktúra údajov v súbore 1, zmení sa verzia záznamu,

b) verzia elektronického podpisu personálnych údajov s číselnou hodnotou 1; ak sa zmení šifrovanie štruktúry údajov v súbore 1, zmení sa verzia záznamu,

c) verzia kľúčov s číselnou hodnotou 1; ak sa zmenia šifrovacie kľúče v súbore 1, zmení sa hodnota verzie kľúčov,

d) jednoznačný identifikátor držiteľa preukazu určený vydavateľom preukazu v textovom formáte; textový zápis je ukončený ukončovacím znakom 0x00,

e) názov ulice a číslo domu, kde má držiteľ preukazu trvalý pobyt v textovom formáte; textový zápis je ukončený ukončovacím znakom 0x00,

f) názov obce, v ktorej má držiteľ preukazu trvalý pobyt v textovom formáte; textový zápis je ukončený ukončovacím znakom 0x00,

g) poštové smerové číslo obce, v ktorej má držiteľ preukazu trvalý pobyt v číselnom formáte,

h) rezerva na zarovnanie,

i) elektronický podpis, pričom údaje budú podpísané ľubovoľným algoritmom podľa Čl. 6 ods. 10; pre podpis sa využije algoritmus s kľúčom dlhým 160 bitov, dĺžka podpisu je 40 bytov (320 bitov) a dĺžka poľa 64 byte umožní budúce rozšírenie kľúča.

(6) Kódovanie údajov je takéto

a) „číslo“ je binárne kódované číslo,

b) „text“ je textový reťazec v kódovaní UTF8 ukončený binárnym znakom 0,

c) „dátum“ je formát dátumu uložený v tvare DMRR, kde D obsahuje binárne kódovaný deň v mesiaci s hodnotami 1 až 31, M binárne kódovaný mesiac s hodnotami 1 až 12 a RR binárne kódovaný rok, formát little-endian,

d) „ID“ je osobné číslo vo formáte textového reťazca, ktorý môže obsahovať ľubovoľné alfanumerické znaky uložené v kódovaní ASCII a je ukončený binárnym znakom 0; prideľovanie osobných čísel je v pôsobnosti vydavateľa preukazu tak, aby ním nebol všeobecne vypovedajúci identifikátor podľa osobitného predpisu[1]),

e) „RLC kódovanie“ jednoznačne identifikuje prvý znak mena a prvý znak priezviska v textovom reťazci v kódovaní UTF8; nultý bajt je rozdelený na horné dva bity, ktoré určujú typ položky 00=meno alebo 01=priezvisko a spodných šesť bitov, ktoré určujú začiatok ďalšej položky.

(7) Integrita údajov je zabezpečená použitým kontrolným súčtom a elektronickým podpisom údajov. Elektronický podpis v súbore 0 i v súbore 1 zabezpečuje integritu údajov s jedinečným číslom čipu karty.

Čl. 9
Technické vyhotovenie preukazu pri použití čipu Mifare DESFire EV1

(1) Presné označenie čipu je Mifare DESFire EV1 4 kB/8 kB, MF3 IC D41/D81.

(2) Pri práci s aplikačnými sektormi sa využíva adresár podľa štandardu Mifare Application Directory (MAD). Aplikácia „Personálne údaje držiteľa preukazu“ má unikátny identifikátor z medzinárodného registra aplikácií, ktorý má hodnotu 0xF58510. Vydavatelia preukazu aplikácie sa odlišujú verziou zapisovacieho kľúča. Verzia kľúča sa získava APDU príkazom (0x64) - GetKeyVersion kľúča K3 podľa odseku 6 písm. d).

(3) Ak počet registrovaných subjektov vytvárajúcich aplikácie v čipe preukazu presiahne 256, bude použité nové AID aplikácie so zmeneným najnižším voľne použiteľným bitom AID (0xF58511). Zoznam platných AID vydavateľov preukazu sa poskytuje všetkým vydavateľom preukazu, prípadne ďalším fyzickým osobám alebo právnickým osobám podľa § 73 ods. 5 zákona.

(4) Šifrovanie údajov, overovanie podpisov a generovanie diverzifikovaných kľúčov sa vykonáva bezpečným spôsobom.

(5) Pre zabezpečenie operácií s čipom DESFire EV1 je definovaný „Master kľúč“, ktorý vlastní vydavateľ preukazu. Vydavateľ preukazu umožní vytvorenie aplikácií v čipe „PICC Master kľúč“ s označením „PMK“.

(6) Aplikácia „Personálne údaje držiteľa preukazu“ používa kľúče

a) master kľúč „AMK“ aplikácie „Personálne údaje držiteľa preukazu“,

b) kľúč „K1“ pre čítanie obsahu údajového súboru 0,

c) kľúč „K2“ pre čítanie obsahu údajového súboru 1,

d) prevádzkový kľúč „K3“ pre čítanie a zápis do údajového súboru 0 a 1,

e) kľúč „K4“ pre nastavenie práv pre prístup k jednotlivým súborom a

f) záložný kľúč „K5“.

(7) Čítacie kľúče k súborom 0 a 1, distribuované medzi všetkých vydavateľov preukazu, budú jednotné pre všetkých vydavateľov preukazu.

(8) Nastavenie kľúčov v súboroch pre

a) „Súbor 0“

1. kľúč pre čítanie „K1“,
2. kľúč pre zápis nie je definovaný ,
3. kľúč pre zápis a čítanie „K3“ a
4. kľúč pre nastavenie práv pre prístup k súboru „K4“,

b) „Súbor 1“

1. kľúč pre čítanie „K2“,
2. kľúč pre zápis nie je definovaný,
3. kľúč pre zápis a čítanie „K3“ a
4. kľúč pre nastavenie práv pre prístup k súboru „K4“.

(9) Typy kľúčov K1, K2, K3, K4 sú diverzifikované jedinečným číslom čipu (UID).

(10) Algoritmom diverzifikácie je algoritmus AES. Dĺžka kľúča je definovaná algoritmom AES 128 bitov.

(11) Pre zabezpečenie údajov aplikácie „Personálne údaje držiteľa preukazu“ sú definované kľúče

a) AK_Private ako súkromná časť kľúča pre vytvorenie elektronického podpisu a

b) AK_Public ako verejná časť kľúča pre overenie elektronického podpisu; kľúč AK_Public nie je potrebné chrániť, môže byť zverejnený na webovom sídle vydavateľa preukazu.

(12) Elektronický podpis je vytvorený 160 bitovým kľúčom algoritmom ECDSA. Podpisujú sa údaje vytvorené hašovacou funkciou SHA-1 z UID karty a údajov príslušného súboru.

(13) Vydavateľ preukazu zabezpečí bezpečné uloženie prístupových kľúčov pre komunikáciu s ním vydávanými preukazmi, napríklad modulu SAM. Bezpečné úložisko kľúčov rovnako zabezpečuje všetky šifrovacie operácie vykonávané s údajmi podľa príloh č. 2 a 3.

(14) Vlastník kľúčov, ktorým je vydavateľ preukazu, zabezpečí ochranu všetkých kľúčov pred stratou. Všetky strany, ktoré majú prístup ku kľúčom na čítanie záznamu, zabezpečia ich ochranu pred prezradením.

(15) Ministerstvo odporúča rezervovať priestor v pamäti preukazu pre

a) aplikácie umožňujúce použitie preukazu na preukázanie nároku na študentskú zľavu, časový lístok prípadne na elektronickú peňaženku Železničnej spoločnosti Slovensko, dopravných spoločností SAD a podnikov mestskej hromadnej prepravy osôb a

b) aplikáciu „Knižničný (kultúrny) preukaz“, umožňujúcu použitie preukazov v akademických a vedeckých knižniciach, prípadne ďalších kultúrnych a vzdelávacích organizáciách v rezorte kultúry.

Štvrtá časť

Kontaktný čip

Čl. 10
Technické vyhotovenie preukazu pri použití kontaktného čipu

(1) Preukaz môže byť bezpečným úložiskom PKI kľúčov pre použitie elektronického podpisu, a to použitím kontaktného čipu podľa štandardu ISO 7816-1, ISO 7816-2, ISO 7816-3 a ISO 7816-4 a aplikácií tohto čipu.

(2) Kontaktný čip je procesorový čip s kryptografickým koprocesorom. Koprocesor musí podporovať aspoň algoritmus RSA s dĺžkou kľúčov 2048 bitov.

(3) Operačný systém podporuje GlobalPlatform 2.1.1, SCP 01 a 02 alebo novšie verzie.

(4) Pamäť (EEPROM) kontaktného čipu má aspoň 72kB.

(5) Bezpečnostná certifikácia čipu a operačného systému je aspoň FIPS 140-2 level 3, prípadne CC EAL 4; relevantné profily ochrany sú tie, ktoré sú založené na Global Platform Smart Card Security Target Guidelines a Secure Signature-Creation Device.

Čl. 11
Aplikácia pre podporu práce s kľúčmi a certifikátmi

(1) V ROM alebo EEPROM pamäti kontaktného čipu je uložená aspoň jedna PKI aplikácia, podporujúca

a) generovanie páru kľúčov vo vnútri čipu,

b) kryptografické operácie so súkromným kľúčom vo vnútri čipu,

c) možnosť importovať pár kľúčov do čipu,

d) nemožnosť exportovať súkromný kľúč z čipu,

e) nemožnosť prečítať súkromný kľúč z čipu,

f) použitie súkromných kľúčov len po úspešnej autentizácii oprávneného držiteľa preukazu prostredníctvom príslušného PIN kódu; použitie súkromného kľúča bez predchádzajúcej úspešnej autentizácie pomocou PIN je neprípustné,

g) zablokovanie PIN kódu po niekoľkých neúspešných pokusoch o jeho overenie; dôsledkom zablokovania PIN je nemožnosť použitia príslušných súkromných kľúčov,

h) uloženie certifikátov X.509 k užívateľským kľúčom, prípadne aj certifikačných autorít,

i) uloženie všeobecných dátových objektov, pri ktorých je možné zvoliť, či majú byť voľne čitateľné alebo čitateľné až po úspešnej autentizácii oprávneného držiteľa preukazu prostredníctvom PIN,

j) uloženie atribútov objektov; aspoň

1. popis a identifikátor pre objekty typu verejný kľúč, súkromný kľúč a certifikát,
2. rozlíšenie použitia kľúča aspoň pre operácie sign/verify a encrypt/decrypt a
3. názov aplikácie, popis a identifikátor pre všeobecné dátové objekty,

k) rozlíšenie oblastí pre elektronický podpis a zaručený elektronický podpis podľa všeobecne záväzných právnych predpisov v oblasti elektronického podpisu a zaručeného elektronického podpisu,

l) vykonanie operácie bezpečnej reinicializácie oblasti preukazu, najmä oblasti dát PKI aplikácie, pri zachovaní čísla preukazu v pamäti čipu

1. bezpečným odstránením všetkých užívateľských dát v čipe, najmä kľúčov, certifikátov a dátových objektov formou atomickej operácie a

2. nastavením PIN alebo PUK oblasti na neinicializované hodnoty alebo na hodnoty vopred známe.

(2) Čip obsahuje inicializovanú oblasť pre elektronický podpis; môže obsahovať aj oblasť pre zaručený elektronický podpis.

(3) Ak sú v čipe oblasti pre elektronický podpis aj pre zaručený elektronický podpis

a) kontaktný čip preukazu má certifikáciu Národného bezpečnostného úradu a

b) každá oblasť má vlastnú oddelenú sadu PIN, prípadne PUK pre autorizáciu prístupu k údajom a operáciám so súkromnými kľúčmi.

Čl. 12
Technická špecifikácia ovládačov kontaktných čipov

(1) Spolu s kontaktnými čipmi sú vždy dodané ovládače pre ich aplikačné využitie, ktoré implementujú štandardné rozhranie PKCS#11. Pre oblasť elektronického podpisu je dodaný aj ovládač implementujúci rozhranie do CryptoAPI typu CSP alebo CNG KSP operačného systému MS Windows.

(2) PKCS#11 ovládač pre zaručený elektronický podpis musí byť možné používať na bezpečné generovanie a uloženie kľúčových párov súkromného a verejného kľúča, na vyhotovovanie a overovanie zaručeného elektronického podpisu, uloženie kvalifikovaných certifikátov a certifikátov a ich použitie v aplikáciách podporujúcich elektronické podpisovanie.

(3) Okrem štandardných funkcií musia ovládače implementovať funkcie pre prečítanie plného sériového čísla preukazu

a) pre Mifare Standard obsahujúceho 10 číslic,

b) pre Mifare DESFire EV1 obsahujúceho 17 číslic.

(4) Spôsob čítania sériového čísla preukazu z kontaktného čipu je

a) volaním CryptGetProvParam/PP_SMARTCARD_GUID cez CryptoAPI,

b) volaním NCryptGetProperty/NCRYPT_SMARTCARD_GUID_PROPERTY cez CryptoAPI s podporou CNG,

c) volaním C_GetTokenInfo a čítaním serialNumber v štruktúre CK_TOKEN_INFO; tento spôsob je použiteľný len pre preukazy s bezkontaktným čipom Mifare Standard,

d) čítaním hodnoty atribútu CKA_SERIAL_NUMBER objektu CKO_HW_FEATURE cez PKCS#11.

(5) Spôsob vykonania operácie bezpečnej reinicializácie oblasti dát PKI aplikácie preukazu je

a) volaním C_InitToken cez PKCS#11 tak že,

1. ak parameter pLabel obsahuje binárne nuly, nový Label je implicitne vyplnený názvom a číslom preukazu,
2. ak sú parametre pPin/ulPinLen prázdne (NULL/0), PKCS#11 knižnica zobrazí vlastné grafické rozhranie pre zadanie nové hodnoty PUK,
3. PIN je možné inicializovať volaním funkcií C_SetPIN alebo C_InitPIN; ak hodnota PIN nie je predaná v parametroch funkcií, PKCS#11 knižnica zobrazí vlastné grafické rozhranie pre zadanie nové hodnoty PIN,

b) volaním CryptSetProvParam/PP_REINITIALIZE_SMARTCARD (0x8A500001) cez CryptoAPI, tak, že

1. parameter pbData môže voliteľne odkazovať na dva po sebe nasledujúce, nulou ukončené reťazce s novými hodnotami PUK a PIN,
2. ak nové hodnoty PUK a PIN nie sú uvedené, CSP knižnica zobrazí vlastné grafické rozhranie pre zadanie nových hodnôt PUK a PIN,

c) volaním NCryptSetProperty/NCRYPT_REINITIALIZE_SMARTCARD (L“ReinitializeSmartCard“) cez CryptoAPI s podporou CNG tak, že

1. parameter pbInput môže voliteľne odkazovať na dva po sebe nasledujúce, nulou ukončené reťazce s novými hodnotami PUK a PIN,
2. ak nové hodnoty PUK a PIN nie sú uvedené, KSP knižnica zobrazí vlastné grafické rozhranie pre zadanie nových hodnôt PUK a PIN.

(6) Ovládače musia byť dostupné aspoň pre 32bit aj 64bit operačné systémy MS Windows 2000 a vyššie a Linux (aspoň 3 bežne užívané distribúcie).

Piata časť

Elektronický podpis

Čl. 13
Oblasť pre elektronický podpis akceptovaný v rezorte školstva

(1) Certifikáty používané v oblasti pre elektronický podpis akceptovaný v rezorte školstva vydáva „Certifikačná autorita rezortu školstva“.

(2) Požadované vlastnosti PKI aplikácie pre prácu s oblasťou pre nekvalifikované certifikáty

a) sériové číslo uložené v kontaktnom čipe preukazu je zhodné so sériovým číslom (SNR, UID) bezkontaktného čipu podľa tohto usmernenia

1. pre Mifare Standard štvorbajtové,
2. pre Mifare DESFire EV1 sedembajtové,

b) v pamäti kontaktného čipu je v rámci oblasti elektronického podpisu uložený bezpečnostný prvok preukazujúci pravosť sériového čísla preukazu formou elektronického podpisu sériového čísla preukazu; bezpečnostný prvok je vytvorený v rámci prvotnej inicializácie kontaktného čipu a v priebehu života nesmie byť dovolené jeho vymazanie, či modifikácia,

c) ovládače dodané k preukazom umožňujú kontrolu bezpečnostného prvku podľa písmena b) minimálne pred prvou operáciou vykonanou s kontaktným čipom po jeho

vložení do čítačky; ak je bezpečnostný prvok porušený, nesmie byť ďalšia práca s oblasťou elektronického podpisu čipu umožnená,

d) priestor pre uloženie minimálne 6 RSA kľúčov dĺžky 2048 bitov, zostávajúci priestor môže byť obsadený aj kľúčmi menšej dĺžky,

e) priestor pre uloženie užívateľských certifikátov X.509, celkom aspoň 12KB,

f) priestor pre uloženie 2 koreňových certifikátov, celkom aspoň 4KB,

g) priestor pre všeobecné dátové objekty nechránené pomocou PIN aspoň 4KB,

h) priestor pre všeobecné dátové objekty chránené pomocou PIN aspoň 3KB,

i) podpora Smart Card Logon do OS Windows,

j) podpora diakritiky v certifikátoch,

k) automatická registrácia certifikátov na karte do operačného systému pri vložení karty a pri vybratí karty automatické odstránenie certifikátov z operačného systému.

Čl. 14
Oblasť pre zaručený elektronický podpis

Požadované vlastnosti PKI aplikácie pre prácu s oblasťou pre kvalifikované certifikáty

a) sériové číslo uložené v kontaktnom čipe preukazu je zhodné so sériovým číslom (SNR, UID) bezkontaktného čipu, podľa tohto usmernenia

   1. pre Mifare Standard štvorbajtové,

   2. pre Mifare DESFire EV1 sedembajtové,

b) v pamäti kontaktného čipu je v rámci oblasti zaručeného elektronického podpisu uložený bezpečnostný prvok preukazujúci pravosť sériového čísla preukazu formou elektronického podpisu sériového čísla preukazu; bezpečnostný prvok je vytvorený v rámci prvotnej inicializácie kontaktného čipu a v priebehu života nesmie byť dovolené jeho vymazanie, či modifikácia,

c) ovládače dodané k preukazom umožňujú kontrolu bezpečnostného prvku podľa písmena b) minimálne pred prvou operáciou vykonanou s kontaktným čipom po jeho vložení do čítačky; ak je bezpečnostný prvok porušený, nesmie byť ďalšia práca so oblasťou čipu pre zaručený elektronický podpis umožnená,

d) priestor pre minimálne 2 RSA kľúče dĺžky 2048 bitov,

e) priestor pre uloženie užívateľských certifikátov X.509 aspoň 3KB,

f) priestor pre uloženie 2 koreňových certifikátov aspoň 4KB.

Šiesta časť

Čl. 15
Používanie preukazov inými fyzickými osobami alebo právnickými osobami podľa § 73 ods. 5 zákona

(1) Vydavateľ preukazu môže so zvyšným pamäťovým priestorom v bezkontaktnom čipe nakladať spôsobom, ktorý uzná za vhodný. Časti tohto pamäťového priestoru môžu byť

vydavateľom preukazu poskytnuté pre aplikácie iných fyzických osôb alebo právnických osôb podľa § 73 ods. 5 zákona.

(2) Aplikácie iných fyzických osôb alebo právnických osôb podľa § 73 ods. 5 zákona môžu používať zmluvne dohodnuté osobné údaje z aplikácie „Personálne údaje držiteľa preukazu“, pričom s nimi nakladajú spôsobom a zabezpečujú ich náležitú ochranu podľa osobitného predpisu[1]).

(3) Vydavateľ preukazu zodpovedá za správnosť osobných údajov v aplikácii „Personálne údaje držiteľa preukazu“ podľa Čl. 8 ods. 2 až 5. Iná fyzická osoba alebo právnická osoba podľa § 73 ods. 5 zákona zodpovedá za správnosť údajov vo svojej aplikácii na preukaze.

(4) Údaje podľa Čl. 8 ods. 2 nahrádzajú v celom rozsahu papierové potvrdenie školy o nároku na štátom garantovanú zľavu pre študenta dennej formy štúdia do 26 rokov.

Siedma časť

Spoločné, zrušovacie a záverečné ustanovenia

Čl. 16

(1) Technologické a informatické skratky použité v usmernení sú vysvetlené v prílohe č. 4.

(2) Grafické vyhotovenie preukazov vydaných pred 1. januárom 2011 nie je potrebné meniť.

Čl. 17

Zrušuje sa usmernenie č. CD-2004-3048/6280-1:sekr. zo dňa 1. marca 2004.

Čl. 18
Účinnosť

Toto metodické usmernenie nadobúda účinnosť 1. januára 2011.

minister

Zoznam príloh

Obsah