Metodické usmernenie č. 16/2014
o použití, štruktúre údajov a technickom vyhotovení preukazu študenta

Gestorský útvar: sekcia vysokých škôl tel.: 02 / 59 374 356 2014-6277/18997:2-15A0

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
Špecifikácia a spôsob použitia preukazu

Čl. 1
Úvodné ustanovenia a vymedzenie niektorých pojmov

(1) Toto metodické usmernenie určuje:

a) spôsob použitia, vyhotovenie a vizuálnu úpravu preukazu,

b) údaje o držiteľovi preukazu a spôsob ich zápisu do bezkontaktného pamäťového čipu v preukaze (ďalej len „čip“),

c) technickú špecifikáciu kontaktného čipu v preukaze a spôsob jeho použitia na bezpečné uloženie kľúčov PKI pre elektronický podpis držiteľa preukazu.

(2) Na účely tohto usmernenia

a) preukazom je preukaz študenta vysokej školy, preukaz vysokoškolského učiteľa, preukaz iného zamestnanca vysokej školy alebo iný preukaz vydaný podľa tohto usmernenia,

b) vydavateľom preukazu je vysoká škola pôsobiaca v Slovenskej republike podľa zákona; ak ide o zahraničnú vysokú školu, vydavateľom preukazu je len ak uskutočňuje akreditované študijné programy podľa zákona a ide o študenta niektorého z týchto študijných programov,

c) držiteľom preukazu je študent vysokej školy, vysokoškolský učiteľ alebo iný zamestnanec vysokej školy, ktorého osobné údaje sú viditeľne uvedené na preukaze a elektronicky zapísané v pamäti preukazu,

d) poskytovateľom služieb je právnická osoba alebo fyzická osoba, ktorá je na základe dohody s vydavateľom preukazu alebo s ministerstvom oprávnená čítať údaje z pamäte preukazu v súvislosti s poskytovaním služieb vyžadujúcich použitie preukazu,

e) UID preukazu je unikátny identifikátor bezkontaktného čipu v preukaze,

f) aplikáciou je osobitná časť pamäťového priestoru bezkontaktného čipu v preukaze, ktorá je vyhradená na konkrétny účel,

g) pamäťou preukazu je aplikácia „Preukaz študenta, učiteľa alebo iného zamestnanca vysokej školy“, do ktorej vydavateľ preukazu zapisuje údaje o držiteľovi preukazu podľa tohto usmernenia a jeho príloh,

h) internou aplikáciou je aplikácia v preukaze, ktorú vytvára a používa vydavateľ preukazu,

i) externou aplikáciou je aplikácia v preukaze, ktorú vytvára a používa poskytovateľ služieb,

j) International Student Identity Card (v skratke „ISIC“) je označenie grafického vyhotovenia preukazu na základe licencie medzinárodného identifikačného preukazu študenta podporovaného Organizáciou Spojených národov pre výchovu, vedu a kultúru,

k) International Teacher Identity Card (v skratke „ITIC“) je označenie grafického vyhotovenia preukazu na základe licencie medzinárodného identifikačného preukazu učiteľa.

(3) Ak sa vydavateľ preukazu rozhodne vydávať aj ďalšie preukazy pre iné osoby, odporúča sa použiť toto usmernenie aj pre štruktúru údajov a technické vyhotovenie týchto preukazov.

Čl. 2
Použitie preukazu

(1) Údaje viditeľne uvedené na preukaze sa považujú za rovnocenné s príslušnými údajmi zapísanými v pamäti preukazu a v celom rozsahu nahrádzajú písomné potvrdenie o návšteve školy, najmä na účely preukazovania nároku na zľavu vo verejnej osobnej doprave, ak nie je inak uvedené v tarife, prepravnom poriadku alebo inom dokumente vydanom dopravcom.

(2) Pri overovaní údajov na preukaze sa odporúča prednostne používať údaje zapísané v pamäti preukazu; overovanie údajov na preukaze prostredníctvom údajov viditeľne uvedených na preukaze sa odporúča až ak ich nemožno overiť z pamäte preukazu.

(3) Vydavateľ preukazu zodpovedá za správnosť a aktuálnosť údajov o držiteľovi preukazu

a) viditeľne uvedených na preukaze v čase vydania preukazu alebo v čase predĺženia platnosti preukazu,

b) elektronicky zapísaných v pamäti preukazu v čase vydania preukazu, predĺženia platnosti preukazu alebo inej aktualizácie údajov v preukaze.

(4) Údaje v pamäti preukazu [čl. 1 ods. 2 písm. g)] môže

a) zapisovať len vydavateľ príslušného preukazu,

b) čítať len vydavateľ preukazu, poskytovateľ služieb a ministerstvo; verejne prístupné údaje, ktoré nie sú chránené šifrovaním, môže čítať každý, komu držiteľ preukazu poskytne preukaz na tento účel.

(5) Poskytovateľ služieb môže čítať údaje zapísané v pamäti preukazu a použiť ich pre svoje vnútorné potreby v súlade s dohodnutým účelom použitia preukazu pri dodržiavaní zásad ochrany osobných údajov podľa osobitného predpisu,[1)] vrátane vyžiadania súhlasu na spracovanie osobných údajov od držiteľa preukazu.

(6) Interné aplikácie v preukaze vytvára vydavateľ preukazu. Môže na to využiť voľný pamäťový priestor v čipe preukazu spôsobom, ktorý uzná za vhodný.

(7) Externé aplikácie v preukaze vytvárajú poskytovatelia služieb po dohode s vydavateľom preukazu alebo s ministerstvom. Za správnosť údajov v týchto aplikáciách zodpovedá ten, kto ich do preukazu zapísal. Ako zdroj údajov o držiteľovi preukazu sa odporúča použiť údaje v pamäti preukazu zapísané podľa tohto usmernenia.

(8) Ak vydavateľ preukazu poskytne elektronicky poskytovateľovi služieb na základe § 73 ods. 5 zákona údaje o držiteľovi preukazu, k poskytnutým údajom možno pripojiť UID preukazu. Na poskytnutie osobných údajov, ktoré nie sú uvedené v § 73 ods. 5 zákona, je potrebný súhlas držiteľa preukazu podľa osobitného predpisu.[1)]

(9) Vydavateľ preukazu poučí držiteľa preukazu o zaobchádzaní s preukazom. V tomto poučení vydavateľ preukazu uvedie rozsah údajov, ktoré sú vydavateľom preukazu elektronicky zapísané v preukaze a text: „Držiteľ preukazu s preukazom zaobchádza šetrne a nie je oprávnený zasahovať do jeho grafickej úpravy a do údajov elektronicky zapísaných v preukaze. Držiteľ preukazu bezodkladne oznámi vysokej škole potrebu vykonania zmeny údajov viditeľne uvedených na preukaze alebo údajov, ktoré zapísala do preukazu elektronicky vysoká škola. Držiteľ preukazu v takomto prípade, a aj po prerušení štúdia a po skončení štúdia zabezpečí, aby vysoká škola tieto skutočnosti zapísala elektronicky do preukazu. Údaje elektronicky zapísané v preukaze držiteľ preukazu odovzdáva poskytovateľovi služieb priložením preukazu k čítaciemu zariadeniu; za takéto poskytnutie údajov elektronicky zapísaných v preukaze vysoká škola nenesie zodpovednosť. Vzhľadom na bezkontaktnú technológiu preukazu nie je technicky vylúčená možnosť zosnímať údaje elektronicky zapísané v preukaze aj na diaľku - inak ako priamym priložením preukazu k čítaciemu zariadeniu, a preto sa odporúča s preukazom používať tieniacu kartu alebo tieniaci obal na doklady.“.

Čl. 3
Platnosť preukazu študenta

(1) Začiatok platnosti preukazu študenta v príslušnom akademickom roku je 1. septembra. Ak ide o novoprijatého študenta, ktorý sa na štúdium zapísal v priebehu príslušného akademického roka, začiatok platnosti preukazu študenta je deň zápisu na štúdium.

(2) Koniec platnosti preukazu študenta v príslušnom akademickom roku je 30. septembra kalendárneho roku, v ktorom končí príslušný akademický rok. V

[1)] Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

akademickom roku, v ktorom má študent podľa študijného plánu absolvovať štúdium, je koniec platnosti preukazu študenta 30. júna príslušného akademického roku; ak študent do tohto dňa štúdium neukončí, platnosť preukazu študenta sa predlžuje podľa prvej vety.

(3) Preukaz študenta stráca platnosť pred dátumom podľa odseku 2

a) v prípade poškodenia alebo straty,

b) pri skončení alebo prerušení štúdia podľa § 69 ods. 3 zákona.

(4) Ak sa študent zapíše po prerušení štúdia, platnosť preukazu sa obnovuje ku dňu takého zápisu.

Druhá časť
Vyhotovenie a grafická úprava preukazu

Čl. 4
Technické vyhotovenie preukazu

Preukaz sa vyhotovuje vo forme bezkontaktnej čipovej karty, hybridnej čipovej karty alebo. čipovej karty s duálnym rozhraním. Bezkontaktný čip spĺňa normu ISO/IEC 14443A najmenej v častiach 1 až 3.

Čl. 5
Štruktúra údajov viditeľne uvedených na preukaze

(1) Ak ide o preukaz študenta, viditeľne sa na ňom uvádza nápis „Tento preukaz je vydaný podľa zákona č. 131/2002 Z. z. a je dokladom o štúdiu jeho držiteľa na vysokej škole.“. Ak ide o preukaz vydaný v grafickom vyhotovení ISIC, tento nápis sa uvádza na zadnej strane preukazu.

(2) Na prednej strane preukazu sa viditeľne uvádza

a) označenie typu preukazu a jeho držiteľa

1. „Študent“ alebo „Preukaz študenta“ pre študenta v dennej forme štúdia; „Medzinárodný preukaz študenta“, ak ide o preukaz vydaný v grafickom vyhotovení ISIC,
2. „Externý študent“ pre študenta v externej forme štúdia,
3. „Učiteľ“ alebo „Preukaz učiteľa“ pre učiteľa; „Medzinárodný preukaz učiteľa“, ak ide o preukaz vydaný v grafickom vyhotovení ITIC,
4. „Zamestnanec“ alebo „Preukaz zamestnanca“ pre iného zamestnanca vysokej školy,

b) názov a logo vydavateľa preukazu,

c) názov fakulty, ak študijný program, na ktorého štúdium je študent zapísaný, sa uskutočňuje na fakulte, alebo ak učiteľ je v pracovnoprávnom vzťahu organizačne zaradený na fakulte vysokej školy; uvádzanie tohto údaju sa nevyžaduje,

d) meno a priezvisko držiteľa preukazu,

e) akademické tituly, vedecko-pedagogické tituly, umelecko-pedagogické tituly a vedecké hodnosti držiteľa preukazu v takom rozsahu, aby nezasahovali do fotografie držiteľa preukazu; uvádzanie týchto údajov sa nevyžaduje,

f) dátum narodenia držiteľa preukazu v tvare „Dátum narodenia: <dátum>“,

g) začiatok platnosti preukazu v tvare „Platný od: <dátum>“,

h) koniec platnosti preukazu v tvare „Platný do: POZRI RUB“, ak ide o preukaz vydaný v grafickom vyhotovení ISIC, inak v tvare „Platný do: <dátum-MR>“,

i) fotografia držiteľa preukazu zobrazujúca jeho aktuálnu podobu; minimálny rozmer je 2,5 x 3,0 cm, maximálny rozmer je 3,0 cm x 3,5 cm, minimálna výška tváre je 2,0 cm,

j) UID preukazu v dekadickom tvare,

k) číslo licencie ISIC alebo ITIC, ak je preukaz vydaný v grafickom vyhotovení podľa príslušnej licencie.

(3) Na zadnej strane preukazu sa viditeľne uvádza

a) podpisové pole a nápis „PODPIS DRŽITEĽA PREUKAZU:“, ak ide o preukaz vydaný v grafickom vyhotovení ISIC alebo ITIC,

b) koniec platnosti preukazu v tvare „Platný do: <dátum-MR>”, ktorý vyjadruje maximálnu dobu platnosti preukazu v príslušnom akademickom roku, ak ide o preukaz vydaný v grafickom vyhotovení ISIC alebo ITIC.

(4) Údaj o konci platnosti preukazu je viditeľne uvedený na prolongačnej známke, ktorá je zhotovená z holografickej samodeštrukčnej fólie alebo vytlačený vydavateľom preukazu priamo na preukaze. Na prolongačnej známke môže byť aj ďalší text, nesmie však vizuálne potláčať údaj o platnosti preukazu. V prípade rozporu medzi údajom o konci platnosti preukazu viditeľne uvedeným na preukaze a údajom o konci platnosti preukazu elektronicky zapísaným v preukaze, rozhodujúci je elektronicky zapísaný údaj.

(5) Na miestach označených „<dátum>” sa uvádza dátum v tvare DD.MM.RRRR, kde DD je číselné vyjadrenie dňa, MM je číselné vyjadrenie mesiaca a RRRR je číselné vyjadrenie roku (všetko s vedúcimi nulami). Na miestach označených „<dátum-MR>“ sa uvádza úplný dátum, alebo len mesiac a rok v tvare MM/RRRR alebo MM.RRRR.

(6) Okrem údajov uvedených v odsekoch 1 a 2 vydavateľ preukazu môže umiestniť na preukaz aj ďalšie údaje tak, aby sa nenarušila čitateľnosť informácií na preukaze.

Čl. 6
Grafická úprava preukazu

(1) Pre študentov v dennej forme štúdia sa odporúča grafická úprava preukazu podľa vzoru ISIC, pre vysokoškolských učiteľov podľa vzoru ITIC.

(2) Ak nie je preukaz vydaný v grafickom vyhotovení podľa odseku 1, odporúča sa zachovať rovnaké rozloženie údajov a veľkosť fotografie pre všetky preukazy vydávané jedným vydavateľom.

Tretia časť
Údaje v pamäti preukazu

Čl. 7
Štruktúra údajov v pamäti preukazu

(1) Dátový záznam v pamäti preukazu je dlhý 480 bajtov a skladá sa z týchto častí:

a) hlavička záznamu (16 bajtov),

b) dátový blok č. 0, ktorý obsahuje verejné údaje o preukaze (nešifrované),

c) dátový blok č. 1, ktorý obsahuje potvrdenie o štúdiu na vysokej škole (šifrované kľúčom K1),

d) dátový blok č. 2, ktorý obsahuje osobné údaje držiteľa preukazu (šifrované kľúčom K2),

e) elektronický podpis vydavateľa preukazu (48 bajtov).

(2) Časť záznamu, ktorá nie je vyplnená údajmi podľa odseku 1, sa vyplní binárnymi znakmi 0x00.

Čl. 8
Hlavička záznamu

Hlavička záznamu je dlhá 16 bajtov a obsahuje tieto údaje:

a) verzia záznamu (1 bajt), ktorá jednoznačne určuje zoznam a štruktúru položiek v dátových blokoch; záznamy vytvorené podľa tohto usmernenia majú číslo verzie 5,

b) verzia šifrovacieho kľúča K1 (1 bajt), ktorá jednoznačne určuje konkrétny kľúč na šifrovanie a dešifrovanie údajov v dátovom bloku č. 1; kľúč K1 vydaný spolu s týmto usmernením má číslo verzie 1

c) verzia šifrovacieho kľúča K2 (1 bajt), ktorá jednoznačne určuje konkrétny kľúč na šifrovanie a dešifrovanie údajov v dátovom bloku č. 2; kľúč K2 vydaný spolu s týmto usmernením má číslo verzie 1

d) registračné číslo kľúča k elektronickému podpisu (1 bajt), ktoré identifikuje vydavateľa preukazu a ním vydaný verejný kľúč na overenie elektronického podpisu v zázname,

e) dĺžka údajov v dátovom bloku č. 0 v bajtoch (2 bajty, little-endian),

f) dĺžka údajov v dátovom bloku č. 1 v bajtoch (2 bajty, little-endian),

g) dĺžka údajov v dátovom bloku č. 2 v bajtoch (2 bajty, little-endian),

h) rezerva na neskoršie použitie (6 bajtov), ktorá obsahuje binárne znaky 0x00.

Čl. 9
Štruktúra dátových blokov

(1) Dátový blok obsahuje údaje v tvare súvislého reťazca znakov, ktorý sa vnútorne člení na položky. Dátový blok je zostavený z položiek vo formáte CSV s oddeľovacím znakom „|“. Položky sú kódované znakovo a v každej z nich je uložený jeden údaj s pevnou alebo premenlivou dĺžkou bez koncových medzier.

Dátový blok obsahuje všetky predpísané položky v správnom poradí a okrem nich neobsahuje žiadne ďalšie údaje. Prázdne položky sa vkladajú do dátového bloku ako prázdny reťazec[2)]. Dátový blok sa dopĺňa binárnymi znakmi 0x00 tak, aby jeho dĺžka bola násobkom 16 bajtov.

(2) Štruktúra dátových blokov je uvedená v Prílohe č. 1, ktorá obsahuje záväzný zoznam položiek, ich význam a spôsob vypĺňania, prípadne kódovania.

(3) Kódovanie údajov v položkách závisí od typu ich hodnoty, pričom:

a) „číslo“ je znakovo vyjadrené celé číslo alebo číselný kód,

b) „dátum“ je 8 znakov v tvare RRRRMMDD, kde R je rok, M je mesiac s hodnotami 01 až 12 a D je deň v mesiaci s hodnotami 01 až 31,

c) „znaky“ sú krátky reťazec alfanumerických znakov bez slovenskej diakritiky, kódovaný podľa normy ASCII,

d) „text“ je textový reťazec so slovenskou diakritikou, kódovaný podľa normy UTF-8.

(4) Ak celková dĺžka všetkých dátových blokov v dôsledku dlhých textov alebo veľkého počtu znakov so slovenskou diakritikou v položkách typu „text“ presiahne kapacitu dátového záznamu podľa čl. 7, textové položky v dátových blokoch sa primerane skrátia.

(5) Dátové bloky č. 1 a 2 sa šifrujú takto:

a) pri zarovnaní dĺžky bloku podľa odseku 1 sa v bloku rezervujú 4 bajty na kontrolný súčet bloku podľa štandardu Mifare CRC-32, ktorý používa modul Mifare SAM AV2 v režime AV1,

b) kontrolný súčet bloku sa vloží do posledných 4 bajtov bloku v tvare „little-endian“; vypočíta sa zo všetkých predchádzajúcich bajtov v bloku,

c) celý dátový blok sa šifruje algoritmom AES-128 v režime CBC, Padding=None a s nulovým inicializačným vektorom,

d) na šifrovanie údajov sa použije príslušný kľúč K1 alebo K2 podľa čl. 12.

Čl. 10
Elektronický podpis vydavateľa preukazu

(1) Ako podklad pre elektronický podpis vydavateľa preukazu sa použije kontrolný súčet dátového záznamu, ktorý sa vytvorí hašovacou funkciou SHA-1. Kontrolný súčet je dlhy je 20 bajtov (160 bitov) a nevkladá sa do dátového záznamu. Na jeho výpočet sa použijú tieto údaje:

a) všetky časti dátového záznamu podľa čl. 7, ktoré sa nachádzajú pred elektronickým podpisom vydavateľa preukazu,

b) UID preukazu v tvare „little-endian“ (7 bajtov alebo 4 bajty podľa typu čipu).

(2) Údaje obsiahnuté v dátovom zázname sa elektronicky podpisujú takto:

[2)] 0 znakov s príslušným oddeľovačom

a) kontrolný súčet sa podpisuje algoritmom na asymetrický podpis ECDSA, krivka NIST P-192, známa aj pod označením X9.62 prime192v1 alebo secp192r1,

b) na elektronický podpis vydavateľ preukazu použije dvojicu kľúčov (certifikát) podľa hlavičky dátového záznamu,

c) elektronický podpis je dlhý 48 bajtov; tvorí ho dvojica položiek R a S podľa kryptografického štandardu ECDSA, každá z nich je uložená v tvare „big-endian“.

(3) Elektronický podpis vydavateľa preukazu slúži na potvrdenie správnosti údajov prečítaných z preukazu. Vydavateľ preukazu nezodpovedá za prípadné škody, ktoré vzniknú poskytovateľovi služieb alebo inej osobe, ak si títo neoveria platnosť elektronického podpisu údajov.

Štvrtá časť
Technické vyhotovenie preukazu

Čl. 11
Technické vyhotovenie preukazu s čipom Mifare DESFire

(1) Na vyhotovenie preukazov podľa tohto usmernenia sa používajú karty s bezkontaktným čipom, ktorý je kompatibilný so štandardom Mifare DESFire EV1 8 kB / 4 kB / 2 kB, MF3 IC D81 / D41 / D21.

(2) Aplikácia na prácu s preukazmi je zapísaná v medzinárodnom registri aplikácií Mifare a jej vlastníkom je ministerstvo. Na identifikáciu aplikácie podľa štandardu Mifare Application Directory (MAD3) sa použije identifikátor AID s hodnotou „0xF585F0“.

(3) V čipe sa pre aplikáciu podľa odseku 2 vyhradí jeden súbor údajov s kapacitou 480 bajtov, do ktorého sa zapíše dátový záznam zostavený podľa čl. 7. Prístup k súboru na čítanie sa nastaví ako verejný s kľúčom č. 14 (0x0E).

(4) Kľúče vydavateľa preukazu na zápis údajov do pamäte preukazu sa diverzifikujú podľa UID preukazu.

(5) V preukaze sa odporúča rezervovať priestor pre tieto aplikácie:

a) externé aplikácie vo verejnej osobnej doprave,

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

c) vlastné záznamy držiteľa preukazu podľa štandardov NFC a NDEF.

(6) Pamäťový priestor a transportné kľúče pre všetky plánované aplikácie vydavateľ preukazu nastaví pri prvotnej inicializácii čipu v preukaze podľa dohody s príslušnými poskytovateľmi služieb.

Čl. 12
Čítanie údajov z pamäte preukazu

(1) Na šifrovanie a dešifrovanie dátových blokov č. 1 a 2 v pamäti preukazu sa použijú kľúče K1 a K2, ktoré určuje ministerstvo jednotne pre všetkých vydavateľov preukazov. Kľúče sú dlhé 16 bajtov.

(2) Kľúče K1 a K2 ministerstvo vydá vydavateľom preukazov a poskytovateľom služieb na základe ich žiadosti. Poskytovateľom služieb ministerstvo vydá kľúče zapísané v pamäti bezpečnostných modulov „SAM“, odkiaľ ich nemožno spätne prečítať; iný spôsob vydania kľúčov sa použije len v odôvodnených prípadoch. O vydaných kľúčoch ministerstvo vedie evidenciu.

(3) Kľúč K2 ministerstvo vydá len tým poskytovateľom služieb, ktorí v žiadosti preukážu, že pre svoju činnosť potrebujú aj osobné údaje držiteľa preukazu uvedené v dátovom bloku č. 2.

(4) Fyzické osoby a právnické osoby, ktoré majú prístup ku kľúčom K1 a K2 zabezpečia ich ochranu pred zneužitím, stratou alebo prezradením.

(5) Na bezpečné uloženie kľúčov K1 a K2 podľa odseku 2 a na dešifrovanie údajov v pamäti preukazu pomocou týchto kľúčov sa použijú moduly „SAM“ kompatibilné so štandardom Mifare SAM AV2 (v režime AV2 alebo AV1).

(6) Na overenie platnosti elektronického podpisu údajov v pamäti preukazu sa používa verejný kľúč vydavateľa preukazu podľa štandardu PKI. Platné kľúče jednotlivých vydavateľov centrálne registruje a zverejňuje ministerstvo.

(7) Príklady použitia algoritmov na šifrovanie a elektronický podpis údajov v preukaze sú uvedené v Prílohe č. 2.

Piata časť
Kontaktný čip a elektronický podpis držiteľa preukazu

Čl. 13
Technické vyhotovenie preukazu s kontaktným čipom

(1) Preukaz možno použiť aj ako bezpečné úložisko PKI kľúčov pre elektronický podpis držiteľa preukazu, a to použitím kontaktného čipu podľa štandardu ISO 7816-1, 7816-2, 7816-3 a 7816-4 a aplikácií tohto čipu.

(2) Tento čip musí mať pamäť (EEPROM) aspoň 72 kB a jeho operačný systém musí podporovať GlobalPlatform 2.1.1 a SCP 01 a 02 alebo ich novšie verzie.

Čl. 14
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 kľúčových párov vo vnútri čipu,

b) kryptografické operácie so súkromným kľúčom v pamäti čipu,

c) možnosť importovať kľúčový pár do pamäte čipu,

d) možnosť zákazu čítania a exportovania súkromných kľúčov z pamäte čipu,

e) použitie súkromných kľúčov len po úspešnej autentizácii oprávneného držiteľa preukazu prostredníctvom príslušného PIN kódu,

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

g) uloženie certifikátov X.509 k používateľským kľúčom, prípadne aj certifikátov certifikačných autorít,

h) uloženie atribútov objektov, a to 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,
   3. názov aplikácie, popis a identifikátor pre všeobecné dátové objekty,

i) vykonanie operácie bezpečnej reinicializácie oblasti preukazu, najmä oblasti dát PKI aplikácie, pri zachovaní čísla preukazu v pamäti čipu, a to
   1. bezpečným odstránením všetkých používateľských dát v čipe, najmä kľúčov, certifikátov a dátových objektov formou atomickej operácie,
   2. nastavením PIN alebo PUK oblasti na neinicializované hodnoty alebo na hodnoty vopred známe.

(2) Čip obsahuje inicializovanú oblasť pre elektronický podpis a 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,

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

Čl. 15
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 na prečítanie UID bezkontaktného čipu v preukaze.

(4) Ovládače musia byť dostupné aspoň pre 32-bitové aj 64-bitové operačné systémy MS Windows XP a vyššie a Linux (aspoň 3 bežne používané distribúcie).

Čl. 16
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) Požadovanými vlastnosťami PKI aplikácie pre prácu s oblasťou pre nekvalifikované certifikáty sú:

a) UID uložené v kontaktnom čipe preukazu je zhodné s UID bezkontaktného čipu preukazu,

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

c) priestor pre uloženie užívateľských certifikátov X.509, celkom aspoň 12 kB,

d) priestor pre uloženie 2 koreňových certifikátov, celkom aspoň 4 kB,

e) podpora Smart Card Logon do OS Windows,

f) podpora diakritiky v certifikátoch,

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

Šiesta časť
Prechodné, zrušovacie a záverečné ustanovenia

Čl. 17

(1) Grafické vyhotovenie preukazov vydaných pred dňom účinnosti tohto usmernenia nie je potrebné meniť.

(2) Ak v pamäti preukazu s čipom podľa čl. 11 existujú kratšie súbory vytvorené podľa doterajších predpisov

a) AID aplikácie sa nemení (0xF58510),

b) do aplikácie sa doplní ďalší súbor, ktorý kapacitu doterajších súborov doplní na potrebnú dĺžku; napríklad ak dva doterajšie súbory sú dlhé 192 bajtov, nový súbor bude dlhý 96 bajtov,

c) dátový záznam sa zapíše po častiach do všetkých súborov aplikácie,

d) prístup ku všetkým súborom aplikácie sa nastaví podľa čl. 11 ods. 3.

Čl. 18

(1) Preukazy s čipom Mifare Classic 4kB, MF1 IC S70 (ďalej len „čip Classic“), vydávané podľa doterajších predpisov, možno vydávať najdlhšie do 30. septembra 2015 a takto vydané preukazy možno používať najdlhšie počas doby šesť rokov, ktorá vychádza z životnosti kariet garantovanej výrobcom. Toto usmernenie sa na ne vzťahuje primerane, ak tento článok neustanovuje inak.

(2) Na identifikáciu aplikácie v preukaze s čipom Classic podľa štandardu Mifare Application Directory (MAD2) sa použije identifikátor AID s hodnotou „0x585F“.

(3) V pamäti preukazu s čipom Classic sú pre aplikáciu vyhradené sektory č. 0x20 a 0x21, do ktorých sa dátový záznam zapíše v dvoch častiach po 240 bajtov.

(4) Kľúč na čítanie sektorov v preukaze s čipom Classic sa nastaví ako verejný s hodnotou 0xA0A1A2A3A4A5. Prístupové práva k sektorom sa nastavia na hodnotu 0x78778800.

(5) V pamäti čipu Classic sa pri prvotnej inicializácii tohto čipu odporúča rezervovať priestor pre tieto aplikácie:

a) sektor 0x22 na uloženie prípadných ďalších centrálne určených údajov,

b) sektory 0x01 až 0x0F pre externé aplikácie vo verejnej osobnej doprave,

c) sektory 0x11 až 0x1F a 0x23 až 0x27 na ďalšie účely, vrátane aplikácie „Knižničný (kultúrny) preukaz“, ktorá umožňuje použitie preukazov v akademických a vedeckých knižniciach, prípadne ďalších kultúrnych a vzdelávacích organizáciách.

Čl. 19
Zrušovacie ustanovenia

Zrušuje sa usmernenie č. 13/2010-R zo 7. júla 2010.

Čl. 20
Účinnosť

Toto metodické usmernenie nadobúda účinnosť 1.septembra 2014.

minister

Zoznam príloh

Obsah