

TECHNICKÁ ŠPECIFIKÁCIA OSVEDČENIA O EVIDENCII ČASTI I

1. Formát čipovej karty

(1) Čipová karta sa vyhotoví v súlade s technickými normami uvedenými v časti 5.

(2) Fyzická bezpečnosť dokumentov je ohrozená

- a) zhotovením falošných kariet – vytvorením nového objektu, ktorý vykazuje veľkú podobnosť s dokumentom buď tak, že je zhotovený ako nový, alebo je kópiou pôvodného dokumentu,
- b) podstatnou zmenou: zmenou vlastností pôvodného dokumentu, napríklad zmenou niektorých údajov vytlačených na dokumente.

2. Uloženie údajov a ochrana

(1) Na čipovej karte sa ukladajú:

- a) povinne údaje podľa prílohy č. 5 časti A ods. 1 a 2,
- b) nepovinne údaje podľa prílohy č. 5 časti A ods. 3,
- c) nepovinne doplňujúce údaje podľa prílohy č. 5 časti A ods. 4,
- d) overovacie údaje zhodnoverenia evidenčných dát.

(2) Údaje uvedené v prvom bode písm. a) a b) sa ukladajú v dvoch súboroch s transparentnou štruktúrou.¹⁾ Údaje uvedené v prvom bode písm. c) sa ukladajú v ľubovoľnom formáte. Pre tieto súbory nie sú žiadne obmedzenia z hľadiska ich čítania. Zápisový prístup k týmto súborom je obmedzený vydávajúcim orgánom, ktorý čipovú kartu vystavuje. Zápisový prístup je povolený len po asymetrickej hodnovernosti s výmenou relačného kľúča na ochranu relácie medzi evidenčnou kartou vozidla a bezpečnostným modulom. Preto sa pred procesom zhodnoverenia vymenia osvedčenia overujúce kartu.²⁾ Osvedčenia overujúce kartu obsahujú zodpovedajúce verejné kľúče, ktoré sa musia vyvolať a použiť v procese zhodnoverenia. Tieto osvedčenia podpisujú národné orgány a obsahujú predmet zhodnoverenia³⁾ držiteľa osvedčenia, aby sa mohol na kartu uložiť zakódovaný druh prístupového oprávnenia. Toto druhovo špecifické prístupové oprávnenie sa vzťahuje k národnému orgánu. Zodpovedajúce verejné kľúče národného orgánu sú na karte uložené ako základný verejný kľúč. Za špecifikáciu súborov a príkazov potrebných na proces zhodnoverenia a proces zapisovania sú zodpovedné členské štáty. Stupeň zabezpečenia sa schváli na základe spoločných kritérií hodnotenia podľa EAL4+. Rozšírenia sú tieto:

- 1. AVA_MSU.3 Analýzy a testy pre nestále stavy,
- 2. AVA_VLA.4 Vysoká odolnosť.

(3) Vydávajúci orgán vypočíta svoj elektronický podpis pre všetky dáta súboru obsahujúceho údaje uvedené v prvom bode písm. a) alebo písm. b) a uloží ich v

¹⁾ ISO/IEC 7816-4 Identifikačné karty. Karty s integrovanými obvodmi. Časť 4: Štruktúra, bezpečnosť a príkazy pre výmenu.

²⁾ ISO/IEC 7816-8 Identifikačné karty. Karty s integrovanými obvodmi. Časť 8: Príkazy pre bezpečnostné operácie.

³⁾ ISO/IEC 7816-9 Identifikačné karty. Karty s integrovanými obvodmi. Časť 9: Príkazy pre správu kariet.

zodpovedajúcim súbore. Tieto podpisy umožňujú overiť hodnovernosť uložených údajov. Na karty sa uložia tieto údaje:

- a) elektronický podpis evidenčných dát podľa prvého bodu písm. a),
- b) elektronický podpis evidenčných dát podľa prvého bodu písm. b).

(4) Na overenie týchto elektronických dát na karte sa uložia osvedčenia vystavujúceho orgánu, ktorý vypočítal podpisy k dátam uvedeným v bode 1 písm. a) a b). Elektronické podpisy a osvedčenia musia byť čitateľné bez obmedzenia. Prístup k zapisovaniu do elektronických podpisov a osvedčení je obmedzený na príslušné národné orgány.

3. Rozhrania

Pre rozhrania sa používajú vonkajšie kontakty. Kombinácia vonkajších kontaktov s transpondérmi je nepovinná.

4. Kapacita pamäte karty

Karta musí mať dostatočnú kapacitu na uloženie údajov uvedených v časti 2.

5. Normy

Čipové karty a použité čítacie zariadenia zodpovedajú príslušným požiadavkám na identifikačné karty.⁴⁾

6. Technické charakteristiky protokolov procesu

(1) Formátom⁵⁾ je ID-1. Karta podporuje protokol procesu $T = 1$.⁶⁾ Dodatočne môžu byť podporované iné protokoly procesu, napr. $T = 0$, USB alebo bezkontaktné protokoly.

(2) Na prenos bitu sa uplatňuje „direct convention“.⁶⁾

- a) Napájacie napätie, programovacie napätie; karta pracuje s $V_{cc} = 3V (+0,3 V)$ alebo s $V_{cc} = 5 V (+0,5 V)$. Karta nevyžaduje programovacie napätie pri kontakte C6.

⁴⁾ Napríklad STN ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti (36 9725).

STN ISO/IEC 7816-1 Identifikačné karty. Karty s integrovanými obvodmi a s kontaktmi. Časť 1: Fyzikálne vlastnosti (36 9734).

ISO/IEC 7816-2 Identifikačné karty. Karty s integrovanými obvodmi. Časť 2: Karty s kontaktmi. Rozmery a umiestnenie kontaktov.

ISO/IEC 7816-3 Identifikačné karty. Karty s integrovanými obvodmi. Časť 3: Karty s kontaktmi. Elektrické rozhranie a protokoly prenosu.

ISO/IEC 7816-4 Identifikačné karty. Karty s integrovanými obvodmi. Časť 4: Štruktúra, bezpečnosť a príkazy pre výmenu.

ISO/IEC 7816-5 Identifikačné karty. Karty s integrovanými obvodmi a kontaktmi. Časť 5: Systém číslovania a registračný postup identifikátorov aplikácií.

ISO/IEC 7816-6 Identifikačné karty. Karty s integrovanými obvodmi. Časť 6: Medziodborové dátové prvky pre rozhranie.

ISO/IEC 7816-8 Identifikačné karty. Karty s integrovanými obvodmi. Časť 8: Príkazy pre bezpečnostné operácie.

ISO/IEC 7816-9 Identifikačné karty. Karty s integrovanými obvodmi. Časť 9: Príkazy pre správu kariet.

⁵⁾ Napríklad STN ISO/IEC 7810 Identifikačné karty. Fyzikálne vlastnosti (36 9725).

⁶⁾ ISO/IEC 7816-3 Identifikačné karty. Karty s integrovanými obvodmi. Časť 3: Karty s kontaktmi. Elektrické rozhranie a protokoly prenosu.

- b) Odpoveď na resetovanie; bit pre veľkosť informačného poľa karty v ATR sa prezentuje v znaku TA3. Táto hodnota je najmenej „80h“ (= 128 bitov).
- c) Voľba parametra protokolu; podpora voľby parametra protokolu (PPS)⁶⁾ je povinná. Používa sa pre voľbu $T = 1$, ak je dodatočne na karte k dispozícii $T = 0$, a na dohodnutie parametrov Fi/Di na dosiahnutie vyšších prenosových rýchlostí.
- d) Protokol procesu $T = 1$ Podpora zretazenia je povinná. Povolené sú tieto zjednodušenia:
 1. NAD Byte: nepoužitý,
 2. S-Block ABORT: nepoužitý,
 3. S-Block VPP chyba stavu: nepoužitý.

(3) Veľkosť informačného poľa zariadenia (IFSD) IFD ukáže ihneď po ATR; t. j. IFD prenesie S-blok IFS požiadavku po ATR a karta vyšle späť S-blok IFS. Odporúčaná hodnota pre IFSD je 254 bitov.

7. Rozsah teplôt

Osvedčenie o evidencii vo formáte čipovej karty správne funguje za všetkých klimatických podmienok a v stanovenom teplotnom rozsahu.⁵⁾ Karty musia správne fungovať v rozsahu vlhkosti od 10 % do 90 %.

8. Fyzická životnosť

Ak sa karta používa v súlade s environmentálnymi a elektrickými špecifikáciami, musí riadne fungovať počas obdobia desiatich rokov. Materiál karty sa musí zvoliť tak, aby bola táto životnosť zabezpečená.

9. Elektrické charakteristiky

Počas prevádzky musia karty zodpovedať z hľadiska elektromagnetickej kompatibility predpisu Európskej hospodárskej komisie Organizácie Spojených národov č. 10⁷⁾ a musia byť chránené pred elektrostatickým výbojom.

10. Štruktúra súboru

V tabuľke č. 1 sú povinné základné súbory (EF) aplikácie DF¹⁾ DF. Registration. Všetky tieto súbory majú transparentnú štruktúru. Prístupové požiadavky sú popísané v časti 2.

Tabuľka č. 1

Názov súboru	Identifikátor súboru	Opis
EF.Registration_A	„D001“	Evidenčné údaje podľa prílohy č. 5
EF.Signature_A	„E001“	Elektronický podpis pre úplný dátový obsah EF.Registration_A

⁷⁾ Dohoda o prijatí jednotných podmienok pre homologáciu (overovanie zhodnosti) a o vzájomnom uznávaní homologácie výstroja a súčastí motorových vozidiel v znení neskorších predpisov (vyhláška ministra zahraničných vecí č. 176/1960 Zb.).

EF.C.IA_A.DS	„C001“	X.509v3 osvedčenie vystavujúceho orgánu, ktorý vypočítal podpisy pre EF. Signature_A
EF.Registration_B	„D001“	Evidenčné údaje podľa prílohy č. 5
EF.Signature B	„E001“	Elektronický podpis pre úplný dátový obsah EF.Registration_B
EF.C.IA_B.DS	„C001“	X.509v3 osvedčenie vystavujúceho orgánu, ktorý vypočítal podpisy pre EF. Signature_B

11. Štruktúra dát

(1) Uložené osvedčenia sú vo formáte X.509v3.⁸⁾ Elektronické podpisy sú uložené transparentne.

(2) Evidenčné údaje sú uložené ako BER-TLV dátové objekty¹⁾ v zodpovedajúcich základných súboroch. Hodnotové polia sú kódované ako ASCII-znak,⁹⁾ hodnoty „C0“-„FF“ sú definované normami.¹⁰⁾ Formát dát je RRRRMDD.

(3) V tabuľke č. 2 sú identifikačné znaky dátových objektov zodpovedajúce evidenčným dátam podľa prílohy č. 5 časti A odsekov 1 a 2 spolu s doplňujúcimi údajmi tejto prílohy časti 1. Ak nie je ustanovené inak, dátové objekty uvedené v tabuľke č. 2 sú povinné. Nepovinné dátové objekty sa môžu vynechať. Stĺpec „Znaky“ udáva úroveň vkladania do seba. V tabuľke č. 3 sú Identifikačné znaky dátových objektov zodpovedajúce evidenčným dátam podľa prílohy č. 5 časti A odseku 3. Dátové objekty uvedené v tabuľke č. 3 sú nepovinné.

Tabuľka č. 2

Znak				Opis
„78“				Orgán pridelujúci kompatibilný znak, vložený objekt „4F“ ¹¹⁾
	„4F“			Identifikátor aplikácie ¹⁾
„71“				Medziodborová šablóna ¹¹⁾ zodpovedajúca povinným údajom osvedčenia o evidencii časti 1

⁸⁾ ISO/IEC 9594-8 Informačné technológie. Prepojenie otvorených systémov. Verejný kľúč a atribúty certifikačného rámca.

⁹⁾ ISO/IEC 8824-1 Informačné technológie. Jazyk ASN.1 (Zápis abstraktnej syntaxe č. 1). Vymedzenie základnej notácie.

¹⁰⁾ ISO/IEC 8859-1 Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou. Časť 1: Latinská abeceda č. 1.

ISO/IEC 8859-5 Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou. Časť 5: Latinská abeceda/Cyrilika.

ISO/IEC 8859-7 Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou. Časť 7: Latinská abeceda/grécka abeceda.

¹¹⁾ ISO/IEC 7816-4 Identifikačné karty. Karty s integrovanými obvody. Časť 4: Štruktúra, bezpečnosť a príkazy pre výmenu.

ISO/IEC 7816-6 Identifikačné karty. Karty s integrovanými obvody. Časť 6: Medziodborové dátové prvky pre rozhranie.

	„80“			Verzia definície znaku
	„9F33“			Názov členského štátu vystavujúceho osvedčenie o evidencii časť 1
	„9F34“			Iné (napríklad predchádzajúce národné) označenie ekvivalentného dokumentu (nepovinné)
	„9F35“			Názov príslušného orgánu
	„9F36“			Názov orgánu vystavujúceho osvedčenie o evidencii (nepovinné)
	„9F37“			Použitá množina znakov: „00“ ¹²⁾ „01“ ¹³⁾ „02“ ¹⁴⁾
	„9F38“			Jednoznačné poradové číslo dokumentu používané v členskom štáte
	„81“			Evidenčné číslo
	„82“			Dátum prvej evidencie
	„A1“			Osobné údaje, vložené objekty „A2“ a „86“
		„A2“		Držiteľ osvedčenia o evidencii, vložené objekty „83“, „84“ a „85“
			„83“	Priezvisko alebo obchodné meno
			„84“	Iné mená alebo iniciály (nepovinné)
			„85“	Adresa v členskom štáte
		„86“		„00“: je majiteľ vozidla „01“: nie je majiteľ vozidla „02“: nie je označený ako majiteľ vozidla
	„A3“			Vozidlo, vložené objekty „87“, „88“ a „89“
		„87“		Značka vozidla
		„88“		Typ vozidla
		„89“		Obchodné označenie vozidla
	„8A“			Identifikačné číslo vozidla
	„A4“			Hmotnosť, vložené „8B“
		„8B“		Najväčšia technicky prípustná hmotnosť naloženého vozidla

¹²⁾ ISO/IEC 8859-1 Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou. Časť 1: Latinská abeceda č. 1.

¹³⁾ ISO/IEC 8859-5 Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou. Časť 5: Latinská abeceda/Cyrilika.

¹⁴⁾ ISO/IEC 8859-7 Informačné technológie. Množiny grafických znakov kódované jednou 8-bitovou slabikou. Časť 7: Latinská abeceda/grécka abeceda.

	„8C“			Hmotnosť vozidla v prevádzke s karosériou
	„8D“			Obdobie platnosti
	„8E“			Dátum evidencie, na ktorú sa osvedčenie vzťahuje
	„8F“			Typové schvaľovacie číslo
	„A5“			Motor, vložené objekty „90“, „91“ a „92“
		„90“		Zdvihový objem motora
		„91“		Najväčší čistý výkon motora
		„92“		Motor: druh paliva
	„93“			Pomer výkon/hmotnosť
	„A6“			Miesta na sedenie, vložené objekty „94“ a „95“
		„94“		Počet miest na sedenie
		„95“		Počet miest na státie

Tabuľka č. 3

Znak				Opis
„78“				Orgán pridelujúci kompatibilný znak, vložený objekt „4F“ ¹¹⁾
	„4F“			Identifikátor aplikácie ¹⁾
„72“				Medziodborová šablóna ¹¹⁾ zodpovedajúca nepovinným údajom osvedčenia o evidencii časti 1, vložené všetky nasledujúce objekty
	„80“			Verzia definície znaku
	„A1“			Osobné údaje, vložené objekty „A7“, „A8“ a „A9“
		„A7“		Vlastník vozidla, vložené objekty „83“, „84“ a „85“
			...	
		„A8“		Druhý vlastník vozidla, vložené objekty „83“, „84“ a „85“
			...	
		„A9“		Osoba, ktorá môže používať vozidlo na základe iného práva, ako je vlastnícke právo, vložené objekty „83“, „84“ a „85“
			...	
	„A4“			Hmotnosť, vložené objekty „96“ a „97“
		„96“		Najväčšia technicky prípustná hmotnosť naloženého vozidla v prevádzke
		„97“		Najväčšia technicky prípustná hmotnosť celého vozidla

			v prevádzke
	„98“		Kategória vozidla
	„99“		Počet náprav
	„9A“		Rázvor
	„AD“		Rozloženie najväčšej technicky prípustnej naloženej hmotnosti na nápravy, vložené objekty „9F1F“, „9F20“, „9F21“, „9F22“ a „9F23“
		„9F1F“	Náprava 1
		„9F20“	Náprava 2
		„9F21“	Náprava 3
		„9F22“	Náprava 4
		„9F23“	Náprava 5
	„AE“		Najväčšia technicky prípustná prípojná hmotnosť prípojného vozidla, vložené objekty „9B“ a „9C“
		„9B“	Brzdená
		„9C“	Nebrzdená
	„A5“		Motor, vložené objekty „9D“ a „9E“
		„9D“	Menovité otáčky
		„9E“	Identifikačné číslo motora
	„9F24“		Farba vozidla
	„9F25“		Najväčšia rýchlosť
	„AF“		Hladina hluku, vložené objekty „DF26“, „DF27“ a „DF28“
		„9F26“	Stojace vozidlo
		„9F27“	Otáčky motora
		„9F28“	Za jazdy
	„B0“		Výfukové emisie, vložené objekty „9F29“, „9F2A“, „9F2B“, „9F2C“, „9F2D“, „9F2E“, „9F2F“, „9F30“ a „9F31“
		„9F29“	CO
		„9F2A“	HC
		„9F2B“	NO _x
		„9F2C“	HC + NO _x
		„9F2D“	Častice zo vznetových motorov

		„9F2E“		Korigovaný súčiniteľ absorpcie pre vznetové motory
		„9F2F“		CO ₂
		„9F30“		Kombinovaná spotreba paliva
		„9F31“		Údaj o environmentálnej kategórii typového schválenia EÚ
	„9F32“			Objem palivových nádrží

12. Čítanie evidenčných dát

Čítanie evidenčných dát

- voľba aplikácie: aplikácia „Registrácia vozidla“ sa môže zvoliť pomocou SELECT DF¹⁾ so svojím identifikátorom aplikácie (AID). Hodnota AID sa vyžiada z laboratória vybraného Európskou komisiou,
- čítanie dát zo súborov: súbory zodpovedajúce časti 2 odseku 1 písm. a) až d) sa zvolia pomocou SELECT¹⁾ s príkazovými parametrami P1 nastavenými na „02“, P2 nastavenými na „04“ a príkazovým dátovým poľom obsahujúcim identifikátor súboru. Späť odoslaná šablóna FCP obsahuje veľkosť súboru, ktorá môže byť užitočná na čítanie týchto súborov. Tieto súbory sú čitateľné s READ BINARY,¹⁾ pričom chýba príkazové dátové pole a Le je nastavená na dĺžku očakávaných dát, s použitím krátkej Le,
- overovanie hodnovernosti dát: na overenie hodnovernosti uložených evidenčných dát sa môže využiť zodpovedajúci elektronický podpis. Okrem evidenčných dát sa môže z karty čítať aj zodpovedajúci elektronický podpis. Osvedčenia obsahujú verejný kľúč a totožnosť príslušného orgánu. Overenie podpisu sa môže vykonať iným systémom, ako je evidenčná karta.