

Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky

Príloha č. 1 k metodickému usmerneniu č. 13

Typ položky	Popis údajov	Formát	Garantovaná veľkosť v bajtoch
1	druh preukazu 1 = študent dennej formy štúdia, 2 = študent externej formy štúdia 3 = učiteľ 4 = iný zamestnanec ako učiteľ 5 = iný používateľ	číslo	1
2	začiatok platnosti preukazu podľa Čl. 5	dátum	4
3	koniec platnosti aplikácií preukazu vzťahujúcich sa na štátom garantované zľavy podľa Čl. 5	dátum	4
4	jednoznačný identifikátor držiteľa preukazu určený vydavateľom preukazu (osobné číslo)	ID	11
5	akademické tituly, vedecko-pedagogické tituly a umelecko-pedagogické tituly pred menom	text	16
6	meno (mená)	text	25
7	Priezvisko	text	25
8	akademické tituly a vedecké hodnosti za menom	text	11
9	dátum narodenia	dátum	4
10	názov a sídlo vydavateľa preukazu, prípadne aj názov fakulty (kód podľa katalógu VŠFAKU JÚZ)	text	9
11	názov ulice a číslo domu, kde má držiteľ preukazu trvalý pobyt	text	25
12	názov obce, v ktorej má držiteľ preukazu trvalý pobyt	text	20
13	poštové smerové číslo obce, v ktorej má držiteľ preukazu trvalý pobyt	číslo	5
14	stupeň štúdia: 1 = vysokoškolský študijný program 1. stupňa 2 = vysokoškolský študijný program 2. stupňa 3 = vysokoškolský študijný program 3. stupňa	číslo	1
15	Pohlavie	text	1

Typ položky	Popis údajů	Formát	veľkosť v bytoch
1	verzia záznamu personalizačných údajov	číslo	1
2	verzia elektronického podpisu personalizačných dát	číslo	1
3	verzia kľúčov	číslo	1
4	druh karty	číslo	1
5	stupeň štúdia	číslo	1
6	Pohlavie	text	1
7	tituly pred menom	text	19
8	meno a priezvisko	text, RLC kódovanie	56
9	tituly za menom	text	12
10	dátum narodenia	dátum	4
11	začiatok platnosti preukazu podľa Čl. 5	dátum	4
12	koniec platnosti aplikácií preukazu vzťahujúcich sa na štátom garantované zľavy podľa Čl. 5	dátum	4
13	názov a sídlo vydavateľa preukazu, prípadne aj názov fakulty (kód podľa katalógu VSFAKU JÚZ)	text	9
14	Zarovnanie		14
15	elektronický podpis		64

Typ položky	Popis údajja	Formát	veľkosť v bytoch
1	verzia záznamu personalizačných údajov	číslo	1
2	verzia elektronického podpisu personalizačných údajov	číslo	1
3	verzia kľúčov	číslo	1
4	jednoznačný identifikátor držiteľa preukazu určený vydavateľom preukazu (osobné číslo)	ID	12
5	názov ulice a číslo domu, kde má držiteľ preukazu trvalý pobyt	text	50
6	názov obce, v ktorej má držiteľ preukazu trvalý pobyt	text	50
7	poštové smerové číslo obce, v ktorej má držiteľ preukazu trvalý pobyt	číslo	5
8	zarovnanie		8
9	elektronický podpis		64

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)
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	Electrical 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 IDentifier (výrobné číslo karty pre čipové karty)
UTF8	8-bit Unicode Transformation Format (bezstratové kódovanie s variabilnou dĺžkou určené pre Unicode znaky)