

Príloha č. 3 Použité technologické a informatické skratky

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)
CSV	Comma-separated values (jednoduchý formát na zápis alebo prenos tabuľkových údajov vo forme čistého textu, kde hodnoty jednotlivých položiek v riadku sú navzájom oddelené dohodnutým oddeľovacím znakom)
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	Electrically Erasable Programmable Read Only Memory (elektronická súčiastka, pamäť)
ESC	European Student Card (európsky preukaz študenta)
ESCN	European Student Card Number (jedinečný identifikátor karty, ktorý slúži na identifikáciu a overovanie európskych študentských preukazov) https://erasmus-plus.ec.europa.eu/european-student-card-initiative/card/how-it-works
ESI	European Student Identifier (digitálny identifikátor študenta, jedinečný naprieč inštitúciami a krajinami) https://erasmus-plus.ec.europa.eu/european-student-card-initiative/card/european-student-identifier
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	International 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#1 1	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	Signature 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)