

Elektronický podpis a IVK

Glosár

Pojmy, ktorých význam
ste vždy chceli vedieť

NAJAUTHORITATÍVNEJŠÍ ZDROJ

e podpis

POZNÁMKA

Glosár elektronického podpisu a IVK – pojmy, ktorých význam ste vždy chceli vedieť

© Ivar Elznic • 2002

Pri príprave tohto Glosára sa úzkostlivo dbalo na správnosť informácií. Autor, webové sídlo e-podpis.sk a osoby s ním spojené však nie sú zodpovední za chyby v tomto Glosári.

Šíriť alebo rozmnožovať tento Glosár je dovolené pod podmienkou, že bude šírený alebo rozmnožovaný vcelku – vrátane tejto poznámky.

A

abstrakčná funkcia hash function

Algoritmus, ktorý zo vstupného reťazca znakov vyprodukuje iný reťazec znakov tak, že

- použitie algoritmu na ten istý vstupný reťazec vždy dá tú istú výslednú hodnotu,
- je matematicky neuskutočniteľné získať alebo zrekonštruovať pôvodný reťazec znakov na základe vedomosti výslednej hodnoty funkcie,
- je matematicky neuskutočniteľné zostaviť dva rôzne vstupné reťazce znakov s rovnakou výslednou hodnotou funkcie.

abstrakt digest

Hodnota alebo výsledok vyprodukovaný abstrakčnou funkciou. Slúži na vytvorenie elektronického podpisu.

AES AES

Skratka výrazu **ADVANCED ENCRYPTION STANDARD**, čiže **NORMA VYSPELÉHO ŠIFROVANIA**.

Roku 1997 sa americké Ministerstvo obchodu rozhodlo nájsť náhradu za DES a vyhlásilo súťaž. Víťazom sa stal algoritmus Rijndael belgických kryptografov Joan Daemen a Vincenta Rijmena. Rijndael je bloková šifra, ktorá operuje na 128 bitov veľkých blokoch s kľúčmi 128 bitov dlhými.

akreditácia accreditation

- proces posudzovania spôsobilosti žiadateľa o oprávnenie vykonávať istú činnosť,
- oprávnenie vykonávať istú činnosť – pozitívny výsledok procesu (a).

akreditovaná certifikačná autorita accredited certification authority

Certifikačná autorita, ktorá získala akreditáciu.

Certifikačné autority, ktoré na Slovensku akredituje Národný bezpečnostný úrad, môžu vyhotovovať kvalifikované certifikáty a časové pečiatky.

algoritmus SHA-1 SHA-1 algorithm

Skratka výrazu **SECURE HASH ALGORITHM ONE**, čiže **BEZPEČNÝ ABSTRAKČNÝ ALGORITMUS JEDEN**.

Je najpoužívanejšia abstrakčná funkcia v elektronickom styku. Špecifikoval ho Národný Inštitút Normalizácie a Techniky v Spojených štátoch v norme FIPS 180-1 roku 1995. SHA-1 produkuje 160-bitový abstrakt, ktorý sa považuje za oveľa bezpečnejší ako dovtedajšie komerčné algoritmy.

architektúra IVKX PKIX architecture

Model infraštruktúry verejného kľúča v súlade s normou X.509, ktorý sa skladá z týchto hlavných komponentov:

- klient
- certifikačná autorita
- registračná autorita
- rezpozitórium.

pozri **KLIENT** | **CERTIFIKAČNÁ AUTORITA** | **REGISTRAČNÁ AUTORITA** | **REPOZITÓRIUM**.

ASN.1 ASN.1

Skratka výrazu **ABSTRACT SYNTAX NOTATION ONE**, čiže **ABSTRAKTNÁ NOTÁCIA SYNTAXE JEDEN**.

Dáta typizujúci jazyk určený na špecifikovanie komunikačného protokolu aplikačnej vrstvy. ASN.1 je definovaná v norme ISO/IEC 8824.

asymetrické šifrovanie asymmetric encryption

Technika šifrovania, ktorá využíva jeden kľúč na zašifrovanie správy a druhý kľúč na dešifrovanie správy. Táto technika tvorí základ infraštruktúry verejného kľúča.

pozri **SYMETRICKÉ ŠIFROVANIE**.

autentifikácia authentication

Proces overovania informácií o totožnosti, vlastníctve a oprávnení. Metódy autentifikácie zahŕňajú heslá, výrobky na elektronický podpis, šikovné karty a biometrické prístroje.

pozri **BEZPEČNOSŤ INFORMÁCIÍ A ELEKTRONICKEJ KOMUNIKÁCIE** | **ROZDIEL MEDZI AUTENTIFIKÁCIOU A IDENTIFIKÁCIOU**.

autorizácia
authorization

Proces určovania a udeľovania práv na vykonávanie činností alebo na prístup k informáciám v rámci informačného systému.

Autorizácia je jeden zo šiestich faktorov, ktoré rozhodujú o bezpečnosti informácií a elektronickej komunikácie.

pozri BEZPEČNOSŤ INFORMÁCIÍ A ELEKTRONICKEJ KOMUNIKÁCIE.

B

bezpečná pošta
secure mail

Technika, vďaka ktorej používateľ má možnosť overiť totožnosť odosielateľa, preveriť integritu informácií a zabezpečiť dôveryhodnosť správ.

bezpečnosť informácií a elektronickej komunikácie
information and communication security

Pojem bezpečnosti a ochrany informačného systému sa v súčasnosti rozširuje a posúva za hranice ohňových múrov a smerovačov. Informácie a elektronická komunikácia sú bezpečné, ak informačný systém vašej organizácie podporuje tieto procesy:

- identifikácia
- autentifikácia
- autorizácia
- integrita
- utajenie
- nepopierateľnosť.

pozri IDENTIFIKÁCIA | AUTENTIFIKÁCIA | AUTORIZÁCIA | INTEGRITA | UTAJENIE | NEPOPIERATEĽNOSŤ | ROZDIEL MEDZI AUTENTIFIKÁCIOU A IDENTIFIKÁCIOU.

bezpečnostný audit
security audit

Prieskum dodržiavania certifikačných zásad a bezpečnostných pravidiel. Interný audit vykonáva osoba, ktorá je zamestnaná v organizácii a poverená na túto úlohu. Externý audit vykonáva nezávislý orgán.

bezpečný systém
secure system

Systém, v ktorom prístup k údajom a spôsob ich použitia je v súlade s bezpečnostnými pravidlami a certifikačnými zásadami.

biometrika
biometrics

Metóda autentifikácie používateľa, ktorá využíva jednoznačné fyzické vlastnosti, napr. odtlačky prstov, skenovaný obraz sietnice oka, geometriu ruky, hlasovú stopu a iné.

brána
gateway

Modul, ktorý umožňuje prenos informácií medzi sieťami postavenými na rozdielnych komunikačných protokoloch. Brána prenáša a pretvára údaje do podoby, ktorá je kompatibilná s protokolom prijímajúcej siete.

brutálna sila
brute force

Technika útoku, ktorá namiesto logiky používa opakované, tie isté kroky s cieľom premôcť ochranu. Používa sa na vyskúšanie rôznych variantov prístupového hesla alebo na zisťovanie aktívnych modemových liniek.

C

CA
CA

Skratka slovenského výrazu CERTIFIKAČNÁ AUTORITA alebo anglického výrazu CERTIFICATION AUTHORITY.

pozri CERTIFIKAČNÁ AUTORITA.

certifikačná autorita
certification authority

Dôveryhodný orgán, ktorý vyhotovuje a zrušuje certifikáty. V koncepcii infraštruktúry verejného kľúča X.509 je certifikačná autorita jedna zo štyroch základných zložiek.

pozri KLIENT | REGISTRAČNÁ AUTORITA | REPOZITÓRIUM | ARCHITEKTÚRA IVKX.

certifikát certificate

Elektronický doklad totožnosti majiteľa certifikátu. Do certifikátu sa zaznačuje množstvo údajov. Niektoré z nich sú povinné zo zákona, iné sú dobrovoľné. Pre používateľa bezpečnej elektronickej komunikácie je dôležitý fakt, že bez certifikátu nie je možné podpisovať dokumenty elektronickým podpisom.

časová pečiatka time stamp

Zápis, ktorý určuje dátum a čas podpisania elektronickeho dokumentu. Používanie časovej pečiatky významne podporuje princíp nepopierateľnosti a bráni útoku akým je prehrávanie zo záznamu.

D

DER DER

Skratka výrazu **DISTINGUISHED ENCODING RULES**, čiže **PRAVIDLÁ JEDNOZNAČNÉHO KÓDOVANIA**.

V ASN.1 zásady kódovania dátatypových hodnôt do podoby reťazcov bitov.

DES DES

Skratka výrazu **DATA ENCRYPTION STANDARD**, čiže **NORMA ŠIFROVANIA ÚDAJOV**.

DES je najbežnejšia metóda symetrického šifrovania. Americké Ministerstvo obchodu ju schválilo na šifrovanie správ, ktoré nemuseli byť utajené, roku 1977 v norme FIPS 46. Roku 1994 bola znova publikovaná v norme FIPS 46-2. Je veľmi rýchla a často sa používa pri asymetrickom šifrovaní na šifrovanie dlhých textov.

dešifrovanie decryption

Proces, ktorým sa pretvára šifrovaný text do pôvodnej podoby nazývanej zrozumiteľný text.

Diffieho-Hellmanov algoritmus Diffie-Hellman algorithm

Roku 1976 Whitfield Diffie a Martin Hellman publikovali geniálnu techniku, ktorá umožňuje dvom stranám dohodnúť sa na spoločnom tajnom kľúči pre vzájomnú komunikáciu. Výhoda

tejto techniky je, že nevyžaduje šifrovanie a môže sa používať aj na nezabezpečených komunikačných kanáloch.

Direktíva o elektronickom podpise Electronic Signature Directive

Celý názov je Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (OJ L 13, 19.1.2000), čiže Direktíva 1999/93/EK Európskeho Parlamentu a Rady z 13. decembra 1999 o Komunitnom rámci pre elektronické podpisy.

Právna norma, ktorá určuje základné pravidlá a požiadavky súvisiace s používaním elektronickeho podpisu v elektronickej komunikácii v rámci Európskej Komunity.

dĺžka kľúča key length

Dĺžka reťazca bitov tvoriaceho kľúč. Dĺžka kľúča a druh šifrovacieho algoritmu rozhodujú o bezpečnosti šifrovaných údajov.

dôverovaná tretia strana trusted third party

Aj keď v striktnom zmysle slova je rozdiel medzi dôverovanou osobou a dôveryhodnou osobou, e-podpis.sk dáva prednosť pojmu dôveryhodná tretia strana.

pozri DÔVERYHODNÁ TRETIA STRANA.

dôveryhodná tretia strana trusted third party

Osoba alebo inštitúcia, ktorá má dôveru účastníkov transakcie. Certifikačná autorita je dôveryhodná tretia strana, pretože garantuje totožnosť jedného alebo oboch účastníkov.

druh certifikátu certificate class

Vyjadruje stupeň bezpečnosti a ochrany certifikátu, ktorý certifikačná autorita vyhotovuje pre používateľa, a stupeň zodpovednosti, ktorý certifikačná autorita nesie vo vzťahu k certifikátu.

E

elektronický podpis electronic signature

Elektronický podpis je technika, spôsob, ktorým sa podpisujú elektronické dokumenty a ktorým možno dodatočne preukázať, že sa v dokumente neurobili neoprávnené zmeny.

e-podpis electronic signature

- (a) najautoritatívnejší zdroj informácií o elektronickom podpise v strednej Európe – webové sídlo www.e-podpis.sk,
- (b) elektronický podpis.

extranet extranet

Sieť, ktorú spravuje organizácia sama alebo ju v mene organizácie spravuje iná organizácia. Zmyslom extranetu je umožniť komunikáciu medzi organizáciou a externými používateľmi. Extranet využíva možnosti verejnej siete Internetu, ale odopiera prístup osobám, ktoré nie sú organizáciou oprávnené. Podnik tak môže dať zákazníkom, spriazneným firmám a obchodným partnerom prístup k zdrojom podniku pomocou extranetového webového serveru.

F

FTP FTP

Skratka výrazu **FILE TRANSFER PROTOCOL**, čiže **PROTOKOL PRENOSU SÚBOROV**.

Umožňuje v súčinnosti s protokolom TCP prenášať údaje medzi systémami. Bezpečnosť sa zaisťuje identifikáciou používateľa a heslom.

G

Gejtvej Gateway

pozri BRÁNA.

H

hashovacia funkcia hash function

Anglický výraz “hash” znamená v slovenčine rozsekať, rozomlieť. Webové sídlo e-podpis.sk sa domnieva, že namiesto výrazu hashovacia funkcia alebo rozomieľacia funkcia, je výraz abstrakčná funkcia vhodnejší.

pozri ABSTRAKČNÁ FUNKCIA.

heslo password

Chránený súkromný reťazec znakov.

Najjednoduchší spôsob ochrany integrity systému a kontroly prístupu k údajom.

HTML HTML

Skratka výrazu **HYPERTEXT MARKUP LANGUAGE**, čiže **ZNAČKOVACÍ JAZYK HYPERTEXTU**.

Populárny programovací jazyk, ktorým sa vyrábajú webové stránky. Jazyk umožňuje definovať obsah a formát hypermediálnych dokumentov umiestnených na webe.

HTTP HTTP

Skratka výrazu **HYPERTEXT TRANSFER PROTOCOL**, čiže **PROTOKOL PRENOSU HYPERTEXTU**.

Protokol používa mechanizmus výzvy a odpovede a umožňuje používateľovi prezerat' zdroje webovej siete.

HTTPS HTTPS

Skratka výrazu **HYPERTEXT TRANSFER PROTOCOL SECURE**, čiže **PROTOKOL BEZPEČNÉHO PRENOSU HYPERTEXTU**.

Bezpečný variant HTTP, ktorým sa pomocou protokolu SSL šifrujú jednotlivé dokumenty namiesto celých seáns.

IDEA IDEA

Skratka výrazu **INTERNATIONAL DATA ENCRYPTION STANDARD**, čiže **MEDZINÁRODNÁ NORMA ŠIFROVANIA ÚDAJOV**.

Symetrický šifrovací algoritmus mnohými považovaný za nástupcu algoritmu DES. Je patentovaný v Európe a smie sa bezplatne používať na nekomerčné účely.

identifikácia identification

Proces spoznania osoby alebo zistenia totožnosti osoby. Ľudí identifikujeme spoznaním ich fyzických vlastností, napr. tváre alebo postavy. v kryptografickom zmysle a z hľadiska infraštruktúry verejného kľúča cieľom je viazať s osobou nejakú jedinečnú informáciu, ktorú len táto osoba dokáže reprodukovať a navyše zabrániť odpočúvateľovi zaznamenať túto jedinečnú informáciu. Identifikácia je jeden zo šiestich faktorov, ktoré rozhodujú o bezpečnosti informácií a elektronickej komunikácie.

pozri **BEZPEČNOSŤ INFORMÁCIÍ A ELEKTRONICKEJ KOMUNIKÁCIE | ROZDIEL MEDZI AUTENTIFIKÁCIOU A IDENTIFIKÁCIOU**.

IETF IETF

Skratka výrazu **INTERNET ENGINEERING TASK FORCE**, čiže **ÚDERKA INTERNETOVÝCH INŽINIEROV**.

pozri **ÚDERKA INTERNETOVÝCH INŽINIEROV**.

infraštruktúra verejného kľúča public key infrastructure

Súbor infraštruktúrálnych služieb technického a právneho rázu, ktorý umožňuje používanie elektronickeho podpisu a šifrovanie.

integrita integrity

Proces, ktorým sa zabezpečuje súdržnosť údajov – že údaje nie sú neoprávnene vytvorené, pozmenené alebo zničené.

Integrita je jeden zo šiestich faktorov, ktoré rozhodujú o bezpečnosti informácií a elektronickej komunikácie.

pozri **BEZPEČNOSŤ INFORMÁCIÍ A ELEKTRONICKEJ KOMUNIKÁCIE**.

intranet intranet

Vnútorňá sieť organizácie. Používa sa najmä na distribúciu dokumentov, prístup k databázam a vývoj softvéru. Využíva webové aplikácie ako webové stránky, prezerače, FTP a e-mail. Prístup do vnútornej siete majú len pracovníci organizácie.

IP IP

Skratka výrazu **INTERNET PROTOCOL**, čiže **INTERNETOVÝ PROTOKOL**.

Protokol siet'ovej vrstvy na Internete. IP definuje spôsob formátovania údajov nazývaných hlavička a prirad'ovania hlavičiek k paketom údajov, ktoré sa odosielajú. IP je nespojovací protokol – každý paket je nezávislý. Vnútorne Internetový protokol nie je bezpečný.

IPSec IPSec

Skratka výrazu **INTERNET PROTOCOL SECURITY**, čiže **BEZPEČNOSŤ INTERNETOVÉHO PROTOKOLU**.

Šifrovací systém, ktorý kontroluje integritu datagramov IP. Služi na zabezpečenie odosielaných údajov medzi dvoma alebo viacerými sieťami. Je hlavným prvkom virtuálnych súkromných sietí.

ISO ISO

Skratka výrazu **INTERNATIONAL STANDARDS ORGANIZATION**, čiže **MEDZINÁRODNÁ ORGANIZÁCIA PRE NORMALIZÁCIU**.

ITU ITU

Skratka výrazu **INTERNATIONAL TELECOMMUNICATIONS UNION**, čiže **MEDZINÁRODNÁ ÚNIA TELEKOMUNIKÁCIÍ**.

IVK PKI

Skratka výrazu **INFRAŠTRUKTÚRA VEREJNÉHO KĽÚČA**, čiže **PUBLIC KEY INFRASTRUCTURE**.

pozri **INFRAŠTRUKTÚRA VEREJNÉHO KĽÚČA**.

J

jednoznačné meno
distinguished name

Jednoznačný, neopakovateľný reťazec vlastností, ktorý z celkového pohľadu určuje totožnosť osoby, napr. subskribenta alebo certifikačnej autority. Koncepcia infraštruktúry verejného kľúča vyžaduje, že s každým jednotlivcom sa spája jednoznačné meno v registri.

K

Kerberos
Kerberos

Autentifikačný a autorizačný systém klient-server, ktorý bol vyvinutý v MIT koncom 70tych rokov minulého storočia. Používa symetrické šifrovanie.

klient
client

V zmysle architektúry IVKX klient je

- (a) koncový používateľ certifikátu,
- (b) osoba alebo systém, pre ktorý je certifikát vyhotovený.

pozri CERTIFIKAČNÁ AUTORITA | REGISTRAČNÁ AUTORITA | REPOZITÓRIUM | ARCHITEKTÚRA IVKX.

kľúč
key

Tajné údaje používané pri šifrovaní alebo dešifrovaní.

kompromitovaný kľúč
compromised key

Súkromný kľúč, ktorý bol vyzradený alebo existuje podozrenie, že jeho utajenie bolo porušené.

krížový certifikát
cross certificate

Certifikát, ktorý vyhotovila jedna certifikačná autorita druhej certifikačnej autorite na podporu verejného kľúča druhej certifikačnej autority.

kryptoanalýza
cryptanalysis

Odbor v kryptológii, ktorý sa zaoberá lámaním šifier.

kryptografia
cryptography

Odbor v kryptológii, ktorý sa zaoberá vývojom šifier a techník šifrovania.

kryptografický akcelerátor
cryptographic accelerator

Zariadenie na podporu kryptografických operácií. Pretože šifrovanie a dešifrovanie sú matematicky a výpočtovo intenzívne operácie, používa sa urýchľovač operácií. Zariadenie sa môže používať aj na bezpečnú úschovu podpisových kľúčov.

kryptografický algoritmus
cryptographic algorithm

Algoritmus na šifrovanie a dešifrovanie údajov v elektronickej komunikácii cez sieť. Známe kryptografické algoritmy sú DES, RSA, MD5, SHA, IDEA.

kryptogram
cryptogram alebo cipher text

pozri ŠIFROVANÝ TEXT.

kryptológia
cryptology

Veda a štúdium kryptografie a kryptoanalýzy.

kvalifikovaný certifikát
qualified certificate

Výmysel Európskej Komisie, ktorá stanovila v Direktíve o elektronickej podpise, že certifikát vyhotovený pre fyzickú osobu sa bude volať kvalifikovaný certifikát. Na Slovensku kvalifikovaný certifikát musí spĺňať zákonom určené požiadavky.

L

LAN
LAN

Skratka výrazu LOCAL AREA NETWORK, čiže MIESTNA SIEŤ.

Množina počítačov, ktoré sú navzájom prepojené v obmedzenom priestore. Miestna sieť je

obvyčajne vysoko priepustná a komunikácia cez ňu býva veľmi rýchla.

LDAP LDAP

Skratka výrazu **LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL**, čiže **ODĽAĤENÝ PROTOKOL PRÍSTUPU K REGISTRU**.

Ludia, časti telekomunikačných sietí, počítačové aplikácie alebo iné automatizované systémy potrebujú vyhľadávať a získavať informácie. Medzinárodná Telekomunikačná Únia a Medzinárodná Organizácia Normalizácie v 80tych rokoch minulého storočia špecifikovali v norme X.500 model polyfunkčného distribuovaného katalógu. Táto technológia sa však ukázala byť veľmi zložitá a finančne nákladná. Internetová verejnosť vyvinula svoj protokol, ktorý je úplne kompatibilný s X.500, je však jednoduchší a ľahšie sa implementuje. Preto sa volá odľahčeným protokolom.

lehota platnosti certifikátu certificate validity period

Údaj o platnosti certifikátu. Po lehote platnosti možno certifikát použiť len na potvrdenie činnosti vykonanej v čase jeho platnosti, napr. na overenie elektronického podpisu na starom dokumente.

M

MAC MAC

Skratka výrazu **MESSAGE AUTHENTICATION CODE**, čiže **AUTENTIFIKAČNÝ KÓD SPRÁVY**.

Matematická funkcia, ktorá prijíma reťazec bitov ľubovoľnej dĺžky ako vstup a produkuje ako výstup kód nemennej dĺžky. Autentifikačný kód správy sa pripája k správe a slúži na potvrdenie pravosti správy, t.j., že správa nebola pri prenose nikým neoprávnene pozmenená. Dve rozšírené metódy generovania autentifikačných kódov sú abstrakčná funkcia a systém symetrických šifier.

maškaráda masquerade

Útok na bezpečnosť elektronickej komunikácie, pri ktorom narušiteľ falošne predstiera, že je legitímnym používateľom.

MD5 MD5

Skratka výrazu **MESSAGE DIGEST FIVE**, čiže **ABSTRAKT SPRÁVY PÄŤ**.

Abstrakčný algoritmus, ktorý vyvinula spoločnosť RSA. Produkuje 128 bitov dlhý abstrakt, je však optimalizovaný pre 32-bitové procesory.

muž v strede man in the middle

Útok na bezpečnosť elektronickej komunikácie, pri ktorom sa narušiteľ umiestni medzi dvoch nič netušiacich účastníkov počas komunikačnej seansy.

N

Národný bezpečnostný úrad National Security Bureau

Orgán na Slovensku, ktorý v súvislosti s používaním elektronického podpisu a infraštruktúry verejného kľúča vykonáva aj tieto činnosti:

- (a) udeľuje a odníma certifikačným autoritám akreditáciu,
- (b) eviduje certifikačné authority pôsobiace na Slovensku,
- (c) certifikuje výrobky na elektronický podpis.

NBÚ NBU

Skratka výrazu **NÁRODNÝ BEZPEČNOSTNÝ ÚRAD**, čiže **NATIONAL SECURITY BUREAU**.

pozri **NÁRODNÝ BEZPEČNOSTNÝ ÚRAD**.

nepopierateľnosť non-repudiation

Bezpečnostný princíp v elektronickej komunikácii, ktorý chráni jedného účastníka komunikácie pred falošným tvrdením druhého účastníka, že komunikácia sa neuskutočnila. Nepopierateľnosť je jeden zo šiestich faktorov, ktoré rozhodujú o bezpečnosti informácií a elektronickej komunikácie.

pozri **BEZPEČNOSŤ INFORMÁCIÍ A ELEKTRONICKEJ KOMUNIKÁCIE**.

NIST

Skratka výrazu **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**, čiže **NÁRODNÝ INŠTITÚT NORMALIZÁCIE A TECHNIKY**.

Pôsobí v Spojených štátoch.

norma X.509 x.509 standard

Norma, ktorá tvorí všeobecne uznávaný základ infraštruktúry verejného kľúča. Definuje formáty údajov a postupy distribúcie certifikátov verejného kľúča. Mimoriadne významná je norma X.509v3, ktorá určuje štruktúru certifikátu a zoznamu zrušených certifikátov.

O

obnovenie certifikátu certificate renewal

Postup, ktorého účelom je predĺžiť platnosť vyhotoveného ešte platného certifikátu.

OCSP OCSP

Skratka výrazu **ONLINE CERTIFICATE STATUS PROTOCOL**, čiže **PROTOKOL OZNAMOVANIA STAVU CERTIFIKÁTU ONLINE**.

Protokol, ktorý umožňuje overiť platnosť certifikátu v reálnom čase.

odopretie služby denial of service

Útok na bezpečnosť elektronickej komunikácie, pri ktorom narušiteľ zavalí kritický informačný systém, napr. autentifikačný alebo webový server, alebo uzavrie k nemu prístup.

ohňový múr firewall

Hardvérový a softvérový modul, ktorý chráni zdravú časť siete pred nekontrolovateľne sa šíriacim nebezpečenstvom v inej časti siete. Ohňový múr je obvyčajne umiestnený medzi vnútornou sieťou organizácie a verejnou internetovou chrbitcou.

OID

Skratka výrazu **OBJECT IDENTIFIER**, čiže **IDENTIFIKÁTOR OBJEKTU**.

Identifikátor objektu je hodnota obsahujúca alfanumerickú postupnosť, ktorá sa môže prideliť registrovanému objektu a má tú vlastnosť, že je jedinečná medzi všetkými identifikátormi objektov. OID je definovaný v norme ISO/IEC 9834.

opätovné získanie kľúča key recovery

Postup, ktorým sa vytvorí stratený súkromný šifrovací kľúč.

P

pár kľúčov key pair

Jedinečná kombinácia súkromného a verejného kľúča, ktorá sa vyskytuje v systéme asymetrického šifrovania. Umožňuje zabezpečiť integritu, autentickosť a nepopierateľnosť v elektronickej komunikácii.

PEM PEM

Skratka výrazu **PRIVACY ENHANCED MAIL**, čiže **POŠTA SO ZVÝŠENOU DÔVERNOSŤOU**.

Norma, ktorú roku 1993 vypracovala internetová verejnosť s cieľom zvýšiť bezpečnosť elektronickej pošty. Norma nebola úspešná, stala sa však základom pri vyvíjaní infraštruktúry verejného kľúča.

PGP PGP

Skratka výrazu **PRETTY GOOD PRIVACY**, čiže **NIE ZLÁ DÔVERNOSŤ**.

Softvér, ktorý umožňuje bezpečnú elektronickej poštu. Vyvinul ho počítačový vedec a politický aktivista Phil Zimmerman. PGP získal popularitu, pretože bol bezplatný. Komerčnú verziu prestala spoločnosť Network Associates podporovať v marci 2002.

PIN PIN

Skratka výrazu **PERSONAL IDENTIFICATION NUMBER**, čiže **OSOBNÉ IDENTIFIKAČNÉ ČÍSLO**.

Súkromný kód, ktorý slúži na identifikáciu používateľa.

PKCS #7 PKCS #7

Skratka výrazu **PUBLIC KEY CRYPTOGRAPHY STANDARD NUMBER SEVEN**, čiže **NORMA ČÍSLO 7 ŠIFROVANIA VEREJNÉHO KEÚČA**.

Okrem číselného označenia má táto norma aj svoj názov Cryptographic Message Syntax Standard, v slovenčine Norma syntaxe šifrovanej správy. Definuje ochranu správ šifrovaním. Jej význam je ešte väčší v súčinnosti s normou PKCS #10.

PKCS #12 PKCS #12

Skratka výrazu **PUBLIC KEY CRYPTOGRAPHY STANDARD NUMBER TWELVE**, čiže **NORMA ČÍSLO 12 ŠIFROVANIA VEREJNÉHO KEÚČA**.

Okrem číselného označenia má táto norma aj svoj názov Personal Information Exchange Syntax Standard, v slovenčine Norma syntaxe výmeny osobných údajov. Norma definuje šifrovaný skladovací kontajner, ktorý možno používať ako prenosný formát na bezpečné prenášanie kľúčov z jedného úložného miesta na iné.

PKI PKI

Skratka výrazu **PUBLIC KEY INFRASTRUCTURE**, čiže **INFRAŠTRUKTÚRA VEREJNÉHO KEÚČA**.

Aj na Slovensku často používaná skratka. Webové sídlo e-podpis.sk sa domnieva, že anglický výraz možno ľahko a bezbolestne preložiť do slovenčiny a preto používa skratku IVK – infraštruktúra verejného kľúča.

pozri INFRAŠTRUKTÚRA VEREJNÉHO KEÚČA.

PKIX PKIX

Skratka výrazu **PUBLIC KEY INFRASTRUCTURE X.509**, čiže **INFRAŠTRUKTÚRA VEREJNÉHO KEÚČA X.509**.

Pod týmto názvom roku 1994 Úderka Internetových Inžinierov (Internet Engineering Task Force) ustanovila pracovnú skupinu a poverila ju najmä dvoma úlohami –

- (a) prepracovať normu X.509, aby vyhovovala potrebám internetových protokolov,
- (b) vypracovať ďalšie špecifikácie potrebné pre interoperabilitu internetových protokolov a pre aplikácie využívajúce certifikáty založené na norme X.509.

poskytovateľ certifikačných služieb certification service provider

Výraz “poskytovateľ certifikačných služieb” je definovaný v Direktíve o elektronickom podpise. Používa ho nemecké aj francúzske právo.

Slovenský Zákon o elektronickom podpise nepoužíva tento europeizovaný výraz, prevzal americký výraz “certifikačná autorita”. Nuž, aby e-podpis.sk nemohol byť obvinený z klamstva – výraz “poskytovateľ certifikačných služieb” sa vyskytuje v Zákone o elektronickom podpise, slúži však iba na okrasu.

pozastavenie certifikátu certificate suspension

Dočasné prerušenie platnosti certifikátu obyčajne na žiadosť subskribenta. Pozastavenie certifikátu je háklivá vec, pretože X.509 v súčasnosti neuvádza kód na vyznačenie takého stavu.

prehrávanie zo záznamu replay

Útok na bezpečnosť elektronickej komunikácie, pri ktorom narušiteľ neoprávnene používa prístupové heslo, ktoré predtým zachytil. Priradenie časovej pečiatky k heslu eliminuje toto riziko.

R

RA RA

Skratka výrazu **REGISTRAČNÁ AUTORITA**, čiže **REGISTRATION AUTHORITY**.

pozri REGISTRAČNÁ AUTORITA.

RC4 RC4

Skratka výrazu **RIVEST CIPHER FOUR** alebo **RON'S CODE FOUR**, čiže **RIVESTOVA ŠIFRA ŠTYRI** alebo **RONOV KÓD ŠTYRI**.

RC4 je prúdová šifra, ktorá je založená na systéme šifrovania jednotlivých bitov. Je veľmi

rýchla, rýchlejšia ako bloková šifra a podporuje kľúče rôznych dĺžok.

Reg TP Reg TP

Skratka výrazu **REGULIERUNGSBEHÖRDE FÜR TELEKOMMUNIKATION UND POST**, čiže **REGULAČNÝ ÚRAD TELEKOMUNIKÁCIÍ A POŠTY**.

Orgán v Nemecku, ktorý má široké právomoci v oblasti schvaľovania výrobkov na elektronický podpis, dozoru nad poskytovateľmi certifikačných služieb a akreditovania certifikačných autorít.

registrácia registration alebo enrollment

Jedna z činností, ktorú definuje PKIX. v procese registrácie sa koncový používateľ, ktorého meno bude uvedené v certifikáte, predstaví certifikačnej autorite alebo registračnej autorite. Meno a iné údaje, ktoré budú slúžiť na identifikovanie subskribenta, treba overiť v súlade so súpisom certifikačných praktík certifikačnej autority.

registračná autorita registration authority

Dôveryhodná fyzická alebo právnická osoba, ktorá je oprávnená vyhotovovať certifikáty registrovať iné fyzické alebo právnické osoby žiadajúce vyhotovenie certifikátu.

pozri CERTIFIKAČNÁ AUTORITA | KLIENT | REPOZITÓRIUM | ARCHITEKTÚRA IVKX.

repozitórium repository

Systém – môže byť distribuovaný – ktorý zhromažďuje certifikáty a zoznamy zrušených certifikátov a sprístupňuje ich koncovým používateľom. Repoziatórium je jeden z hlavných komponentov architektúry IVKX.

pozri ARCHITEKTÚRA IVKX.

rozdiel medzi autentifikáciou a identifikáciou difference between authentication and identification

V prípade identifikácie overovateľ preskúma predložené údaje vzhľadom na všetky osoby, ktoré pozná, s cieľom zistiť s ktorou osobou má do činenia. V prípade autentifikácie sa však skúmajú údaje vzhľadom na jedinú osobu, ktorej totožnosť už bola kedysi určená.

Rozhodnutie o elektronickom podpise Electronic Signature Decision

Celý názov je Commission Decision 2000/709/EC of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (OJ L 289, 16.11.2000), čiže Rozhodnutie 2000/709/EK Komisie zo 6. novembra 2000 o najmenších možných podmienkach, na ktoré členské štáty musia prihliadať pri určovaní orgánov podľa článku 3 odsek 4 Direktívy 1999/93/EK Európskeho Parlamentu a Rady z 13. decembra 1999 o Komunitnom rámci pre elektronické podpisy.

Právna norma, ktorá stanovuje základné požiadavky pre orgány, ktoré budú posudzovať súlad bezpečných zariadení na tvorbu elektronického podpisu s požiadavkami stanovenými v Doplnku III Direktívy o elektronickom podpise.

RSA RSA

Skratka výrazu **RIVEST SHAMIR ADLEMAN**.

- (a) jeden z prvých šifrovacích systémov verejného kľúča, ktorý bol patentovaný roku 1983. Algoritmus RSA je založený na faktorizácii prvočísel. Považuje sa za bezpečný a vhodný na šifrovanie v rámci infraštruktúry verejného kľúča.
- (b) RSA Security Inc. je meno spoločnosti, ktorú spoločne založili Ron Rivest, Adi Shamir a Larry Adleman.

S

S/MIME S/MIME

Skratka výrazu **SECURE MIME** alebo **SECURE / MULTIPURPOSE INTERNET MAIL EXTENSIONS**, čiže **BEZPEČNÉ/POLYFUNKČNÉ PRÍDAVKY K INTERNETOVEJ POŠTE**.

Norma vypracovaná Internetovou Úderkou Inžinierov, ktorá definuje princípy šifrovania alebo elektronického podpisovania elektronických správ.

samopodpísaný certifikát
self-signed certificate

Certifikát vyhotovovateľa certifikátu, ktorý je podpísaný elektronickým podpisom toho istého vyhotovovateľa certifikátu.

SCP
CPS

Skratka výrazu **SÚPIS CERTIFIKAČNÝCH PRAKTÍK**, čiže **CERTIFICATION PRACTICES STATEMENT**.

pozri **SÚPIS CERTIFIKAČNÝCH PRAKTÍK**.

sériové číslo certifikátu
certificate serial number

Jedinečné číslo certifikátu udelené príslušným vyhotovovateľom certifikátu.

SET
SET

Skratka výrazu **SECURE ELECTRONIC TRANSACTIONS**, čiže **BEZPEČNÉ ELEKTRONICKÉ TRANSAKcie**.

Protokol, ktorý podporuje platby kreditnými kartami. Bol vyvinutý pod vedením spoločností Visa a MasterCard.

SHA-1
SHA-1

Skratka výrazu **SECURE HASH ALGORITHM ONE**, čiže **BEZPEČNÝ ABSTRAKČNÝ ALGORITMUS JEDEN**.

pozri **ALGORITMUS SHA-1**.

smerovač
router

Hardvérový a softvérový modul vybavený smerovacou inteligenciou, ktorý spája miestnu sieť so vzdialenou sieťou.

správa certifikátov
certificate management

Činnosti a procesy, ktoré súvisia s certifikátmi počas ich užitočného života. Správa certifikátov zahŕňa:

- registráciu certifikátu
- obnovenie certifikátu
- zrušenie certifikátu.

pozri **REGISTRÁCIA | OBNOVENIE CERTIFIKÁTU | ZRUŠENIE CERTIFIKÁTU**.

SSL
SSL

Skratka výrazu **SECURE SOCKETS LAYER**, čiže **BEZPEČNOSTNÁ VRSTVA ZÁSUVIEK**.

Protokol vyvinutý spoločnosťou Netscape, ktorý definuje ochranu seanse na rozdiel od protokolu HTTPS, ktorý zabezpečuje jednotlivé transakcie. Technika SSL používa algoritmy RSA a DES na šifrovanie a autorizovanie a MD5 na kontrolu integrity.

SSO
SSO

Skratka výrazu **SINGLE SIGN ON**, čiže **JEDINÁ PRIHLÁŠKA** alebo **LEN JEDNO OZNÁMENIE ÚČASTI**.

Proces, v ktorom používateľ informačného systému uvedie svoju totožnosť len raz, aby získal prístup k niekoľkým aplikáciám alebo zdrojom, bez toho, aby sa musel identifikovať každému zdroju a používať niekoľko prístupových hesiel.

SSSO
SSSO

Skratka výrazu **SECURE SINGLE SIGN ON**, čiže **JEDINÁ BEZPEČNÁ PRIHLÁŠKA** alebo **LEN JEDNO BEZPEČNÉ OZNÁMENIE ÚČASTI**.

Proces akým je SSO, s tým rozdielom, že sa používa tzv. silná autentifikácia totožnosti používateľa. SSSO šifruje všetky pochody a prevádzku informačného systému a využíva certifikáty na identifikovanie klientov a serverov.

strana spoliehajúca sa na elektronický podpis
relying party

Osoba, ktorá získa certifikát subskribenta, aby použila subskribentov verejný kľúč, pričom overí podpis certifikačnej autority na certifikáte pomocou verejného kľúča certifikačnej autority.

subskribent
subscriber

Osoba, pre ktorú bol certifikát vyhotovený. Možno povedať majiteľ certifikátu na rozdiel od držiteľa certifikátu.

súkromný kľúč
private key

Jeden z páru kľúčov v systéme asymetrického šifrovania, ktorý by mal byť vždy utajený a známy len jeho majiteľovi. Majiteľ ho používa najmä na vytvorenie elektronického podpisu.

súpis certifikačných praktík
certification practices statement

Dokument, ktorý definuje zásady a postupy vyhotovovania a spravovania certifikátov, ako aj

práva a povinnosti strán zúčastnených na procese certifikácie. Možno povedať kódex certifikačnej praxe.

symetrické šifrovanie symmetric encryption

Šifrovacia technika, ktorá používa ten istý kľúč na šifrovanie aj dešifrovanie.

pozri ASYMETRICKÉ ŠIFROVANIE.

šifrovací kľúč encryption key

Reťazec bitov používaný šifrovacím algoritmom na šifrovanie. Symetrické algoritmy ho používajú aj na dešifrovanie.

šifrovanie encryption

Kryptografické pretváranie údajov, ktorého výsledkom je šifrovaný text. Takýto text sa tretím osobám javí ako náhodný reťazec znakov, z ktorého nemožno vyčítať užitočnú informáciu.

šifrovaný text cipher text

Zašifrované údaje, ktoré sú nezrozumiteľné bez použitia kryptografických techník a príslušného dešifrujúceho kľúča.

šikovná karta smart card

Karta, ktorá vyzerá ako banková karta, je však vybavená mikroprocesorom. Možno ju používať ako bezpečné médium na uchovávanie a prepravu súkromného kľúča alebo certifikátu.

T

trieda certifikátu certificate class

pozri DRUH CERTIFIKÁTU.

3DES 3DES

pozri TROJITÝ DES.

triple DES triple DES

pozri TROJITÝ DES.

trojitý DES 3DES alebo Triple DES

Blokový šifrovací algoritmus, ktorý prebieha v troch krokoch:

- (1) 64-bitový blok sa zašifruje kľúčom A,
- (2) výsledok prvého kroku sa dešifruje kľúčom B,
- (3) výsledok druhého kroku sa zašifruje kľúčom C.

Kľúče A a C sú niekedy tie isté.

Trojité DES sa všeobecne považuje za oveľa silnejší ako DES. Nevýhodou je vysoké zaťaženie procesoru, najmä ak je algoritmus implementovaný v softvéri.

tScheme tScheme

Názov dobrovoľnej neziskovej organizácie v Spojenom Kráľovstve, ktorej úlohou je skúmať a schvaľovať služby poskytované certifikačnými autoritami.

U

Úderka Internetových Inžinierov Internet Engineering Task Force

Organizácia, ktorá definuje technické špecifikácie a normy týkajúce sa Internetu. Úderka vydáva a spracúva žiadosti o pripomienky (RFC), ktoré sú predzvest'ou nových nápadov neskôr realizovaných.

ÚOOÚ UOOU

Skratka výrazu **ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ**.

Orgán v Česku, ktorý schvaľuje výroby na elektronický podpis, dozerá na poskytovateľov certifikačných služieb a akredituje certifikačné authority.

úrad pre správu certifikačných zásad Policy Management Authority alebo Policy Authority

Orgán, ktorý posudzuje a rozhoduje, či certifikačná autorita spĺňa kritériá infraštruktúry verejného kľúča a ktorá vykonáva pravidelnú kontrolu akreditovaných certifikačných autorít.

Na Slovensku týmto úradom je Národný bezpečnostný úrad.

utajenie confidentiality

Zabezpečenie, že informácia nie je vyzradená alebo prístupná neoprávneným osobám. Utajenie je jeden zo šiestich faktorov, ktoré rozhodujú o bezpečnosti informácií a elektronickej komunikácie.

pozri BEZPEČNOSŤ INFORMÁCIÍ A ELEKTRONICKEJ KOMUNIKÁCIE.

V

verejný kľúč public key

Jeden z páru kľúčov, ktorý sa používa v systéme asymetrického šifrovania na bezpečnú komunikáciu s majiteľom prislúchajúceho súkromného kľúča.

virtuálna súkromná sieť virtual private network

Technológia, ktorá umožňuje vytvorenie uzavretej komunikačnej siete v rámci verejnej prístupnej siete. Vďaka zašifrovanému tunelu len oprávnené osoby majú prístup k dátam.

VPN VPN

Skratka výrazu **VIRTUAL PRIVATE NETWORK**, čiže **VIRTUÁLNA SÚKROMNÁ SIEŤ**.

pozri VIRTUÁLNA SÚKROMNÁ SIEŤ.

vyhotovenie certifikátu certificate issuance

Činnosť, ktorú vykonáva vyhotovovateľ certifikátu, vrátane odovzdania certifikátu osobe, ktorá požiadala o vyhotovenie certifikátu.

výrobok na elektronický podpis cryptographic hardware token

Zariadenie, pomocou ktorého používateľ vytvára alebo overuje elektronický podpis.

Vzorový zákon o elektronickej podpise UNCITRAL Model law on electronic signatures

Vzor zákona o elektronickej podpise, ktorý vypracovala Komisia Spojených Národov pre

Medzinárodný Obchod a Právo v júli 2001 a odporučila členským krajinám Organizácie Spojených Národov.

X

X.509 X.509

pozri NORMA X.509.

Z

zásady certifikácie certificate policy

Dokument, v ktorom certifikačná autorita v ľudske zrozumiteľnom jazyku špecifikuje pravidlá vyhotovovania a zrušovania certifikátov verejného kľúča. Je určený najmä pre používateľov služieb certifikačnej autority a je obvyčajne stručnejšou verziou súpisu certifikačných praktík.

pozri SÚPIS CERTIFIKAČNÝCH PRAKTÍK.

zoznam zrušených certifikátov certificate revocation list

Zoznam publikovaný vyhotovovateľom certifikátov obsahuje certifikáty, ktorých platnosť skončila alebo bola zrušená alebo pozastavená.

zrozumiteľný text plain text alebo clear text

Údaje, ktoré nie sú zašifrované. V kryptografii zrozumiteľný text sú údaje pred zašifrovaním alebo údaje získané ako výsledok dešifrovania.

zrušenie certifikátu certificate revocation

Ukončenie platnosti certifikátu.

Certifikát sa zruší, keď okolnosti vyžadujú, aby sa platnosť certifikátu skončila pred vypršaním lehoty jeho platnosti alebo keď sa naruší vzťah medzi totožnosťou subskribenta a súkromným kľúčom.

Takéto okolnosti môžu byť zmena mena subskribenta alebo zmena funkcie

subskribenta v rámci organizácie. Vzťah medzi subskribentom a súkromným kľúčom je

porušený, keď bol súkromný kľúč kompromitovaný teda vyzradený, alebo ak existuje pochybnosť, že k podpisovému kľúču má prístup len oprávnená osoba.

Po zrušení certifikátu možno certifikát použiť len na potvrdenie činnosti, ktorá sa uskutočnila ešte pred zrušením, napr. na overenie elektronického podpisu na starom dokumente.

ANGLICKO – SLOVENSKÝ SLOVNÍK

A

accreditation

akreditácia

accredited certification authority

akreditovaná certifikačná autorita

AES

AES

ASN.1

ASN.1

asymmetric encryption

asymetrické šifrovanie

authentication

autentifikácia

authorization

autorizácia

B

biometrics

biometrika

brute force

brutálna sila

C

CA

CA

certificate

certifikát

certificate class

druh certifikátu alebo trieda certifikátu

certificate issuance

vyhotovenie certifikátu

certificate management

správa certifikátov

certificate policy

zásady certifikácie

certificate renewal

obnovenie certifikátu

certificate revocation

zrušenie certifikátu

certificate revocation list

zoznam zrušených certifikátov

certificate serial number

sériové číslo certifikátu

certificate suspension

pozastavenie certifikátu

certificate validity period

lehota platnosti certifikátu

certification authority

certifikačná autorita

certification function

certifikačná činnosť

certification practices statement

súpis certifikačných praktík

certification service provider

poskytovateľ certifikačných služieb

cipher text

šifrovaný text alebo kryptogram

clear text

zrozumiteľný text

client

klient

compromised key

kompromitovaný kľúč

confidentiality

utajenie

CPS

SCP

cross certificate

krížový certifikát

cryptanalysis

kryptoanalýza

cryptographic accelerator

kryptografický akcelerátor

cryptographic algorithm

kryptografický algoritmus

cryptographic hardware token

výrobok na elektronický podpis

cryptography

kryptografia

cryptology

kryptológia

D

decryption

dešifrovanie

denial of service

odopretie služby

DES

DES

difference between authentication and identification

rozdiel medzi autentifikáciou a identifikáciou

Diffie-Hellman algorithm

Diffieho-Hellmanov algoritmus

digest

abstrakt

digital signature

digitálny podpis alebo elektronický podpis

distinguished name

jednoznačné meno

E

ECDSA

ECDSA

electronic signature

elektronický podpis

Electronic Signature Decision

Rozhodnutie o elektronickom podpise

Electronic Signature Directive

Direktíva o elektronickom podpise

encryption

šifrovanie

encryption key

šifrovací kľúč

enrollment

registrácia

e-podpis

e-podpis

extranet

extranet

F

firewall

ohňový múr

FTP

FTP

G

gateway

brána alebo gejtvej

H

hash function

abstrakčná funkcia alebo hashovacia funkcia

HTML

HTML

HTTP

HTTP

HTTPS

HTTPS

I

IDEA

IDEA

identification

identifikácia

IETF

IETF

information and communication security

bezpečnosť informácií a elektronickej komunikácie

integrity

integrita

Internet Engineering Task Force

Úderka Internetových Inžinierov

intranet

intranet

IP

IP

IPSec

IPSec

ISO

ISO

ITU

ITU

K

Kerberos

Kerberos

key

kľúč

key length

dĺžka kľúča

key pair

pár kľúčov

key recovery

opätovné získanie kľúča

L

LAN

LAN

LDAP

LDAP

M

MAC

MAC

man in the middle

muž v strede

masquerade

maškaráda

MD5

MD5

N

National Security Bureau

Národný bezpečnostný úrad

NBU

NBÚ

NIST

NIST

non-repudiation

nepopierateľnosť

O

OCSP

OCSP

OID
OID

P

password
heslo

PEM
PEM

PGP
PGP

PIN
PIN

PKCS #7
PKCS #7

PKCS #12
PKCS #12

PKI
IVK

PKIX
IVKX

PKIX architecture
architektúra IVKX

plain text
zrozumiteľný text

policy authority
úrad pre správu certifikačných zásad

policy management authority
úrad pre správu certifikačných zásad

private key
súkromný kľúč

public key
verejný kľúč

public key infrastructure
infraštruktúra verejného kľúča

Q

qualified certificate
kvalifikovaný certifikát

R

RA
RA

RC4
RC4

Reg TP
Reg TP

registration
registrácia

registration authority
registračná autorita

relying party
strana spoliehajúca sa na elektronický podpis

replay
prehrávanie zo záznamu

repository
rezpozitórium

router
smerovač

RSA
RSA

S

S/MIME
S/MIME

secure mail
bezpečná pošta

secure system
bezpečný systém

security audit
bezpečnostný audit

self-signed certificate
samopodpísaný certifikát

SET
SET

SHA-1
SHA-1

SHA-1 algorithm
algoritmus SHA-1

smart card
šikovná karta

SSL
SSL

SSO
SSO

SSSO
SSSO

subscriber
subsribent

symmetric encryption
symetrické šifrovanie

T

3DES
3DES alebo trojitý DES

time stamp
časová pečiatka

triple DES
trojitý DES

trusted third party
dôveryhodná alebo dôverovaná tretia strana

tScheme
tScheme

U

UNCITRAL Model law on electronic signatures
Vzorový zákon o elektronickom podpise

UOOU
ÚOOÚ

V

virtual private network
virtuálna súkromná sieť

VPN
VPN

X

X.509
X.509

X.509 standard
norma X.509