STU

Vnútorný predpis
Číslo: 01/2016

Certifikačný poriadok IS STU Bratislava CA

Dátum: 01. 03. 2016

STU

Obsah

1. Úvod

Tento „Certifikačný poriadok IS STU Bratislava CA“ (ďalej len certifikačný poriadok) je určený osobám, ktoré využívajú certifikačné služby v rámci uzavretej infraštruktúry verejných kľúčov (ďalej len PKI) prevádzkovanej pre zamestnancov, študentov a iných externých spolupracovníkov Slovenskej technickej univerzity v Bratislave (ďalej len STU).

Tento certifikačný poriadok sa vzťahuje výlučne na certifikáty vydávané certifikačnou autoritou „IS STU Bratislava CA“ (certifikačná autorita informačného systému STU, ďalej len CA). Na žiadnu ďalšiu certifikačnú autoritu používanú na STU sa nevzťahuje.

CA zabezpečuje služby PKI predovšetkým pre potreby zvýšenia bezpečnosti Akademického informačného systému STU (ďalej len AIS) dvojfaktorovou autentifikáciou používateľov.

CA poskytuje certifikačné služby v rámci uzavretého systému v zmysle zákona č. 76/2009 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej len zákon o elektronickom podpise) podľa § 2 odsek 1 písm. j).

1.1 Prehľad

Tento certifikačný poriadok predstavuje vykonávaciu smernicu certifikačnej autority (Certification Practice Statement), a zároveň definuje certifikačnú politiku (Certificate Policy) pre certifikáty vydané CA.

CA poskytuje certifikačné služby v súlade s internými predpismi STU a medzinárodnými štandardmi, a to najmä s:

- Prevádzková bezpečnostná smernica informačného systému STU
- ITU-T X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

1.2 Identifikácia dokumentu

Tento dokument je voľne štruktúrovaný podľa Chokhani, et al, RFC3647. Kapitoly, ktoré nie sú pre túto CA podstatné, boli vynechané.

Názov: Certifikačný poriadok IS STU Bratislava CA
Verzia: 1.0, 01. 03. 2016

1.3 Účastníci PKI

1.3.1 Certifikačné autority

STU ustanovuje v rámci vnútornej PKI certifikačnú autoritu „IS STU Bratislava CA“ pre účely zabezpečovania služieb zaručenej identifikácie a overenia (autentifikácia a autorizácia) konkrétneho používateľa AIS.

Certifikačná autorita predstavuje časť PKI (pracovníci CA, hardvér, softvér, pracovné postupy a pravidlá), ktorá zabezpečuje vytváranie, podpisovanie a vydávanie digitálnych certifikátov, ich spravovanie, uloženie do bezpečného úložiska (čipovej karty), zneplatnenie a správu zoznamu zneplatnených certifikátov (Certification Revocation List, ďalej len CRL).

Poverenie na vykonávanie úloh CA vydáva písomne rektor alebo riaditeľ Centra výpočtovej techniky STU (ďalej len CVT). Na CVT v rámci Výpočtového strediska Vazovova-Mýtna (ďalej len VS V-M) musia byť úlohami CA poverení minimálne dvaja pracovníci. Pracovníci CA sú oprávnený vykonávať aj úlohy registračnej autority.

1.3.2 Registračné autority

Registračnú autoritu (ďalej len RA) v súvislosti s týmto certifikačným poriadkom predstavujú poverení zamestnanci STU. Poverenie na vykonávanie úloh RA vydáva písomne rektor alebo riaditeľ CVT.

Na každej fakulte STU musia byť úlohami RA poverení minimálne dvaja zamestnanci STU, z ktorých aspoň jeden musí byť pracovník fakulty v oblasti technickej podpory, správy počítačových systémov alebo sietí, alebo integrátor AIS.

Pracovníci RA sú zodpovední za manažment žiadostí týkajúcich sa vydania a zneplatnenia certifikátov, a za overenie identity žiadateľa.

Kontaktné pracoviská RA sú zriadené na každej fakulte STU primárne na oddeleniach zabezpečujúcich objednávanie, vydávanie a zrušenie študentských a zamestnaneckých preukazov (študijné a personálne oddelenia).
Kontaktné pracovisko RA s celouniverzitným pôsobením je zriadené vo VS V-M.

1.3.3 Držitelia certifikátov

Držiteľom certifikátu je fyzická osoba, ktorá je certifikátom identifikovaná. Až do úspešného overenia jej identity a prevzatia príslušného certifikátu je táto osoba označovaná ako žiadateľ o certifikát.

Držiteľom certifikátu môže byť len osoba s aktívnym právnym vzťahom s STU:

- zamestnanec STU,
- študent STU,
- externý spolupracovník na základe povolenia rektora alebo na základe iného zmluvného vzťahu, ktorého zmluvne vykonávaná činnosť vyžaduje zaručenú identifikáciu pri práci s AIS.

1.3.4 Strany spoliehajúce sa na certifikát

Certifikačné služby CA nevyužíva žiadna tretia strana.

1.3.5 Ostatní účastníci

Na správe PKI participuje zmluvne definovaná tretia strana, ktorá zabezpečuje vývoj a prevádzku AIS. Táto strana zodpovedá za inštaláciu, konfiguráciu a údržbu systémov CA, vytváranie a spravovanie administrátorských účtov, generovanie kryptografických kľúčov CA a zabezpečuje integráciu služieb CA do AIS.

1.4 Použitie certifikátov

Certifikáty vydané CA je možné používať výhradne na automatizovanú autentifikáciu ich držiteľov v AIS a v informačných systémoch CA.

Certifikáty vydané CA nesmú byť použité na preukazovanie príslušnosti osoby k STU tretím stranám, ďalej nesmú byť použité na potvrdzovanie akýchkoľvek finančných transakcii, ani na účely zaručeného elektronického podpisu a elektronického podpisu v zmysle zákona o elektronickom podpise. CA nie je registrovaná na Národnom bezpečnostnom úrade Slovenskej republiky a zákon o elektronickom podpise sa na jej prevádzku nevzťahuje.

Zakázané je akékoľvek iné použitie certifikátu CA, než to, ktoré je povolené týmto certifikačným poriadkom.

1.5 Kontaktné informácie

Slovenská technická univerzita v Bratislave
Centrum výpočtovej techniky
Vazovova 5
812 43 Bratislava
Slovenská republika

http://pki.stuba.sk

2. Povinnosti

2.1 Povinnosti CA

Povinnosťami CA sú:

- konať v súlade s týmto certifikačným poriadkom,
- zabezpečiť, aby RA boli preukázateľne oboznámené s certifikačným poriadkom a zaškolené v príslušných pracovných postupoch,
- zabezpečiť, aby v certifikátoch boli uvedené len správne a náležité údaje,
- automaticky zapisovať informáciu o zneplatnení certifikátu do CRL,

2.2 Povinnosti RA

Povinnosťami RA sú:

- konať v súlade s týmto certifikačným poriadkom,
- zadávať žiadosti o vydanie certifikátu do AIS prostredníctvom objednania príslušného typu preukazu – čipovej karty,
- overovať identity žiadateľov o certifikát na základe ich dokladu totožnosti,
- odovzdať čipovú kartu s certifikátom a obálku s PIN kódom len osobne a do vlastných rúk žiadateľa,
- po odovzdaní čipovej karty s certifikátom vyznačiť túto udalosť v AIS,
- nahlásiť CA neprevzatie obálky s PIN formulárom,
- nahlásiť CA akýkoľvek incident alebo mimoriadnu udalosť s certifikátom alebo čipovou kartou, ak o ňom má vedomosti,
- zneplatňovať certifikáty v súlade s týmto certifikačným poriadkom,
- odovzdať CA čipové karty, ktoré nemajú platný certifikát,
- poskytnúť držiteľovi certifikátu základné informácie k jeho používaniu, a v prípade problémov mu poskytnúť kontaktné informácie na vecne príslušné pracovisko technickej podpory.

2.3 Povinnosti držiteľa certifikátu

Držiteľ certifikátu je povinný:

- konať v súlade s týmto certifikačným poriadkom,
- chrániť certifikát a čipovú kartu pred stratou, ukradnutím, poškodením, modifikáciou, sprístupnením akejkoľvek osobe a neautorizovaným použitím,
- zachovávať kódy PIN a PUK v tajnosti, a to aj pred pracovníkmi CA a RA,
- okamžite nahlásiť RA podozrenie zo zneužitia, kompromitácie alebo straty certifikátu alebo čipovej karty, a zároveň požiadať o zneplatnenie certifikátu,

- skontrolovať a písomne potvrdiť prevzatie neporušenej obálky s kódmi PIN a PUK, čím zároveň potvrdí, že bol oboznámený s týmto certifikačným poriadkom,
- poškodenú alebo inak kompromitovanú obálku neprevziať,
- bezodkladne informovať RA o zmenách svojich osobných údajov,
- vrátiť čipovú kartu na kontaktnom pracovisku RA po skončení platnosti certifikátu na nej uloženom, s výnimkou držiteľov multifunkčných kariet s platnou licenciou ISIC a ITIC.

3. Poplatky

Základné služby CA sú pre zamestnancov a študentov STU bezplatné. Medzi základné služby patrí prvotné a následné vydanie certifikátu, zneplatnenie certifikátu, poskytnutie informácii o platnosti certifikátu, inštalácia obslužného softvéru, odblokovanie čipovej karty, vydanie prvej čipovej karty (bez licencie ISIC/ITIC), vydanie obálky s PIN a PUK kódmi.

CA pri prvom vydaní čipovej karty bezodplatne zapožičia čítačku kontaktných čipových kariet každému držiteľovi, ktorý je zamestnancom alebo študentom STU. Po skončení používania čipovej karty, ku ktorej bola poskytnutá čítačka, alebo po skončení právneho vzťahu držiteľa s STU, na základe ktorého mu bol vydaný certifikát, je držiteľ povinný čítačku vrátiť na kontaktnom pracovisku RA.

CA zverejní platný cenník svojich služieb prostredníctvom webovej stránky.

4. Identifikácia a autentizácia

4.1 Mená

Mená v certifikátoch CA pozostávajú z nasledovných častí:

Názov položky	Skratka názvu	Hodnota alebo jej popis
Štát	C	*SK*
Organizácia	O	*STU*
Organizačná jednotka	OU	*AIS*
Meno a priezvisko	CN	<meno a priezvisko> [<používateľské meno v AIS>] *Príklad: Adam Technický [technicky]*
Identifikátor	UID	<identifikačné číslo používateľa v AIS> *Príklad: 12345*

Jedinečnosť mien je zabezpečená zahrnutím používateľského mena v AIS do mena držiteľa certifikátu. Používateľské mená generuje AIS vždy jedinečné.

4.2 Overenie identity fyzickej osoby pri prvotnom vydaní certifikátu

Pre urýchlenie procesu vydávania certifikátov sa identifikačné údaje žiadateľa potrebné pre vydanie certifikátu získavajú z databázy AIS, preto je žiadateľ povinný udržiavať svoje osobné údaje evidované v AIS aktuálne. Identita žiadateľa sa overuje osobne na základe fyzického kontaktu medzi žiadateľom a pracovníkom RA, a to predložením občianskeho preukazu alebo pasu k nahliadnutiu. Overenie identity sa vykonáva za fyzickej prítomnosti žiadateľa, keď má pracovník RA k dispozícii vydanú čipovú kartu na meno žiadateľa a príslušnú obálku s kódmi PIN a PUK.

Žiadateľ je povinný osobne navštíviť pracovisko RA zriadené na fakulte, alebo vo VS V-M. RA môže vo výnimočnom prípade vyslať svojho pracovníka na detašované pracovisko fakulty alebo súčasti STU, na ktorom sa zdržiavajú viacerí žiadatelia o certifikát.

Žiadateľ môže byť v procese overenia identity a vydania certifikátu zastúpený inou fyzickou osobou, ktorá musí predložiť úradne overenú (notárom alebo na matrike) plnú moc, z textu ktorej je jednoznačne jasné, že splnomocnená osoba môže za žiadateľa konať v danej veci v jej mene. Splnomocnená osoba musí na kontaktnom pracovisku RA preukázať svoju totožnosť rovnakým spôsobom, aký platí pre žiadateľa. Ak si chce splnomocnená osoba ponechať originál plnej moci, musí RA poskytnúť jej kópiu (kópia nemusí byť úradne overená).

Pracovník RA na predloženom doklade totožnosti žiadateľa kontroluje:

- platnosť predloženého dokladu,
- zhodu medzi fotografiou v doklade a vzhľadom žiadateľa,
- zhodu mena, priezviska a dátumu narodenia na doklade s rovnakými údajmi na čipovej karte alebo v AIS,
- číslo dokladu, ktoré zapíše do overovacieho protokolu.

V prípade overovania splnomocnenej osoby pracovník RA kontroluje:

- platnosť, časové obmedzenie alebo iné podmienky plnej moci,
- potvrdenie o úradnom overení plnej moci (notárom alebo matrikou),
- rozsah plnej moci,
- zhodu mena, priezviska a dátumu narodenia splnomocňujúcej osoby s rovnakými údajmi na čipovej karte alebo v AIS,
- platnosť predloženého dokladu totožnosti splnomocnenej osoby,
- zhodu medzi fotografiou v doklade a vzhľadom splnomocnenej osoby,

- zhodu mena, priezviska a dátumu narodenia na doklade splnomocnenej osoby s rovnakými údajmi na plnej moci,
- číslo dokladu splnomocnenej osoby, ktoré zapíše do overovacieho protokolu,
- originál plnej moci, alebo jej kópia (pracovníkom RA skontrolovaná a uznaná za zhodnú s originálom) sa priloží k overovaciemu protokolu.

V prípade akýchkoľvek odôvodnených pochybností pri procese overenia identity je pracovník RA oprávnený odmietnuť vydať certifikát alebo prijať žiadosť. Dôvod odmietnutia zapíše do overovacieho protokolu. Žiadateľ môže po vykonaní nápravy požiadať RA o opätovné overenie jeho identity.

4.3 Overenie identity pri vydaní následného certifikátu pred skončením platnosti certifikátu

Overenie identity žiadateľa sa vykoná rovnakým spôsobom, ako pri prvotnom vydaní certifikátu.

4.4 Overenie identity pri vydaní následného certifikátu po zneplatnení certifikátu

Overenie identity žiadateľa sa vykoná rovnakým spôsobom, ako pri prvotnom vydaní certifikátu.

4.5 Overenie identity pri žiadosti o zneplatnenie certifikátu

Držiteľ certifikátu môže požiadať o zneplatnenie certifikátu osobne na kontaktnom pracovisku RA. Overenie identity žiadateľa sa vykoná rovnakým spôsobom, ako pri prvotnom vydaní certifikátu.

Držiteľ certifikátu môže požiadať o zneplatnenie certifikátu prostredníctvom príslušnej aplikácie v AIS po overení prihlasovacím menom a heslom.

Držiteľ certifikátu môže požiadať o zneplatnenie certifikátu prostredníctvom e-mailu pri splnení všetkých nasledovných podmienok:

- e-mail bude zaslaný z univerzitného poštového konta s doménou stuba.sk alebo is.stuba.sk,
- e-mailová adresa odosielateľa bude zodpovedať adrese evidovanej v používateľskom profile držiteľa certifikátu v AIS,
- e-mail bude zaslaný na príslušné pracovisko RA s kópiou na pracovisko CA,
- e-mail bude v tele správy obsahovať množinu identifikačných údajov postačujúcu na spoľahlivú identifikáciu držiteľa,

- pracovník RA úspešne overí žiadosť spätným zavolaním na telefónne číslo držiteľa evidované v informačných systémoch STU.

Žiadosť o zneplatnenie certifikátu nebude prijatá na základe telefonického volania iniciovaného držiteľom.

5. Životný cyklus certifikátu

5.1 Žiadosť o vydanie certifikátu

Vydanie certifikátu je podmienené potrebou používateľa využívať aplikácie AIS, ktoré sú chránené dvojfaktorovou autentifikáciou (ďalej len chránené aplikácie AIS). Používatelia, ktorí nebudú používať chránené aplikácie AIS, nemôžu žiadať o vydanie certifikátu. Chránené aplikácie AIS, okruh používateľov s povinnosťou vlastniť certifikát vydaný CA a harmonogram prechodu na dvojfaktorové overovanie definuje príslušná smernica rektora.

Žiadosť o vydanie certifikátu môže inicializovať žiadateľ, alebo pracovník RA, ak mu to prikazuje smernica rektora.

Žiadosť o vydanie certifikátu zadáva do AIS pracovník RA formou požiadavky na výrobu príslušného typu preukazu s kontaktným čipom a vytvorením objednávky na výrobu preukazu.

V prípade žiadosti o vydanie následného certifikátu nie je nutné objednávať nový preukaz, ak je držiteľov preukaz funkčný a platný. Následný certifikát sa uloží na pôvodnú čipovú kartu.

5.2 Vydanie certifikátu

Pracovník CA na základe objednávky výroby preukazov v AIS zabezpečí výrobu personifikovanej kontaktnej čipovej karty. V prípade výroby špeciálnych čipových kariet, ktoré nemožno objednať prostredníctvom AIS, postupuje CA podľa interných predpisov.

Certifikáty CA môžu byť uložené iba v zabezpečenom úložisku kontaktnej čipovej karty bez možnosti exportu súkromného kľúča certifikátu mimo prostredia karty.

Pracovník CA pri vydávaní certifikátu postupuje nasledovne:

1. Autentifikuje sa v softvéri CA vlastnou čipovou kartou.
2. V softvéri CA vyhľadá žiadateľa o certifikát a skontroluje správnosť a zhodu údajov v softvéri s údajmi na personifikovanej čipovej karte žiadateľa.
3. Žiadateľovu čipovú kartu vloží do čítačky a vykoná jej inicializáciu.

4. Softvér CA vygeneruje na čipovej karte súkromný a verejný kľúč, vytvorí certifikačnú požiadavku pre CA (z údajov z AIS a verejného kľúča) a odošle ju CA na podpis. Následne softvér prijme a uloží podpísaný certifikát a vygenerované kódy PIN a PUK na čipovú kartu. Kódy PIN a PUK sa vytlačia na PIN formulár do nepriehľadnej časti.
5. Inicializovanú čipovú kartu spolu s PIN formulárom vloží do samostatnej obálky a zalepí ju. Týmto krokom sa považuje certifikát za vytvorený.

(V ďalšom texte sa pre zjednodušenie môže pojmom „certifikát“ okrem samotného certifikátu označovať aj „obálka s inicializovanou čipovou kartou a PIN formulárom“.)

Pri vydávaní následného certifikátu je postup CA rovnaký, len sa pred inicializáciou čipovej karty vykoná jej formátovanie.

Po vytvorení certifikátu CA doručí certifikát na to pracovisko RA, ktoré je k žiadateľovi príslušné. Prípadná preprava certifikátu na iné pracovisko musí byť zabezpečená tak, aby nedošlo k poškodeniu ani k inej kompromitácii obálky.

5.3 Prevzatie a aktivácia certifikátu

RA po obdržaní certifikátu informuje žiadateľa a vyzve ho k jeho prevzatiu. Pred odovzdaním certifikátu žiadateľovi musí byť žiadateľova identita overená v zmysle bodu 4.2 tohto certifikačného poriadku.

Žiadateľ je povinný skontrolovať neporušenosť obálky s PIN formulárom a v prípade jej poškodenia prevzatie odmietnuť.

Po prevzatí certifikátu držiteľom je pracovník RA povinný príslušný preukaz s kontaktným čipom označiť v aplikácii AIS ako aktívny, čím bude certifikát vydaný a v systémoch AIS plne funkčný.

5.4 Používanie certifikátu

5.4.1 Práva a povinnosti držiteľa pri používaní certifikátu

Držiteľ môže používať certifikát pre účely preukázania svojej identity v informačných systémoch CA a v AIS. Certifikát sa nesmie použiť na iné účely, než povoľuje tento certifikačný poriadok. Smernicou rektora sa stanoví, ktoré aplikácie AIS budú vyžadovať použitie certifikátu CA (ďalej len chránené aplikácie).

Držiteľ pri prístupe do chránenej aplikácie vloží čipovú kartu do čítačky, zvolí certifikát CA a zadá zodpovedajúci PIN kód. Čipovú kartu ponecháva v čítačke počas celej doby práce v chránenej aplikácii.

Po skončení práce s aplikáciou vyžadujúcou použitie certifikátu je držiteľ povinný čipovú kartu vysunúť z čítačky a uchovávať ju bezpečne pri sebe, mimo dosahu tretích osôb.

Držiteľ môže pristupovať k chráneným aplikáciám z ľubovoľného počítača, ktorý je adekvátnym spôsobom zabezpečený (aktualizovaný operačný systém, aktualizovaný antivírusový softvér a iné opatrenia IT bezpečnosti požadované chránenými aplikáciami). Môže pritom použiť ľubovoľnú čítačku kontaktných kariet spĺňajúcu štandard ISO 7816.

Držiteľ nesmie vedome dopustiť, aby jeho čipovú kartu použila iná osoba. Porušenie tohto ustanovenia je hrubým porušením pravidiel certifikačného poriadku, za ktoré sa vyvodia príslušné dôsledky uvedené v smernici rektora.

Použitie čipovej karty treťou osobou, s vedomím držiteľa alebo bez jeho vedomia, je rovnako hrubým porušením pravidiel certifikačného poriadku, za ktoré sa pre tretiu osobu vyvodia príslušné dôsledky uvedené v smernici rektora.

5.4.2 Kódy PIN a PUK

Držiteľ musí chrániť PIN a PUK kódy pred prezradením a pravidelnou zmenou PIN kódu chrániť certifikát pred zneužitím. Kódy PIN a PUK nesmú byť uchovávané v dosahu tretej osoby, ani spolu s čipovou kartou, s čítačkou alebo s počítačom.

PIN kód je držiteľ povinný zmeniť pri prvom použití certifikátu a následne minimálne každých 6 mesiacov. CA zverejní na svojich internetových stránkach softvér na zmenu PIN kódu a návod na jeho použitie. Kód PUK, ktorý slúži na odblokovanie a zmenu PIN kódu, nie je možné zmeniť.

Ak držiteľ zabudne PUK kód, je povinný požiadať RA o zneplatnenie certifikátu. Identita žiadateľa o zneplatnenie certifikátu musí byť overená podľa bodu 4.5 tohto certifikačného poriadku.

5.4.3 Strata, odcudzenie čipovej karty alebo kompromitácia certifikátu

V prípade straty, odcudzenia čipovej karty alebo pri inej kompromitácii certifikátu, napríklad pri podozrení, že s certifikátom mohla nakladať iná osoba, je držiteľ certifikátu povinný bezodkladne požiadať RA o zneplatnenie certifikátu. Identita žiadateľa o zneplatnenie certifikátu musí byť overená podľa bodu 4.5 tohto certifikačného poriadku.

Nálezca čipovej karty vydanej na STU ju môže odovzdať na ktoromkoľvek pracovisku RA, alebo na kontaktnej adrese CA uvedenej v bode 1.5.

5.5 Expirácia a zneplatnenie certifikátu

Prekročením doby platnosti certifikátu sa certifikát nenávratne zneplatní. Platnosť certifikátov CA je stanovená na 3 roky od dátumu ich vydania.

Zneplatnenie certifikátu vykonáva pracovisko RA. O zneplatnenie certifikátu môže požiadať jeho držiteľ. Pre prijatie žiadosti musí byť jeho identita overená podľa bodu 4.5 tohto certifikačného poriadku. V prípadoch stanovených smernicou rektora môže požiadať o zneplatnenie certifikátu aj priamo pracovník CA a RA. V takom prípade sa postupuje podľa interných predpisov.

Po zneplatnení certifikátu bude používateľovi AIS znemožnené pristupovať do chránených aplikácii. V smernici rektora môžu byť ustanovené podmienky dočasného pristupovania do chránených aplikácii bez použitia certifikátu.

5.5.1 Dôvody na zneplatnenie certifikátu

Zneplatnenie certifikátu sa vykoná v nasledujúcich prípadoch:

- vydanie následného certifikátu,
- nahlásená strata alebo krádež certifikátu alebo čipovej karty,
- nález čipovej karty treťou osobou,
- neaktuálnosť údajov v certifikáte,
- zánik právneho vzťahu, na základe ktorého bol certifikát vydaný,
- nepotrebnosť certifikátu,
- podozrenie zo zdieľania, zneužitia alebo inej kompromitácie certifikátu,
- porušenie tohto certifikačného poriadku,
- nefunkčnosť alebo chybná funkčnosť certifikátu alebo čipovej karty,
- iný dôvod, pre ktorý držiteľ požiada o zneplatnenie certifikátu,
- iné odôvodnené prípady.

CA si vyhradzuje právo na zneplatnenie ľubovoľného certifikátu bez udania dôvodu na základe pokynu rektora alebo riaditeľa CVT.

5.5.2 Čas na zneplatnenie certifikátu a zodpovednosť za škodu

CA zneplatní certifikát zverejnením na zozname CRL tak rýchlo ako jej to prevádzkové podmienky umožnia po tom, čo budú splnené podmienky certifikačného poriadku na zneplatnenie certifikátu. Do doby zverejnenia certifikátu v CRL nesie všetku zodpovednosť za prípadné škody spôsobené zneužitím certifikátu jeho držiteľ. Po zverejnení certifikátu v CRL prechádza

zodpovednosť za prípadné škody spôsobené zneužitím certifikátu na tú stranu, ktorá sa na zneplatnený certifikát spoľahla. STU ani CA finančne neručí za škody spôsobené používaním certifikátov, ktoré vydala CA.

V Bratislave dňa 22.02.2016

Prof. Ing. Pavol Horváth, PhD.
Riaditeľ CVT STU