Závěrečná zpráva

Číslo projektu:	380R1/2010
Název projektu:	Zavedení PKI s bezpečnými nosiči osobních elektronických certifikátů
Pracoviště:	Informační centrum, Univerzita Pardubice
Řešitel:	Ing. Lukáš Slánský
Spoluřešitelé:	Ing. Jiří Slanina Ing. et Bc. Ondřej Prusek, Ph.D. Ing. Luboš Kopecký

1 Výchozí stav

Na Univerzitě Pardubice nebyla začátkem roku 2011 zavedena žádná politika používání technologie PKI[1]. Jako úložiště osobních certifikátů[2] bylo ve většině případů používáno systémové úložiště certifikátů operačního systému Windows. V malé míře byly certifikáty uloženy na šifrovacích tokenech.

1.1 Využívané certifikáty

Pro provozní činnost univerzity bylo a v současné době je i nadále využíváno několika typů osobních certifikátů s různým typem užití, důvěryhodností atd. Certifikáty neuvedené níže nejsou a ani nemohou být žádným způsobem evidovány ani kontrolovány, jejich využití je zcela v kompetenci jejich uživatelů.

1.1.1 Kvalifikované certifikáty

Ve smyslu zákona č. 227/2000 Sb. o elektronickém podpisu jsou certifikáty vydávané CA PostSignum užívány pro komunikaci s orgány veřejné správy. Certifikáty jsou oprávněni užívat pouze zaměstnanci mající pověření komunikovat jménem univerzity.

1.1.2 Certifikáty Cesnet CA

Certifikáty Cesnet CA byly do konce 7. 11. 2010 vydávány ověřeným zaměstnancům univerzity. Jejich použití bylo pro ověření komunikace se zaměstnanci CESNETu a jiných univerzit. Vzhledem k roční expirační době certifikátů jsou již v současné době všechny certifikáty neplatné.

1.1.3 Certifikáty Cesnet CA3

Cesnet CA3 je částečným nahrazením Cesnet CA. Využití certifikátů této CA je však pouze pro komunikaci týkající se správy služby Shibboleth. Z tohoto důvodu je také omezeno vydávání tohoto typu certifikátu na správce této služby na univerzitě.

1.1.4 Certifikáty TERENA Certification Service – Personal

Certifikáty TCS-P jsou nahrazením Cesnet CA pro většinu uživatelů (zaměstnanců i studentů) Univerzity Pardubice. Certifikační cesta tohoto typu certifikátů končí u CA *AddTrust External CA Root*, což je certifikát ComodoCA, který je důvěryhodnou autoritou pro většinu e-mailových klientů i webových prohlížečů. Tato důvěra a všeobecná dostupnost předurčuje tento typ certifikátů pro všeobecné zabezpečení elektronické komunikace – podpisy e-mailových zpráv, jejich šifrování či šifrování obecných souborů pro ochranu v nezabezpečeném prostředí.

1.2 Správa platnosti certifikátů z autority univerzity

Certifikáty nebyly systematicky spravovány, případné odvolání platnosti zejména z důvodu ukončení vztahu s univerzitou nebylo spolehlivým způsobem řešeno.

2 Analýza možnosti využití PKI

Pro objektivní zhodnocení možností využití technologie PKI na půdě univerzity jsme zanalyzovali procesy, při kterých k použití i jen potenciálně dochází a role uživatelů procesu. Přínosy a rizika použití technologií a z nich vyplývající doporučení následují dále.

[1] Infrastruktura využívající technologii šifrování s využitím veřejných klíčů – Private Key Infrastructure.
[2] Z pohledu oprávněného vlastníka bude pro jednoduchost psaného textu nadále využíváno spojení „certifikát“ pro soukromý klíč a k němu příslušející veřejný klíč ve formě certifikátu podepsaného příslušnou certifikační autoritou (CA). Z pohledu ostatních subjektů je „certifikát“ pouze veřejný klíč podepsaný příslušnou CA.

Z hlediska možných následků procesů, resp. následků plynoucích z kompromitace soukromého klíče, je možné seřadit role[3] následovně:

1. Uživatel univerzity komunikující s veřejnou správou,
2. správce služby Shibboleth,
3. zaměstnanec univerzity a
4. student univerzity.

2.1 Uživatelé komunikující s veřejnou správou

Specifikace procesu: Uživatelé, kteří komunikují s veřejnou správou, používají z pohledu zákona č. 227/2000 Sb. o elektronických komunikacích svůj kvalifikovaný elektronický podpis ke stejným účelům jako podpis fyzický. Jedná se zejména o elektronické podepisování e-mailových zpráv a dokumentů určených státním orgánům. Použití kvalifikovaného podpisu je v některých případech povinné a nelze se mu vyhnout. Z identifikovaných procesů jsou nejdůležitější:

- komunikace s ČSSZ,
- emailová komunikace Oddělení zadávacích řízení pro zveřejňování veřejných zakázek a komunikaci s uchazeči,
- komunikace s Finačním úřadem,
- komunikace s CA PostSignum týkající se vydávání kvalifikovaných certifikátů a
- podepisování specifických dokumentů, které vyžadují elektronický podpis rektora či prorektorů.

Specifikace skupiny: Uživatelů s oprávněním komunikovat s veřejnou správou jsou na univerzitě jednotky (v současnosti je vydáno celkem 14 certifikátů), jedná se o uživatele s širokou škálou povědomí o elektronické bezpečnosti – od laiků po IT profesionály. Použití komunikačního procesu je relativně výjimečné.

Proces vydání certifikátu: Certifikáty jsou vydávány na základě ověřené žádosti vydané univerzitou pro konkrétního člověka, žádost je certifikační autoritou zpracována a certifikát je vydán pouze oprávněnému uživateli po důkladném ověření jeho identity na příslušném pracovišti certifikační autority.

2.2 Správci služby Shibboleth

Specifikace procesu: Služby Shibboleth je klíčovou pro proces vydávání certifikátů TCS-P. Správci, kteří mají tuto službu na starosti, jsou v rámci federace eduID.cz oprávněni komunikovat s odpovědnými pracovníky CESNETu a vystupovat jménem univerzity. Využití je zejména při podepisování a šifrování e-mailové komunikace a to pouze s ostatními správci Shibbolethu.

Specifikace skupiny: Správců služby Shibboleth je velmi málo (v současnosti dva), jejich kompetence v oboru IT a elektronické bezpečnosti je vysoká. Komunikace probíhá pouze výjimečně. Správci Shibbolethu jsou oprávněni svým elektronickým podpisem autorizovat požadavky směřující na správce služby Shibboleth na úrovni CESNETu.

Proces vydání certifikátu: Certifikáty CESNET CA3 jsou vydávány na základě pověření vydaného univerzitou po ověření identity na pracovišti registrační autority CESNETu.

2.3 Zaměstnanci univerzity

Specifikace procesu: Zaměstnanci univerzity mohou potenciálně využívat elektronický podpis zejména pro podepisování e-mailové komunikace, její šifrování, podepisování (a šifrování) elektronických dokumentů, různých žádanek/formulářů apod.

[3] Jeden uživatel může vystupovat ve více rolích, přičemž každý proces je podmíněn jednou rolí.

Specifikace skupiny: Zaměstnanců pracuje na univerzitě přibližně 1 200, jejich kompetence v elektronické bezpečnosti kolísá od naprostých laiků po profesionály. Potenciál využití technologie elektronického podpisu kolísá v závislosti na osobním zaměření uživatele od denního využití („podepisuji každý e-mail“) po použití nulové.

Proces vydání certifikátu: Certifikáty TCS-P jsou vydávány na základě elektronické žádosti, která je autorizována službou Shibboleth v rámci federace eduID.cz. Pro přihlášení ke službě je nutné použít osobní autentizační údaje, jejichž přidělení probíhá po ověření identity zaměstnance osobním oddělením univerzity.

2.4 Studenti univerzity

Specifikace procesu: Studenti univerzity mohou potenciálně využívat elektronický podpis zejména pro podepisování (a šifrování) e-mailové komunikace, dokumentů (např. odevzdávané práce) či žádostí na orgány fakulty.

Specifikace skupiny: Na univerzitě studuje řádově 10 000 studentů, znalost elektronické bezpečnosti kolísá od nulové po velmi vysokou, v některých případech s až paranoidními prvky. Potenciál využití technologie elektronického podpisu kolísá obdobně jako u zaměstnanců – od nulové po velmi vysoký.

Proces vydání certifikátu: Proces vydání certifikátu je shodný s procesem zaměstnaneckým – s výjimkou ověření identity pracovníky studijních oddělení fakult.

3 Přínosy a rizika použití technologií

Každá z technologií uložení soukromého klíče má pozitivní i negativní konsekvence, které je třeba zvážit při jejich nasazení do prostředí instituce. Ke zvážení není pouze stránka čistě technologická, bezpečnostní a finanční, ale v neposlední řadě také stránka uživatelské přívětivosti s ohledem na cílovou skupinu uživatelů.

3.1 Uložení v souboru

Soukromý klíč uložený v souboru je nejčastěji uložený ve formátu specifikovaném standardem PKCS #12. Uložená data jsou zabezpečena šifrováním založeným na hesle. Toto heslo nepodléhá žádným vynuceným politikám pro tvorbu hesla, což může znamenat volbu hesla s malou sílou, na které je možné s úspěchem použít slovníkové útoky či útoky hrubou silou.

Použití uložení soukromého klíče v souboru je rizikem, které lze omezit správným a poučeným použitím. Jediné smysluplné využití je pro přenos mezi ostatními typy úložišť – samozřejmě zabezpečené silným heslem, které by mělo být jednorázově použito pouze pro dané úložiště.

Druhou možností uložení soukromého klíče a certifikátu je v souboru ve formátu DER[4], ve kterém jsou údaje uloženy v otevřeném stavu a tím velmi náchylné ke kompromitaci. Použití tohoto typu úložiště je **extrémním rizikem**, možnosti využití jsou prakticky nulové.

3.2 Úložiště operačního systému Windows

Systémy Windows NT 4.0 a vyšší (včetně XP, Vista, 7) obsahují integrované CryptoAPI, které zajišťuje operace potřebné pro napojení na PKI. V nejjednodušší podobě jsou klíče a certifikáty uloženy v úložišti *Microsoft Software Key Storage Provider*, které poskytuje dobrou ochranu uložených údajů a je certifikováno dle FIPS 140. Přístup k šifrovacím klíčům je chráněn silným navázáním na jádro systému a šifrováním založeným na ověření identity uživatele, který použití CryptoAPI požaduje.

[4] Distinguished Encoding Rules – forma kódování údajů dle specifikace X.690, používá se zejména pro přenos šifrovacích entit.

Klíčovým prvkem ochrany je zabezpečení přístupu k uživatelskému účtu na počítači. Politika tvorby hesla, jeho expirace a volby nových hesel je vynuceno pravidly uživatelských kont na úrovni správy účtů v Active Directory.

Vzhledem k tomu, že Windows jsou využívány na naprosté většině[5] počítačů zaměstnanců i studentů, je penetrace tohoto typu úložiště velmi vysoká. Tento fakt je umocněn integrací použití do klíčových aplikací Microsoftu, které jsou na Univerzitě Pardubice primárně užívány ke kancelářské práci – balík MS Office a prohlížeč Internet Explorer.

U pracovních počítačů zaměstnanců je politikami zabezpečena dobrá ochrana před neoprávněným přístupem k uživatelskému účtu na počítači. Studentské počítače a domácí počítače zaměstnanců pravděpodobně systematicky spravovanou politiku hesel nemají, a může tak dojít ke kompromitaci šifrovacích aktiv i při pouhém fyzickém přístupu k počítači.

3.3 Šifrovací tokeny

Nejvyšší současnou úroveň zabezpečení osobních certifikátů je možné dosáhnout využitím šifrovacích tokenů – ať už ve formě SmartCard nebo USB tokenu. Tokeny jsou svým návrhem koncipovány tak, aby z nich nebylo možné soukromé klíče exportovat, a jsou-li certifikovány dle FIPS 140-2 Level 2 (či vyšší), je zaručeno i jednoznačné odhalení pokusu o neoprávněný fyzický přístup k šifrovacímu čipu v tokenu integrovanému, případně (pro vyšší levely) i zabezpečení zničení údajů při pokusu o fyzicky, softwarově či jinak vedený průnik. Použití soukromého klíče je podmíněno znalostí příslušného hesla.

Tokeny jsou vhodné pro uložení zejména klíčových certifikátů, které jsou schopny velmi dobře ochránit, bezpečnost a vícefaktorová[6] ochrana údajů je vykoupena nižší uživatelskou přívětivostí, nutností přenášet další „krabičku“ a potřebou doručit čtecí infrastrukturu (čtečky, ovladače do OS, servisní software) na všechna místa, kde budou tokeny využívány.

3.4 Ostatní metody uložení certifikátů

Pro uložení certifikátů je možné využít i další metody – například úložiště ve webových prohlížečích či jiných aplikačních programech nebo využití technologií mobilních telefonů ať už ve formě využití SIM karty jako standardní SmartCard či potenciálu technologie NFC.

4 Realizované řešení

Po zvážení technických, uživatelských a relevantních legislativních informací jsme zvolili řešení zahrnující pouze minimalistickou variantu nasazení technologie PKI na Univerzitě Pardubice.

Důvodem pro volbu řešení byly především vnější okolnosti dané stavem externích projektů, např. projekt e-governmentu ve státní správě (datové schránky apod). Jejich podoba často nevyžaduje (nebo přímo neumožňuje) využívání elektronických certifikátů, podepisování dokumentů kvalifikovaným nebo jiným podpisem. Tím byl zpochybněn smysl plošného zavedení PKI založeného na šifrovacích tokenech a kvalifikovaných certifikátech na Univerzitě Pardubice.

Hlavním důvodem vzniku projektu byla očekávání využívání důvěryhodně elektronicky podepisované komunikace především s poskytovateli dotací, resp. tvorby dokumentace s náležitými podpisy a časovými razítky.

V době podávání projektu se pro podepisovanou elektronickou komunikaci jako nejpravděpodobnější jevily projekty strukturálních fondů, především OP VK a OP VaVpI. Tyto projekty dle *Příruček pro příjemce* mají povinnost archivace, kromě jiných dokumentů, také plné korespondence s řídicím

[5] Dle statistik přístupů k webovým stránkám odhadujeme zastoupení Windows u studentů na více než 97 %, u zaměstnanců na 99 %. Do tohoto počtu jsou započítány i mobilní telefony a další přenosná zařízení.
[6] Něco mám (token) a něco vím (heslo).

orgánem operačního programu (ŘO OP), která ze strany MŠMT probíhá pouze prostými nepodepsanými e-maily s nepodepsanými přílohami různých formátů. Snaha podepisovat dokumenty ze strany UPa pro komunikaci s MŠMT byla zamítnuta ze strany ŘO OP, instituce požaduje nepodepsané soubory, nejčastěji ve formátech kancelářských programů Word a Excel.

Tyto důvody vedly management UPa k rozhodnutí, že nemalé následné investice do finálního zavedení a následného udržování PKI na UPa nejsou v současnosti smysluplné.

Minimalistická varianta níže popsána specifikuje potřeby pouze určitých skupin uživatelů, kteří pro vybranou komunikaci potřebují nebo chtějí nějaké typu certifikátů využívat.

4.1 Kvalifikované certifikáty

Kvalifikované elektronické certifikáty jako důležitý prostředek identifikující zástupce univerzity a fakulty je třeba chránit v maximálním možném rozsahu. Pro jejich použití je **důrazně doporučeno uchovávání na USB tokenech** po celý životní cyklus – od generování páru klíčů po vypršení či odvolání jejich platnosti.

Není-li uložení na tokenu možné, je nutné soukromý klíč chránit jeho uložením v úložišti ve formě, kdy jej nelze z úložiště *Microsoft Software Key Storage Provider* exportovat a silným heslem odlišným od přístupového hesla k uživatelskému účtu[7].

Využití kvalifikovaných certifikátů zůstává ve shodném rozsahu jako před počátkem projektu (blíže viz kap. 2.1) a je řízeno Zákonem č. 227/2000 Sb. o elektronickém podpisu.

4.2 CESNET CA3 certifikáty

Certifikáty autority CESNET CA3 umožňují identifikaci správců služby Shibboleth, respektive služby vydávání osobních certifikátů TCS-P. Pro jejich uložení je **doporučeno obdobné zacházení jako s kvalifikovanými certifikáty**.

Použití certifikátů je omezeno pouze na komunikaci mezi správci služby Shibboleth v rámci CESNETu a ostatních členů federace eduID.cz

4.3 Zaměstnanecké certifikáty

Pro certifikáty je vzhledem k jednoduchosti použití a dostatečnému zabezpečení **doporučené úložiště systému Windows** *Microsoft Software Key Storage Provider* ve standardní konfiguraci. Vyšší stupeň zabezpečení, ať už přísnějším použití Windows úložiště nebo za použití šifrovacích tokenů není vyloučené, není však přímo podporováno Informačním centrem.

Použití certifikátů je zejména pro podepisování a šifrování e-mailové komunikace a dokumentů zejména v komunikaci mezi zaměstnanci a studenty v akademickém prostředí.

4.4 Studentské certifikáty

Certifikáty studentů jsou nejméně významné, co se týká možného dopadu v případě kompromitace. Metoda uložení certifikátu není žádným způsobem regulována, velmi záleží na používaném programovém vybavení používaném studenty.

Použití certifikátu je zejména pro podepisování a šifrování e-mailové komunikace a dokumentů mezi studentem a učitelem, případně studentem a fakultou.

[7] Tuto ochranu lze docílit exportem certifikátu spolu se soukromým klíčem do formátu PKCS #12 a jeho opětovným importem s volbou politiky „neexportovatelný soukromý klíč“ a „silná ochrana privátního klíče“.

4.5 Legislativa a dokumentace

Ve smyslu výše uvedených bodů bylo vypracováno *Doporučení pro bezpečné nakládání s osobními certifikáty*. Pro procesy vydávání certifikátů, použití certifikátu a případy kompromitace soukromého klíče byla připravena sada uživatelských návodů, které popisují procesy pro jednotlivé typy certifikátů.

Návody pro použití byly vytvořeny pro nejčastěji používané kombinace operačních systémů, kancelářských balíků, e-mailových klientů a webových prohlížečů.

Výše uvedené dokumenty jsou zveřejněny na webových stránkách Univerzity Pardubice na adrese http://www.upce.cz/zazemi/ic/certifikaty.html.

5 Tisková zpráva

Univerzita Pardubice (www.upce.cz) zpřístupnila svým uživatelům vydávání osobních elektronických certifikátů, které mohou sloužit pro podepisování pracovní i studentské e-mailové komunikace či jiných elektronických dokumentů.

Pro práci s elektronickými podpisy byla vytvořena doporučení pro bezpečnou práci a přehledné návody, které uvedou uživatele do bezpečnosti zacházení s elektronickými podpisy a jejich užití v nejrozšířenějších aplikacích.