Certifikační infrastruktury veřejných klíčů, PKI

Petr Hanáček[1], Jan Staudek[2]

Abstrakt. Tutoriál se věnuje technickým i netechnickým problémům zavádění a provozování infrastruktur PKI (Public Key Infrastructure). Výklad je zaměřen na architektury PKI, na vlastnosti a služby na rozhraní jejich komponent, na vnitřní technické procesy PKI a na vázání těchto procesů na systém odpovídajících dokumentů, tj. na certifikační politiku a na certifikační prováděcí směrnici. Základním cílem PKI je podpora služeb pro digitální identifikaci. Pro PKI jsou charakteristické vlastnosti: maximálně možné využití standardů, podpora nezávislosti na konkrétních produktech a aplikacích, podpora více mechanismů digitálních podpisů, výměn klíčů a šifrování, podpora funkční separace klíčů, podpora obnovy klíčů a dat, podpora nepopiratelnosti z právního hlediska a z komerčního hlediska tak, aby bylo možné počítat v budoucnosti s případným outsourcingem prvků PKI. Popisované PKI jsou ukázány jak v rovinách potřeb krátkodobé, tak i v rovinách potřeb dlouhodobé interoperability.

Klíčová slova: infrastruktura veřejných klíčů, PKI, služby PKI, autorita, certifikát, certifikace, správa klíčů, správa certifikátů, revokace certifikátu, certifikační politika, certifikační prováděcí směrnice, modely důvěry, provoz PKI.

Text je psán pro čtenáře, od kterého se očekává základní znalost principů bezpečnosti např. v rozsahu publikace [4]. Je vhodné, aby alespoň rámcově znal filozofii a základní principy (asymetrické) kryptografie, digitálního podpisování, odpovídající správy klíčů, bezpečnostních funkcí pro autentizaci, zajištění integrity, zajištění důvěrnosti a kryptografických mechanismů použitelných pro jejich implementaci.

Asymetrická kryptografie, ASK (také *kryptografie s veřejným klíčem*) se stává základní bezpečnostní technologií většiny aplikací IT provozovaných v otevřených sdílených sítích s nedefinovanou úrovní bezpečnosti a požadujících zajištění autentizace a bezpečnosti. Účinné používání ASK požaduje pro důvěryhodné zveřejňování veřejných klíčů a pro jejich správu dostupnost vhodné podpůrné infrastruktury. Je zvykem tuto infrastrukturu nazývat *PKI – Public Key Infrastructure*. Asymetrická kryptografie je bez účinně a výkonně fungující PKI jen marginálně užitečnější než tradiční symetrická kryptografie (kryptografie s tajným klíčem). Autentizace a uplatňování autorizace mezi předem neznámými partnery jsou bez PKI v podstatě neřešitelné.

[1] Ústav informatiky a výpočetní techniky, FEI VUT Brno, Božetěchova 2, 612 66 Brno, hanacek@dcse.fee.vutbr.cz
[2] Katedra programových systémů a komunikací, FI MU Brno, Botanická 68a, 602 00 Brno, staudek@fi.muni.cz

Obsah

1 Úvod do certifikačních infrastruktur veřejných klíčů

Dříve než se budeme věnovat systematičtějšímu rozboru certifikačních infrastruktur veřejných klíčů, *Public Key Infrastructures*, *PKI*, které vesměs podporují používání aplikací IT, které zajišťují důvěrnost dat šifrováním a používají pro podporu bezpečnostních služeb autentizace a nepopiratelnosti digitální (elektronické) podpisy, uvádíme v několika odstavcích přehledový popis PKI a jejich použitelnosti.

PKI jsou založeny na principech vycházejících z idejí asymetrické kryptografie, *ASK*. Asymetrická kryptografie šifruje data pomocí dvou matematicky vázaných klíčů, parametrů kryptografických algoritmů. Jeden klíč je uchováván jako soukromý, důvěrný, druhý je veřejný. Soukromý klíč nelze odvodit ze znalosti veřejného klíče. Jedinec, který chce poslat důvěrnou zprávu příjemci, šifruje její text veřejným klíčem příjemce. Příjemce šifrovanou zprávu dešifruje svým soukromým klíčem. Odesílatel si je tudíž jistý, že zprávu může číst pouze její příjemce.

ASK lze rovněž použít pro digitální podpisování. Digitální podpis zprávy se vytváří tak, že se nejprve vhodnou (hašovací) matematickou funkcí získá hodnota jednoznačně závislá na obsahu zprávy obvykle o délce nejvýše několika málo stovek bitů (*haš*) a tato hodnota se posléze šifruje soukromým klíčem podepisující osoby a připojuje se k původní zprávě. Příjemce podepsané zprávy může podpis ověřit jeho dešifrováním veřejným klíčem podepisující osoby. Příjemce si vypracuje analogickým způsobem jako podepisující osoba stejnou (hašovací) matematickou funkcí hodnotu jednoznačně závislou na obsahu zprávy, *haš*. Pokud se příjemcem jsou dešifrovaná hodnota *haš* a vypočtená hodnota *haš* identické, příjemce si jistý jak autenticitou podepisující osoby tak i integritou podepsané zprávy (tj. tím, že podepsaná zpráva nebyla po podepsání změněna). Poněvadž digitální podpis zprávy závisí na hodnotě soukromého klíče podepisující osoby, je při vhodném zabezpečení důvěryhodnosti znalosti vztahu párových podpisových dat (klíčů) a podepisující osoby podporující infrastrukturou PKI omezena možnost popření pravosti podpisu zprávy.

Základní stavební kámen infrastruktury zajišťující důvěryhodnost vztahu jedince a jeho veřejného klíče (ať již šifrovacího klíče nebo klíče pro ověření podpisu) je *certifikační autorita*, *CA*. Certifikační autorita je důvěryhodná třetí strana, jejíž důvěryhodnost umožňuje důvěřovat vztahu páru klíčů ASK a konkrétní identifikovatelné osoby. Typicky musí být schopná důvěryhodně identifikovat osoby držící ve vlastnictví příslušný pár klíčů ASK, může hodnoty takových klíčů i generovat, musí být schopná veřejně deklarovat platnost vztahu mezi osobou a párem klíčů držených touto osobou a musí být schopna odvolávat platnost vztahu mezi osobou a párem klíčů držených touto osobou. Pro mnohé aplikace musí CA umožnit, aby si párové hodnoty klíčů zúčastněné osoby generovaly samy. CA vydávají elektronické (jimi podepsané) dokumenty, které platnost vztahu osoby a jejího veřejného klíče důvěryhodně potvrzují – *digitální certifikáty*. Potvrzení vlastnictví veřejného klíče danou osobou současně potvrzuje, že tato osoba vlastní odpovídající soukromý klíč. Certifikáty jsou vydávány obvykle ve třech úrovních záruky za důvěryhodnost: nízká, střední a vysoká záruka. Vyšší úroveň poskytované záruky vyjadřuje skutečnost, že CA věnuje větší úsilí při potvrzování identity osob a při zajišťování své bezpečnosti. Propojením dvou a více CA možností se vzájemně certifikovat, vzniká certifikační infrastruktura veřejných klíčů. Jejím hlavním přínosem je, že umožňuje provozovat komunikační a byznys procesy i mezi stranami, které se předem neznají, pokud CA zúčastněných stran lze nějakým způsobem začlenit do společné PKI.

Pravidla, která deklarují použitelnost certifikátů vydávaných danou CA v rámci jisté komunity a/nebo třídy aplikací IT se společnými shodnými požadavky na bezpečnost, definuji *Certifikační politiku* CA., *CP*. Daná CA může uplatňovat více CP, a to jak pro oblast šifrování, tak i pro oblast podpisování zpráv. Certifikační politika je dokumenty – základní

stavební kámen pro budování důvěryhodnosti certifikátů veřejných klíčů. Je technologickou bází pro vzájemnou certifikaci více CA vytvářejících společnou PKI. CP vymezuje důkladnost prověřování autenticity žadatele o vydání certifikátu. Popis toho, jak jsou pravidla dané CP implementována, vyjadřuje další dokument z *dokumentové základny* CA – *Certifikační prováděcí směrnice*, *CPS*. CA může danou CPS podporovat více CP. CA s různými CPS mohou podporovat identické CP. CP stanovuje záruku, se kterou lze důvěřovat certifikátu, CPS dané CA stanovuje, jak tato CA takové záruky dosahuje.

1.1 Cíle a funkce PKI

PKI vytváří provozní prostředí, které v síťovém prostředí s nezaručenou bezpečností podporuje bezpečnost komunikačních a aplikačních transakcí. PKI je částí celkové *bezpečnostní infrastruktury sítě*, do níž integruje dvě základní služby:

1. *používání digitálních certifikátů* jejich držiteli a uživateli
2. *vydávání digitálních certifikátů* certifikačními autoritami.

Digitální certifikát je elektronický dokument, který spolehlivě asociuje identifikaci držitele certifikátu s nějakou jeho vlastností, požadovanou např. bezpečnostními službami implementovanými mechanismy ASK (hodnota ověřovacího nebo šifrovacího klíče) nebo bezpečnostními službami řídícími přístup ke zdrojům s omezenou dostupností (přístupové právo, klasifikace). Digitální certifikáty různých PKI se liší jak formátem, tak i obsahem použitelností; mnohdy velmi podstatně. (Digitální certifikát není totéž co digitální podpis, digitální podpis není digitální certifikát! Pouhým předložením digitálního certifikátu ověřovacího klíče se Alice neautentizuje, pro úspěšnou autentizace musí být schopna se platným způsobem digitálně podepsat. Samotný digitální podpis bez certifikátu není dostatečně důvěryhodný.)

PKI budovaná jako část celkové bezpečnostní architektury je velmi často určená pro správu klíčů a certifikátů používaných bezpečnostními službami budovanými na bázi ASK. PKI podporuje důvěryhodnost takových bezpečnostních služeb, protože umožňuje používat bezpečnostní mechanismy ASK důvěryhodně. Z etymologického hlediska se v informačních technologiích *důvěryhodností* nějakého systému rozumí přesvědčení, že systém splňuje předem dané požadavky a specifikace.

Typická PKI zahrnuje nástroje pro vydávání digitálních certifikátů jednotlivcům, ale použitelnost rovněž i serverům, registrační software, nástroje pro integraci různých druhů seznamů certifikátů, nástroje pro správu, odvolávání (revokaci), prokazování platnosti certifikátů a obnovu platnosti odvolaných certifikátů, poskytuje odpovídající služby a vytváří podpůrné prostředí pro uplatnění těchto služeb. PKI tvoří kombinace software, kryptografických technologií a poskytovaných služeb.

PKI podporuje dosažení důvěryhodnosti. Důvěra ale není tranzitivní vztah. Kdyby byla a kdyby se „pavučina důvěry“ namodelovala hranami vedoucími od Alice k Bobovi jako model vztahu, že Alice důvěřuje Bobovi, pak bychom z tranzitivního uzávěru množiny lidí, kteří si důvěřují, zřejmě odvodili, že všichni lidé na světě si důvěřují a nemuseli bychom se problémem bezpečnosti zabývat vůbec. Dále platí, že důvěra je kvalifikovaný pojem. Je velmi pravděpodobné, že každý z nás věří jiné osobě jen v jistém kontextu, v sféře společného zájmu. Kvalifikace důvěry v jisté oblasti je vyjádřena autorizací. Jestliže banka A vydá majiteli karty Bobovi certifikát s autorizací pro podpisování elektronických šeků banky A čerpajících jeho účet, pak pochopitelně obchodník za jistých podmínek akceptuje elektronické šeky banky A podepsané Bobem, ale neakceptuje šeky jiné banky také podepsané Bobem. Obchodník nedůvěřuje majiteli karty B všeobecně. Obchodník má pravděpodobně s bankou A uzavřenou smlouvu, která mu zaručuje, že když bance A předloží elektronický šek banky A podepsaný klíčem certifikovaným bankou A, pak mu banka A přesune na jeho účet odpovídající finanční částku. Obchodníkovi jde o tento přesun, ne o to, zda může nějakému majiteli karty všeobecně důvěřovat.

Soudobé a perspektivní způsoby užívání IT předpokládají, že podporu ze strany PKI budou při své každodenní činnosti pravděpodobně potřebovat prakticky všichni uživatelé síťových aplikací. Tato skutečnost je dána rostoucím významem síťových prostředí a transakčního zpracování, realizovaného pomocí nedostatečně zabezpečovaných kanálů v sítích. Pro zajištění integrity, důvěrnosti a nepopiratelnosti v takovém prostředí se stále intenzivněji používají mechanismy ASK a bezpečné používání mechanismů ASK si vynucuje podporu ze strany PKI.

PKI umožňuje zpracovávat citlivá data v prostředí sdílených sítí (v prostředí Internet) a automatizovat citlivé funkce, které by bez použití PKI bylo nutné realizovat mimo takové sítě. Tím umožňuje implementovat kvalitnější služby při vynakládání únosných nákladů. Použití PKI dále snižuje náklady a zvyšuje provozní efektivnost spolupráce v distribuovaném heterogenním prostředí tím, že bezpečnostní služby není potřeba duplikovat. Dosažení interoperability si pochopitelně vynucuje použití kompatibilních technologií a standardizovaných implementačních postupů a PKI musí být od počátku navrhována s tímto cílem.

PKI usnadňuje implementaci bezpečnostních služeb nepopiratelnosti, identifikace a autentizace, důvěrnosti, integrity, obnovy dat a klíčů a autorizace (certifikáty mohou vedle identity jednotlivce specifikovat i jemu udělená privilegia). Jako konkrétní příklady oblastí využití PKI lze uvést podporu

- vzdáleného přístupu k informačním systémům pomocí propracovanějších služeb identifikace a autentizace (na rozdíl prosté „heslové“ ochrany)
- zabezpečování finančních transakcí
- bezpečné výměny zpráv se zárukou důvěrnosti a integrity přenášených dat
- bezpečnosti transakcí mezi klienty a servery pomocí tajných klíčů relací
- záruky za autentičnost a integritu veřejně přenášených dokumentů pomocí elektronického podepisování.

Ve své nejběžnější formě je PKI infrastruktura určená pro důvěryhodné šíření hodnot veřejných klíčů ASK, používaných jako podepisovací klíče nebo šifrovací klíče. Mezi další oblasti využití PKI patří např. potvrzování přístupových práv.

1.2 Orientační přehled architektury, principů operací a služeb PKI

Základním požadavkem na efektivní použití ASK a řady dalších bezpečnostních mechanismů v soudobých IT je, aby je mohly bezpečně používat subjekty, které se a priori neznají. Ukazuje se, že v komunitě mnoha miliónů subjektů lze tohoto dosáhnout pomocí poměrně malého počtu důvěryhodných autorit, které certifikují digitálně podepsaným dokumentem hodnoty relevantních vlastností identifikovaných subjektů. Autority nazýváme *certifikační autority*, jimi vydávané dokumenty nazýváme *certifikáty*. Certifikát důvěryhodně potvrzuje hodnotu nějaké vlastnosti *držitele certifikátu*. Subjekt, který se rozhoduje na základě certifikované vlastnosti certifikátem, je *uživatelem certifikátu*.

Držitelé certifikátů předkládají certifikáty jejich uživatelům podle protokolu transakce probíhající mezi držitelem a uživatelem certifikátu. Vydané certifikáty mohou být rovněž zpřístupňovány ve skladech certifikátů – v *repositářích certifikátů*. Pro zpřístupňování certifikátů se používají jak speciální, tak i mnohé universální techniky (databáze a protokoly jakými jsou např. X.500, FTP servery, web servery, LDAP protokoly apod.).

Certifikáty mívají obvykle časově omezenou platnost a navíc existuje možnost platnost certifikátu kdykoliv odvolat – *revokovat*, např. po zjištění, že informace udaná v certifikátu není dále validní (soukromý klíč byl kompromitován, autorizace odvolána apod.). Platnost certifikátů uživatelé ověřují buďto explicitními dotazy kladenými autoritám odpovědným za udržování seznamů revokovaných certifikátů nebo používají v rámci svých transakcí on-line protokoly detekce stavu certifikátu.

Všeobecná orientovanost PKI na využívání ASK a používání PKI pro podporu bezpečnosti aplikací založené na používání ASK mnohdy vyžaduje, aby PKI poskytovala službu

zálohování a zotavení klíčů (Key Backup and Recovery) pro případ řešení situace po zničení média s uloženým soukromým klíčem (pevného disku, čipové karty) nebo zapomenutí heslové fráze umožňující přístup k šifře soukromého klíče, které by mohly způsobit trvalé znepřístupnění šifrovaných citlivých dat.

Časově omezená platnost certifikátů veřejných klíčů nutí jejich držitele periodicky platnost certifikátů aktualizovat (obnovovat, renew). Aktualizace certifikátů formou explicitního vydání nového certifikátu po vypršení platnosti původního certifikátu může mnohdy představovat netriviální validační proces vyžadující často přímý kontakt držitele obnovovaného certifikátu s certifikační autoritou, podobný jako při iniciálním vydání certifikátu. Navíc, po dobu takové obnovy certifikátu je držitel původního certifikátu pro PKI neznámý. Řešením může být poskytování služby *automatické aktualizace klíčů a certifikátů* (Automatic Key Update) odpovídající PKI. Proces automatické aktualizace PKI spouští ještě před uplynutím expirační doby certifikátu.

Poskytování služby automatické aktualizace klíčů a certifikátů přirozeně vyvolává potřebu (automaticky) poskytovat službu *archivace klíčů a certifikátů* (Key History). Po jisté době každý držitel automaticky aktualizovaného certifikátu vlastní několik „starých“ certifikátů a alespoň jeden „aktuální“ certifikát. PKI musí v takovém případě udržovat bezpečný repositář klíčů a při zpřístupňování historických dat podle potřeby provádět zotavování klíčů (recovery) z jejich záloh (backup) dynamicky. Při automatické aktualizaci klíče/certifikátu nelze očekávat, že by se znovu šifrovala nebo podepisovala všechna historická data.

Různorodost aplikací, organizačních a politických uspořádání různých komunit neumožňuje používat jedinou, všezahrnující PKI. PKI se budují postupně, v různých lokalitách a s různým aplikačním zaměřením. Přitom se ale mohou vyskytnout požadavky na bezpečnou komunikaci mezi uživateli náležejícími do domén působnosti různých PKI. Ověřování platnosti a uznávání certifikátů mezi různými PKI zajišťují procesy a protokoly *vzájemné certifikace* (Cross-Certification).

Po PKI se velmi často požaduje, aby podporovala službu *nepopiratelnosti* (Non-Repudiation), která úzce souvisí s digitálním podpisováním dokumentů. PKI samy tuto službu neposkytují, důkazní proces vesměs požaduje využití mnohem širší infrastruktury založené na jurisdikci. PKI zajištění nepopiratelnosti pouze podporují technickými důkazními materiály. Pro zajištění potřebné kvality důkazních materiálů se obvykle vyžaduje akreditace odpovídajících certifikačních autorit podle příslušných zákonných opatření té či oné země.

S poskytováním podpory nepopiratelnosti nutně souvisí další služba, kterou musí PKI podporující nepopiratelnost poskytovat – služba *časového razítkování* (Time Stamping). Důvěryhodná znalost času výskytu nějaké události (vzniku dokumentu, podepsání dokumentu apod.) má pochopitelně širší aplikační použitelnost, než jen v oblasti práva.

Pro implementaci uvedených služeb se používají tradiční bázové bezpečnostní služby zajišťující identifikovatelnost a autenticitu, důvěrnost, integritu, dostupnost. Pomocí tradičních bázových bezpečnostních služeb a výše zmíněných služeb poskytovaných PKI lze budovat další sofistikované nadstavbové bezpečnostní služby, jakými jsou notarizace, bezpečné datové archivy, správa přístupových práv v rozsáhlých IS, delegace pravomocí apod.

Pro implementaci služeb poskytovaných PKI a služeb založených na používání PKI se vyžívají jak bázové bezpečnostní mechanismy typu šifrovač, jednosměrná hašovací funkce, digitální podpis, MAC (Message Authentication Code) nebo seznam přístupových práv, tak i sofistikovanější mechanismy, jakým je např. důvěryhodný zdroj času nebo autentizační systém Kerberos, redundantní multiprocesorové a multipočítačové sestavy, specializované protokoly atd.

Nepominutelnou součástí každé PKI jsou, vedle vnitřních serverů plnících výše popsané služby, netriviální implementace klientských rozhraní podporovaných služeb a mechanismy celkové správy PKI.

Na závěr úvodního přehledu si připomeňme, že zavedení PKI spočívá především v implementování dvou základních kategorií služeb – *používání digitálních certifikátů* (potvrzování platnosti certifikace, proces ověřující, že certifikace je stále platná) a *vydávání digitálních certifikátů* (proces vlastní certifikace, tj. svázání hodnoty veřejného klíče a/nebo nějaké jiné informace s identitou jednotlivce, eventuelně s identitou organizace, tj. se samostatně vystupující entitou, resp. se subjektem). Různé typy PKI (X.509, PGP, PKIX, SPKI, SDSI, DNS PKI, ...) se vzájemně liší jak cílovým zaměřením obou základních služeb, tak i způsobem jejich implementace, a navíc škálou dodatečně poskytovaných služeb.

1.3 Příklady aplikačních orientací PKI

- *Klasická univerzální internetovská PKI* obvykle pouze pomocí certifikačních autorit podporuje autentizaci, integritu a důvěrnost. Neudržuje repositář certifikátů, jejich držitelé je zasílají příslušným uživatelům standardními komunikačními prostředky. Platnost certifikátu se ani automaticky nekontroluje ani neobnovuje. Vzájemná certifikace se neřeší, server i klientský prohlížeč musí důvěřovat společné certifikační autoritě. Nepodporuje se časové razítkování, notarizace, delegace pravomocí apod.
- *PKI podporující provoz extranetu*, ve kterém klienti přistupují ke zdrojům extranetu pomocí svých prohlížečů za podpory SSL autentizace, by měla navíc podporovat revokaci certifikátů, zálohování klíčů a vhodnou certifikací autorizaci pro řízení přístupu.
- Pokud se pro řízení chodu organizace používá standardní elektronická pošta zabezpečovaná pomocí PKI, měla by (*poštovní*) *PKI* navíc proti klasické PKI podporovat zálohování a zotavování klíčů a automatickou aktualizaci klíčů a certifikátů a archivaci klíčů a certifikátů. Poštovní rozhraní prohlížečů klientů bude asi proprietární, standardní poštovní rozhraní takové služby nepodporují.
- *PKI podporující meziorganizační styky*, musí podporovat vzájemnou certifikaci, s komerční činností organizací se obvykle navíc druží požadavek na podporu nepopiratelnosti a může se požadovat i podpora řízení přístupu. Vesměs až na některé doplňkové služby, jakou je např. notarizace, taková PKI poskytuje nebo podporuje plnou škálu služeb zmíněných v celkovém přehledu.

2 Digitální certifikát, procesy certifikace a používání certifikátů

2.1 Digitální certifikát

Digitální certifikát je digitálním (elektronickým) ekvivalentem fyzického (papírového) certifikátu. Fyzickým certifikátem je např. řidičský průkaz, občanský průkaz nebo pas. Fyzický certifikát může sloužit jako nástroj identifikace jednotlivce za jistým účelem nebo jako průkaz potvrzující hodnotu nějaké vlastnosti entity (např. kvalitu výrobku nebo splnění nějaké normy). Digitální certifikát se typicky používá jako průkaz identity jednotlivce a nějaké jeho vlastnosti (např. hodnoty jeho veřejného klíče používaného pro ověřování jeho podpisu nebo pro šifrování jemu zasílaných důvěrných zpráv) nebo jako průkaz jeho práv přístupu k informacím nebo službám. Hlavním a původním cílem digitálního certifikátu je spolehlivě asociovat jednotlivce s jeho veřejným klíčem. Digitální certifikát je reprezentován datovou zprávou obvykle s pevnou a standardizovanou strukturou. Aby plnil funkci spolehlivého identifikačního průkazu nebo spolehlivého průkazu hodnoty nějaké vlastnosti jeho držitele, musí být důvěryhodný.

Důvěryhodnost digitálního certifikátu je založena na stejném principu jako důvěryhodnost fyzického certifikátu. Fyzický certifikát bývá obtížně padělatelnou formou (podpisem, razítkem) vydán a označen nějakou důvěryhodnou autoritou. Podobně je i digitální certifikát[1] vydáván nějakou důvěryhodnou autoritou. Ta je k vydávání certifikátů zplnomocněna zákonem, vnitřní politikou organizace používající PKI apod. Je základní komponentou PKI. Nazývá se *certifikační autorita*, CA. Je odpovědná za potvrzování platnosti informací uváděných v žádostech o vydání certifikátů. Po ověření platnosti informací udávaných v žádosti potvrzuje jejich platnost vydáním certifikátu podepsaného svým obtížně padělatelným digitálním podpisem.

2.2 Základní role vystupující v PKI

Nyní si již můžeme uvést tři základní role, které vystupují v každé PKI:

1. *držitel certifikátu* – entita, jejíž vlastnost (identita) je certifikovaná
2. *certifikační autorita* – vydavatel certifikátu, poskytovatel certifikační služby
3. *uživatel certifikátu* – strana spoléhající se na důvěryhodnost certifikátu.

Digitální certifikát vedle informací o certifikovaných vlastnostech musí obsahovat i identifikační informace o držiteli certifikátu, identifikační informace o CA, která certifikát vydala a podepsala, informace o době platnosti certifikátu, o úrovni jeho důvěryhodnosti (dané prokazatelnou důvěryhodností CA, která digitální certifikát podepsala, která je dána mj. způsobem prověřování žádosti o vydání certifikátu) a případně může obsahovat i informace o možných třídách aplikací (uživatelů certifikátu), které certifikát uznávají.

Jestliže si Alice přeje důvěrně komunikovat pomocí ASK s Bobem, musí bezpečně znát veřejný šifrovací klíč Boba. Bez dostupnosti PKI musí Bob svůj veřejný šifrovací klíč Alici sdělit nějakým bezpečným kanálem. Totéž musí platit i pro opačný směr komunikace. Pokud Alice i Bob důvěřují nějaké společné certifikační autoritě CA_A, pak si Alice může nechat vystavit od CA_A certifikát svého veřejného klíče (Alice je držitelem tohoto certifikátu) a Bobovi takový certifikát zpřístupnit (Bob je uživatelem Alicina certifikátu).

Všechny tři zmíněné role mohou vystupovat jako odlišné entity, ale každá entita může současně vystupovat ve všech třech rolích nebo ve kterýchkoliv dvou ze zmíněných tří rolí. Způsob, kterým se v PKI ustanoví vztah důvěry mezi uvedenými třemi rolemi, je další charakteristikou, kterou se jednotlivé typy PKI od sebe odlišují. Alice věří certifikátům vystaveným její CA_A. Pokud Alice a CA_A jsou různé entity, pak velikost víry uživatele Boba ve spolehlivost certifikační autority CA_A vymezuje velikost důvěry Boba v použití certifikátu veřejného klíče vydaného Alici CA_A pro důvěrnou komunikaci s Alicí.

CA a digitální certifikáty jsou dva základní prvky PKI. PKI obvykle sestává z více komponent, na jejichž funkci a význam upozorníme později.

2.3 Typy digitálních certifikátů

Digitální certifikát lze použít např. i k tomu, aby se klient mohl bez explicitního udávání nějakého přihlašovacího jména a hesla spojit s WWW serverem s řízeným přístupem. Certifikát lze rovněž použít pro ověření autenticity e-mailové zprávy nebo jiného dokumentu podepsaného jejím (jeho) autorem. Zamýšlený příjemce takové podepsané datové zprávy ověřením podpisu získá jistotu, že se jedná o datovou zprávu skutečně vytvořenou jejím původním autorem, že její obsah nebyl ani záměrně ani neúmyslně porušen. Digitální certifikát také umožňuje přijímat důvěrné zprávy, které může číst pouze zamýšlený příjemce. Na sdílené síti s nízkou úrovní komunikační bezpečnosti, jakou je Internet, lze po zavedení PKI používat bezpečnou elektronickou poštu, zabezpečované WWW aplikace a vést bezpečné on-line transakce jak v rámci jednoho distribuovaného informačního systému, tak i

[1] pojem „certifikát“, pokud neřekneme jinak, používáme ve významu „digitální certifikát“.

mezi samostatně provozovanými informačními systémy. Digitální certifikát lze přenášet na disketě, komunikačním kanálem, sítí apod.

Digitální certifikát osoby identifikuje osobu, obsahuje její jméno, případně její další osobní charakteristiky (vlastnosti) a/nebo jí udělená privilegia (obecně – atributy). Používá se např. pro ověřování digitálních podpisů dokumentů, pro zabezpečování e-mailové korespondence nebo pro řízení přístupu k citlivým (hodnotným) informacím. Digitální certifikáty osob umožňují používat všichni významní poštovní klienti respektující standard S/MIME (Secure Multipurpose Internet Mail Extensions) pro formátování pošty (Microsoft Outlook, Netscape). S/MIME formátování přijala většina výrobců systémů pro zasílání zpráv jako standard formátů zpráv. WWW prohlížeče umožňují svému uživateli zavést svůj digitální certifikát osoby a používat ho pro autentizaci vůči vzdálenému serveru (taková autentizace je silnější než autentizace pomocí jména a hesla).

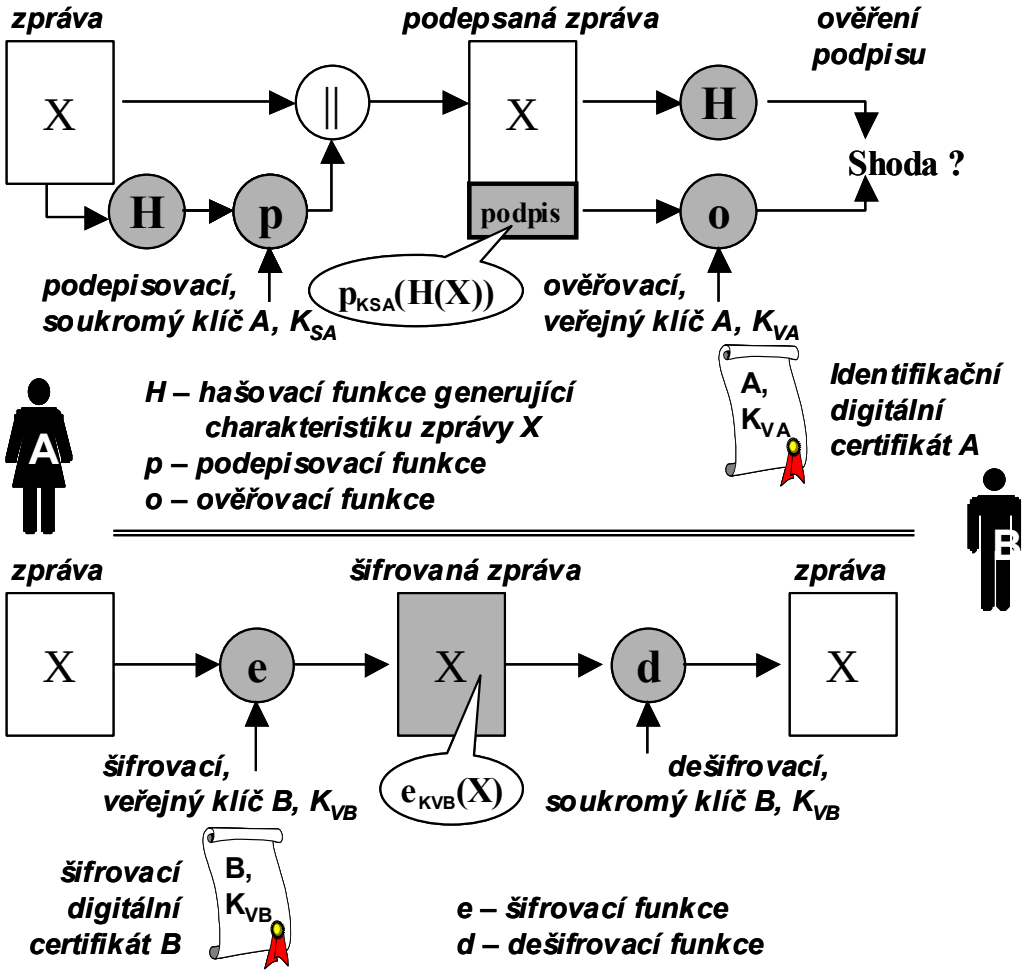
Digitální certifikát serveru potvrzuje identitu serveru (jméno uzlu sítě). Umožňuje zabezpečovat on-line transakce prováděné mezi klientem a serverem.

Některé PKI umožňují používat více typů digitálních certifikátů osob a serverů. *Identifikační digitální certifikát osoby* se používá při digitálním podepisování datových zpráv a jako nástroj pro bezpečnou identifikaci a autentizaci uživatele. *Šifrovací digitální certifikát osoby* se používá při šifrování zpráv zasílaných elektronickou poštou držiteli šifrovacího certifikátu. Používání samostatných digitálních certifikátů pro různé účely zvyšuje bezpečnost, protože pro různé aplikace se nepoužívají stejné klíče (veřejný ověřovací klíč digitálního podpisu Alice je jiný klíč, než její veřejný šifrovací klíč používaný pro zasílání důvěrných zpráv určených Alici). Použití individuálních a šifrovacích certifikátů ilustruje obrázek Obr.1.

Vlastnosti osoby, resp. jí přidělená privilegia (autorizace), se vesměs nazývají „atributy“ a lze je potvrzovat *atributovými digitálními certifikáty osoby*. Atributový certifikát může potvrzovat, že „Alice má právo přístupu k počítači ABC“, že „Bob je certifikovaný makléř“ apod. Atributové certifikáty se mnohdy nazývají *credential certificates*. Existují PKI, které jsou principiálně založeny na používání atributových certifikátů, např. SDSI (Simple Distributed Security Infrastructure) nebo SPKI (Simple Public Key Infrastructure). Širší používání atributových certifikátů nastupuje teprve ve druhé polovině 90. let.

Certifikát serveru rovněž může mít charakter identifikačního, šifrovacího nebo atributového certifikátu.

Certifikáty se liší nejen sémantikou, ale přirozeně také syntaxí. Oba tyto rysy určují PKI, které je vydávají. Struktura certifikátů vydávaných podle doporučení X.509 je jiná, než struktura certifikátu SPKI nebo struktura certifikátu PKI PGP (Pretty Good Privacy). Podrobnější rozbor vybraných typů PKI uvádíme v kapitole 5.



Obr.1 Identifikační a šifrovací certifikát

2.4 Příklady práce s digitálními certifikáty

Proces vyžádání a vydání certifikátu veřejného klíče typicky sestává ze 2 kroků:

1. Osoba požadující certifikát si vhodným způsobem vygeneruje dvojici klíčů ({*veřejný šifrovací klíč, soukromý klíč*}, resp. {*ověřovací klíč, podepisovací klíč*}) a vygenerovaný veřejný šifrovací (ověřovací) klíč, a případné dodatečné informace pro umístění do certifikátu, předá CA společně s důvěryhodným prokázáním své identity.
2. CA prověří platnost dodaných identifikačních informací, případně na vzorku podpisu dat ověří konzistentnost párových klíčových dat, vytvoří nový certifikát, dodaný certifikovaný klíč a případné dodatečné informace do něj umístí, podepíše jej a zašle žádající osobě. Podle důkladnosti a důvěryhodnosti prověřování dodaných informací může CA vydávat certifikáty odlišných kvalit.

Při ověřování digitálního podpisu zprávy se ověřující strana z identifikačního certifikátu podepsané osoby důvěryhodně dozvídá hodnotu ověřovacího klíče podpisu podepsané osoby. Odesílatel důvěrné zprávy zjistí veřejný šifrovací klíč adresáta z jeho šifrovacího certifikátu.

Když se digitální *certifikát serveru* umístí na WWW server, klienti si mohou pomocí takového certifikátu ověřit autenticitu serveru. Certifikát serveru zaručuje, že server je provozován organizací, která má právo používat jméno uvedené v certifikátu serveru. Uživatele tak chrání před důvěřováním neautorizovaným stranám. WWW server může řídit přístup a kontrolovat identitu klientů pomocí *certifikátů klientů*. Takovou vzájemnou autentizaci klientů a serveru umožňuje např. technologie SSL. Vzájemná autentizace a ustanovení výkonného bezpečného kanálu mezi klientem a serverem se dosáhne např. provedením následujících kroků:

1. Klient navštíví WWW server a ze svého prohlížeče ho vyzve k autentizaci.
2. Server prokáže svoji identitu zasláním svých certifikátů serveru (identifikačního a případně i šifrovacího) prohlížeči klienta.
3. Prohlížeč klienta prověří autenticitu serveru podle získaného identifikačního certifikátu serveru, aby si jeho uživatel byl jistý, že navštívil správný server.
4. Server si od prohlížeče klienta vyžádá (identifikační) certifikát klienta.
5. Klient dodá svému prohlížeči svůj identifikační certifikát a prohlížeč ho zašle serveru.
6. Server si ověří autenticitu klienta a případně i jeho privilegia (autorizaci).

Klientův prohlížeč důvěrně zašle serveru tajný klíč relace šifrovaný pomocí veřejného šifrovacího klíče serveru.

Předaný tajný klíč umožní používat při komunikaci mezi serverem a klientem výkonné symetrické šifrování. Tím je ustanoven bezpečný komunikační kanál mezi klientem a serverem, který poskytuje všechny tři základní bezpečnostní služby: zajištění důvěrnosti přenášených zpráv, zajištění integrity přenášených zpráv a zajištění autenticity přenášených zpráv.

2.5 Celkový přehled životního cyklu klíčů a certifikátů

V typické PKI se veškeré certifikační procesy odehrávají ve třech základních etapách životního cyklu klíčů a certifikátů – v iniciální fázi, ve fázi práce s vydanými certifikáty a ve fázi rušení certifikátů. V iniciální fázi dominují procesy registrace žadatele, generování párů klíčů, vytvoření certifikátu a předání certifikátu žadateli, jeho diseminace a případně i proces zálohování. Ve fázi práce s vydanými certifikáty se jedná především o proces získání certifikátu, validace certifikátu, zotavení zálohovaného klíče a automatické aktualizace klíče a certifikátu. Ve fázi rušení certifikátu se jedná o proces vyvolaný uplynutím expirační doby, proces revokace a proces archivace klíčů a certifikátů. Z důvodů omezeného prostoru pro výklad se samostatně věnujeme pouze procesům validace a revokace a. problému určení důvěryhodnosti CA při validaci. Poté souhrnně uvedeme základní charakteristiky ostatních procesů

2.6 Validace certifikátu a proces revokace certifikátu

Validací certifikátu (potvrzováním platnosti vydaných certifikátů) se rozumí proces určující, zda může či nemůže uživatel certifikátu daný certifikát použít v daném kontextu. Validní certifikát musí být podepsán důvěryhodnou CA (pro validaci důvěryhodnosti CA se často používá mechanismus certifikačních cest popsaný v následující podkapitole), ověření podpisu CA musí prokázat zachování integrity certifikátu, certifikát musí být uplatněn před uplynutím jeho expirační doby, nesmí být revokován a musí být uplatněn způsobem konzistentním s omezeními stanovenými certifikační politikou a případnými dalšími omezeními na použití např. certifikovaného klíče, které bývají uváděny v doplňkových (rozšiřujících) položkách certifikátů. Potvrzování platnosti vydaných certifikátů patří mezi standardně poskytované služby PKI.

Uvedli jsme, že platnost certifikátu lze odvolat, certifikát lze *revokovat*. Odvoláním se ruší vazba mezi držitelem certifikátu a jeho veřejným klíčem, resp. jinou certifikovanou vlastností. Platnost certifikátu se odvolává např. při podezření, že držitel certifikátu ztratil výhradní kontrolu nad použitím odpovídajícího párového soukromého klíče nebo v případech, kdy se nějaká skutečnost uvedená v certifikátu změnila. Platnost certifikační cesty je dána informací o stavech certifikátů, které certifikační cestu vytvářejí. Způsob provedení *revokace certifikátů* je tedy další charakteristikou typu PKI.

Uživatel, spoléhající se na platnost certifikátu nebo certifikační cesty, může stav certifikátů zjišťovat dvojím způsobem:

1. zjištěním, že daný certifikát byl revokován v publikovaných *seznamech certifikátů s odvolanou platností*, resp. v *seznamech revokovaných certifikátů*, *CRL* (Certificate Revocation List)
2. on-line dotazy u *poskytovatelů informací o stavu certifikátů, OCSP* (On-line Certificate Status Provider), pomocí některého vesměs standardizovaného dotazovacího protokolu (OCSP je rovněž označení pro jeden takový protokol, On-line Certificate Status Protocol, definovaný v RFC2560).

Seznam revokovaných certifikátů periodicky vydává a podepisuje obvykle CA, která revokované certifikáty původně vydala. Je na uživateli certifikátu, aby si ověřil v posledním vydání CRL nebo on-line dotazem o některého OCSP, že je daný certifikát platný, ještě před použitím certifikátu.

Aby publikovaný CRL byl důvěryhodný, bývá obvykle jeho vydavatelem podepsán. Pro podpis CRL může příslušná CA používat jiný klíč a/nebo algoritmus, než který používá pro podepisování vydávaných certifikátů.

Mezi klíčové problémy revokace certifikátů formou CRL především patří problém časové granularity. Co se děje v době mezi okamžikem, kdy CA získá sdělení, že musí certifikát revokovat a okamžikem vydání nové verze CRL? Po tuto dobu budou uživatelé certifikátu, o jehož zneplatnění byla CA držitelem certifikátu požádána, mylně předpokládat, že daný certifikát je platný.

Problém důvěryhodnosti podepsaného dokumentu i po odvolání platnosti certifikátu ověřovacího klíče budeme řešit samostatně později.

Dalším klíčovým problémem revokace certifikátů formou CRL je velikost CRL. Pro zpřístupňování rozsáhlých CRL a ověřování jejich podpisů musí mít uživatel certifikátů k dispozici dostatečně velkou komunikační šířku pásma a výpočetní výkon. Aby CA minimalizovala nároky na přístup a zpracování svých CRL, může např. tyto seznamy udržovat jako samostatné CRL – CRL identifikačních certifikátů, CRL šifrovacích certifikátů, resp. CRL neplatných atributových certifikátů, tzv. ARL (Attribute Certificate Revocation List). CA rovněž může zveřejňovat CRL samostatně pro jednotlivá dílčí oddělení nějaké organizace (Redirected CRLs).

Vhodným řešením se jeví i častější publikování tzv. *Δ-CRL*, které obsahují pouze změny revokací proti poslednímu vydání plného CRL. Proces potvrzování platnosti certifikátů u uživatele certifikátu pak může začít s plným CRL, který si posléze aktualizuje synchronně s vydáváním Δ-CRL.

Jako perspektivní se jeví on-line potvrzování platnosti certifikátů. Na vývoji odpovídajících metod a protokolů se intenzivně pracuje, požadovaná šířka komunikačního pásma a dostupnost zpracovávatelského výkonu však stále může být pro běžného uživatele certifikátu omezujícím faktorem. On-line dotazování na stav certifikátů připouští budovat politiku potvrzování platnosti certifikátů na úplně jiné ideové bázi. Udržování CRL reprezentuje velmi liberální přístup k potvrzování platnosti certifikátů – certifikát se považuje za platný až do okamžiku zjištění opaku (v CRL). Liberální přístup ale silně trpí problémem časové granularity. On-line potvrzování platnosti může problém časové granularity částečně řešit. Vychází z opačné myšlenky – z konzervativního pohledu na svět. Považuje každý certifikát za neplatný až do okamžiku, kdy se přesvědčí o opaku. Pro mnohé aplikace je konzervativní přístup neakceptovatelný, např. představa, že každá platební karta je při každém použití

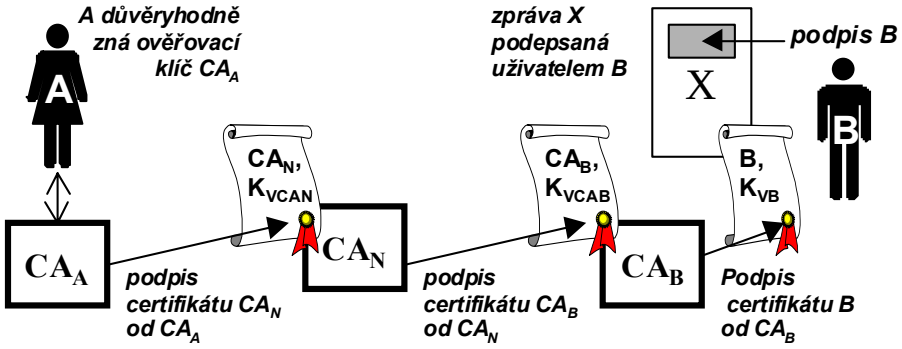
předem považována za blokovanou a odblokuje se až po on-line dotazu (jinými slovy – rizika plynoucí z liberálního přístupu jsou pro banku přijatelná) se nemusí krýt s obchodními zájmy banky.

Nakonec se sluší připomenout, že může existovat představa, že v omezené doméně s konečnou množinou vzájemně známých partnerů, lze implementovat komunikační systém např. i na bázi zabezpečovaných (privátních) virtuálních sítí a pak potvrzování platnosti certifikátů nedělat vůbec, ale to pak musíme i zvažovat zda v takovém případě má smysl zavádět PKI, a „s vaničkou vyléváme i dítě".

2.7 Modely důvěry, certifikační cesty

Dalším klíčovým pojmem PKI *certifikační cesta*. Bylo by zjevně nepraktické provozovat na celém světě jedinou centrální CA. Většina PKI proto povoluje jedné CA certifikovat jinou CA. Certifikující CA říká uživateli, který důvěřuje jí vydaným certifikátům, že může věřit certifikátům vydaným certifikovanou CA.

Certifikační cesta je reprezentována řetězcem identifikačních certifikátů, který začíná certifikátem, vydaným tou CA, které strana přijímající datovou zprávu (Alice, A) důvěřuje, pro nějakou jinou CA_N a končí certifikátem, který předkládá podepisující se strana (Bob, B) jako doklad platnosti podpisu datové zprávy, který vydala CA, které důvěřuje B. Princip certifikační cesty ilustruje Obr. 2.



Obr. 2 Certifikační cesta

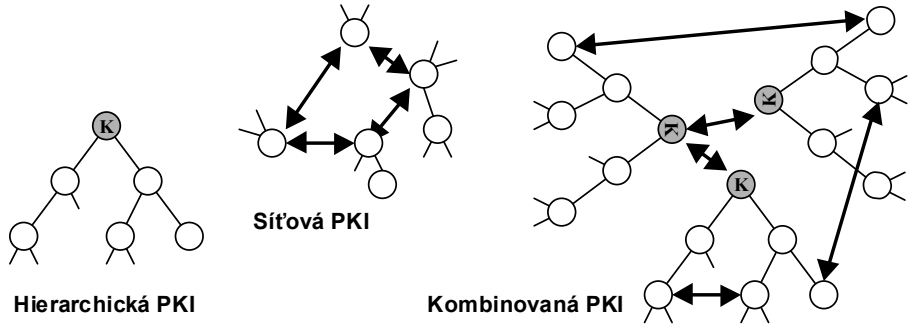
A důvěřuje CA_A, je přesvědčena o její důvěryhodnosti. Počínaje certifikátem vydaným CA_A pro CA_N může strana A spoléhající se na CA_A ověřit platnost řetězce certifikátů vedoucího k identifikačnímu certifikátu strany B. Ověřovací klíč CA_A strana A důvěryhodně zná, byl jí nějakým bezpečným způsobem dodán, např. mimo sdílenou komunikační síť. Držitelům certifikátů bývají takové klíče dodávány i formou certifikátů podepsaných vlastní CA nebo nějakou nadřazenou „kořenovou CA". Strana A důvěřuje CA_A, zná její veřejný klíč. Veřejný klíč CA_N se dozvídá z certifikátu CA_N vydaného CA_A. Může takto postupně ověřit každý certifikát na certifikační cestě vedoucí až k certifikátu strany B a ověřit i certifikát strany B.

CA se mohou nějakým systematickým způsobem certifikovat vzájemně (křížově), vytvářejí tak v PKI *pavučinu důvěry*. Jedna CA může vlastnit certifikát vydaný jinou CA. Dvě CA se mohou certifikovat vzájemně, hovoříme o *křížové certifikaci* (cross-certification) a o *křížových certifikátech*.

Možná uspořádání CA v PKI je další charakteristickou vlastností různých typů PKI. Dvě základní alternativní topologie PKI jsou hierarchická topologie a síťová topologie, základní topologie lze dále kombinovat do složitějších struktur, viz Obr. 3.

PKI s *hierarchickou topologií* má svoje CA uspořádány pod nějakou „kořenovou" CA hierarchicky. Všichni klienti PKI bezpečně znají veřejný klíč její kořenové CA. Certifikát držitele se ověřuje po certifikační cestě, která vede zpět do kořenové CA (v obrázku Obr. 2 je

certifikační cestou posloupnost CA_B, CA_N, CA_A, pokud je CA_A kořenovou CA). Hierarchická PKI odpovídá modelu systému s centralizovanou důvěrou, ve kterém je naprostá většina operací správy klíčů často prováděna mimo přímý vliv klientů PKI. Ti vkládají velkou část důvěry v jiné činitele a ve správnost operací prováděných těmito činiteli. Jedná se především o problém generování párových klíčů. Ty se sice mohou generovat „lokálně", pod výhradní kontrolou klienta a v centru se pak pouze certifikují, mnohdy se však generují nějakou třetí stranou mimo kontrolu klienta a v centru se posléze pouze certifikují, případně se v centru i generují nebo se generují za spoluúčasti klienta a centra. V hierarchické PKI se nepoužívá křížové uznávání certifikátů. Řízení a správa hierarchických PKI je poměrně snadná. Použitelnost hierarchických PKI je však silně omezená, protože mnohé organizace hierarchicky organizovány nejsou.



Obr. 3 Příklady možných topologií PKI

V *síťové PKI* se nezávislé CA certifikují vzájemně podle nějaké zavedené obecné sítě vztahů důvěry mezi nimi. Klient zná veřejný klíč jemu blízké CA (obvykle té lokální CA, která mu vydala certifikát) a předložené certifikáty ověřuje po certifikační cestě, která vede zpět do jemu blízké CA. Takových cest může existovat více. Pokud taková cesta neexistuje, pak předloženému certifikátu nedůvěřuje. Síťová PKI je pružnou strukturou, lze ji aplikovat na libovolně zavedené vztahy důvěry. Při jejím zavedení se předpokládá, že uživatel mnohem více důvěřuje své lokální CA než nějaké vzdálené kořenové CA. Veřejný klíč lokální CA se může poměrně rychle distribuovat klientům, kteří se na ni spoléhají. Na druhé straně jsou v síťové PKI složité strategie hledání efektivních certifikačních cest a klient nemůže všem svým komunikačním partnerům sdruženým v síťové PKI garantovat jednu jedinou certifikační cestu pro ověřování svých podpisů. V plně nestrukturované PKI je de facto každá CA svou vlastní kořenovou CA a je plně odpovědná za to, jak je jí přidělována důvěra. Např. v PKI PGP (Pretty Good Privacy) každá CA zakládá svoji důvěru na certifikátech všech ostatních CA – jestliže vlastní dostatečný počet certifikátů ostatních CA, které vážou jisté jméno s konkrétní hodnotou klíče, může daná CA této vazbě s jistou důvěryhodností důvěřovat (tzv. *web-of-trust*).

Kompromisním řešením architektury PKI je *kombinovaná PKI*, obvykle tvořená několika vhodně propojenými hierarchickými PKI. Jejich kořenové CA náleží do vhodné síťové PKI. V kombinované PKI lze přitom zavádět vztahy vzájemné důvěry i mezi některými (nekořenovými) CA přímo.

Delegování důvěry je poměrně složitý problém z hlediska tranzitivity důvěry. Jestliže A důvěřuje B a B důvěřuje C ještě neznamená, že B definuje pojem důvěry stejně přísně jako A. Hodnota klíče, kterou A dostane od C zprostředkovaně přes B, může být pro A plně nedůvěryhodná, i když pro B je dostatečně důvěryhodná. Tento problém nabývá tím většího významu, čím více se certifikační cesty prodlužují. Hierarchické modely délky cest spíše prodlužují. Centrální kořenová autorita je pochopitelně velmi atraktivním cílem pro útoky a navíc musí její veřejný klíč všichni uživatelé PKI a priori znát. Vhodně nastavené „příčky" v topologii kombinované PKI mohou délky certifikačních cest podstatně zkrátit.

Uvedli jsme, že certifikáty obsahují identifikace použitých algoritmů. Algoritmus, kterým podepisuje certifikát CA a algoritmus, kterým se podepisuje držitel tohoto certifikátu

nemusí být shodné, certifikát může potvrzovat platnost ověřovacího klíče pro algoritmus DSS a vlastní certifikát může být podepsán algoritmem RSA. Certifikační cestu může tvořit posloupnost takto „nekonzistentních“ certifikátů, certifikáty podepsané jedním algoritmem mohou certifikovat klíč pro jiný algoritmus.

2.8 Ostatní procesy a služby správy klíčů a certifikátů PKI

Mezi procesy odehrávající se v iniciální etapě životního cyklu certifikátů a klíčů patří procesy registrace, generování klíčů, vytvoření certifikátu a předání certifikátu žadateli, diseminace certifikátu a zálohování klíčů.

Registrace

Ověřuje se identita žadatele o certifikát. Za registraci je odpovědná CA nebo nějaká jí podřízená registrační autorita (RA). Náročnost ověření předpisuje certifikační politika (CP) a certifikační prováděcí směrnice (CPS). Pojmy RA, CP a CPS blíže rozvádějí následující kapitoly o autoritách PKI a dokumentové základně CA.

Generování klíčů

Generují se párové hodnoty klíčů ASK. Hodnoty mohou být vygenerovány s předstihem a nebo se generují přímo v procesu registrace. Klíče může generovat prohlížeč žadatele o certifikát, RA, CA nebo nějaká další třetí důvěryhodná strana. Umístění generátoru klíčů je ovlivněno aplikovanými výkonnostními, funkčními, bezpečnostními a legislativními omezeními a rovněž zamýšleným použitím klíčů. Jestliže má PKI podporovat nepopiratelnost, měl by si klíče generovat klient sám; generovat je může i dostatečně důvěryhodná CA. Generování klíčů je poměrně náročný proces a proto mnohdy bývají generovány ve výkonných stanicích CA. Na generování klíčů v rámci PKI mohou kladeny různě silné bezpečnostní požadavky, typickým a velmi široce používaným kritériem bezpečnosti procesu generování klíčů je (US) standard FIPS 140-1 (Federal Information Processing Standard).

Vytvoření certifikátu a předání certifikátu žadateli

Proces vytvoření certifikátu je předmětem činnosti autorizované CA. Pokud certifikované klíče negeneruje přímo taková CA, musí být provozován odpovídajícím způsobem bezpečný komunikační kanál pro předání certifikovaného klíče této CA. Pokud si klíče negeneruje žadatel, musí být provozován i dostatečně bezpečný kanál pro předání generovaného soukromého klíče.

Diseminace certifikátů

Zpřístupňování vydaných certifikátů jejich uživatelům se může odehrávat off-line předáváním certifikátů mimo přímé komunikační kanály aplikace používající certifikáty (out-of-band), vystavením vydaných certifikátů ve vhodně on-line dostupné bázi dat, resp. v repositáři vydaných certifikátů nebo v rámci komunikačních protokolů aplikace, která se na použití certifikátů spoléhá (in-band), jak to např. činí systém bezpečné elektronické pošty S/MIME.

Zálohování klíčů

Zálohování klíčů je volitelný proces, vesměs prováděný vhodnou třetí důvěryhodnou stranou a jeho provádění v PKI podporující nepopiratelnost by muselo být explicitně povolenou příslušnou legislativou, což ale není dobrá cesta. V ostatních typech PKI může zálohování provádět CA, která např. klíče vydala, nebo některá jiná třetí důvěryhodná strana. Zálohování klíčů má být děláno s cílem dosažení dobrých obchodních praktik, nikoli s cílem prosazení práva nebo zájmů státu. Techniky a procesy typu „Key Escrow“ jsou samostatnou kapitolou ve sféře aplikovatelnosti ASK, které v tomto tutoriálu ponecháváme stranou.

Mezi procesy odehrávající se v etapě používání vydaných certifikátů patří procesy získání certifikátu, validace certifikátu, zotavení zálohovaného klíče a automatické aktualizace klíče a certifikátu. Proces validace certifikátu jsme už podrobili hlubšímu zkoumání.

Získání certifikátu

Certifikát si uživatel zpřístupňuje v případech, když potřebuje šifrovat data zasílaná jinému subjektu, ověřit podpis jiného subjektu, případně ověřit jeho autorizaci na základě certifikovaných atributů jiného subjektu. Možné způsoby získávání certifikátů jsou dány způsobem jejich diseminace.

Zotavení zálohovaného klíče

Jedná se o komplementární proces k procesu zálohování klíčů. Opětovné získání kopie zálohovaného klíče je vesměs aplikovatelné pouze v případě šifrovacích certifikátů. Zálohování a zotavování podepisovacích klíčů by bylo vůči požadavkům na nepopiratelnost kontraproduktivní.

Automatická aktualizace klíče a certifikátu

Automatická aktualizace klíče a certifikátu se odehrává „těsně“ před vypršení expirační doby certifikátu. Jejím cílem je vygenerování nové párové dvojice klíčů a vydání příslušného certifikátu. Přirozeným požadavkem držitele certifikátu je, aby proces automatické aktualizace byl vůči němu transparentní. Co znamená „těsně“ je diskutabilní, obvykle to znamená ne dříve než po uplynutí 75% doby platnosti právě platného certifikátu (a klíče).

Ve fázi rušení certifikátu se odehrávají procesy vyvolané uplynutím expirační doby, revokace certifikátů a archivace klíčů a certifikátů. Proces revokace jsme už podrobili hlubšímu zkoumání.

Uplynutí expirační doby

Po uplynutí expirační doby certifikátu se obvykle volí jedna z následujících variant dalšího postupu: [1] dosavadní držitel certifikátu přestává být členem komunity subjektů obhospodařovaných danou PKI, [2] dosavadnímu držiteli se vydá nový obnovený certifikát se stejnou certifikovanou hodnotou (ověřovacího klíče) a s nově definovanou dobou platnosti, tzv. „certificate renewal“, prolongace certifikátu, a nebo [3] dosavadnímu držiteli se vydá nový aktualizovaný certifikát s novou certifikovanou hodnotou (ověřovacího klíče) a s nově definovanou dobou platnosti, tzv. „certificate update“, aktualizace certifikátu. Prolongace certifikátu je jiný proces než aktualizace certifikátu. Prolongace zachovává původní párová klíčová data, aktualizace ne. Předností prolongace, za předpokladu zachování

dostatečné odolnosti proti kryptoanalytickému útoku, je zachování do doby prolongace používaného provozního prostředí. Automatická aktualizace certifikátů je bezpečnější, její uplatnění však vyvolává nezanedbatelné zvýšení režie.

Archivace klíčů a certifikátů

Motivačním faktorem pro uchovávání historie klíčů je hrozba další nedostupnosti šifrovaných dat po uplynutí expirační doby šifrovacího certifikátu a jím certifikované hodnoty klíče. Klíčové materiály v případě existence takového rizika, tj. jde především hodnotu dešifrovacího soukromého klíče, je nutné bezpečně uchovávat s cílem možnosti následného zotavení hodnoty uchovaného klíče. Historie klíčů se často uchovává v lokalitě jejich vlastníka, někdy tuto službu poskytuje CA nebo jiná důvěryhodná třetí strana. Někdy se zvlášť vyzdvihuje dlouhodobá paměť klíčového materiálu a hovoří se „archivu klíč“ jako o samostatné entitě odlišné od „historie klíčů“. Pod pojmem archivu klíčů se pak rozumí sofistikovanější dlouhodobě uplatnitelná služba typicky poskytovaná třetí důvěryhodnou stranou mnohdy doplňovaná o notarizaci, časové razítkování, archivaci a zotavování historií klíčů u koncových uživatelů, s možností auditu apod.

3 Více o autoritách PKI

Certifikační autority patří mezi entity bezpečnostních struktur, které označujeme jako *poskytovatele důvěryhodných služeb TSP* (Trusted Service Provider). TSP jsou prvky bezpečnostní infrastruktury, které vztah důvěry mezi ostatními zúčastněnými stranami (podepisující osoba a ověřovatel podpisu, odesílatel a příjemce důvěrné zprávy atd.) pomáhají budovat. Podporují ustanovení vztahu důvěry mezi zúčastněnými stranami poskytováním potřebných podpůrných služeb – vydávají certifikáty, podporují křížové uznávání certifikátů, generují časová razítka, udržují a vydávají seznamy neplatných certifikátů, umožňují on-line zpřístupňování stavu certifikátů, udržují a vydávají seznamy neplatných atributových certifikátů atd.

Důvěryhodnost TSP je dána především deklarovanou, dostupnou a uznávanou politikou TSP. *Politikou TSP* rozumíme množinu pravidel pro plnění poskytovaných služeb a metodiku pro hodnocení bezpečnosti používaných produktů či systémů. Po pozitivně hodnocení způsobu uplatnění deklarovaných pravidel se poskytované služby považují za bezpečné (důvěryhodné). Politiky TSP vystupujících v soudobých PKI obvykle musí vyhovovat nějakým standardním bezpečnostním požadavkům (např. ověřeně splňují předem stanovený „Protection Profile“ podle normy ISO/IEC 15408 / Common Criteria for Information Security Evaluation).

3.1 Přehled autorit PKI

V PKI se využívají služby především těch typů TSP, které jsou v následujících odstavcích uvedeny následujícím výčtem:

1. *Certifikační autorita*, CA – vydává certifikáty žadatelům o vydání certifikátu.
2. *Registrační autorita*, RA (Registration Authority) – obstarává pro nějakou(é) CA prověření identifikace a provádí registraci entit požadujících certifikát.
3. *Atributová autorita, AA* (Attribute Authority) – přiděluje privilegia (autorizace) uživatelům vydáváním atributových certifikátů.
4. *Repositář* – publikuje seznamy certifikátů, seznamy revokovaných certifikátů, seznamy revokovaných atributových certifikátů, ARL (Attribute certificate Revocation List), politiky TSP apod.

5. *Vydavatel certifikačních politik*, *PMA* (Policy Management Authority) – definuje technické a procedurální požadavky na vytváření a ověřování digitálních certifikátů pro potřeby nějaké třídy aplikací, resp. skupiny uživatelů.
6. *Schvalovatel certifikačních politik*, *PAA* (Policy Approving Authority) – provádí hodnocení politik a vypracovává jejich „hodnotící zprávy".

Aplikace, které využívají služeb PKI mohou ale požadovat služby poskytované sofistikovanějšími typy TSP, jakými jsou např. *elektronický notář* potvrzující existenci jisté datové zprávy před udanou dobou, *časová autorita, TSA* (Time Stamping Authority), vydávající časová razítka k dokumentům a/nebo k digitálním podpisům, *vydavatel podepisovacích politik, SPA* (Signature Policy Authority), který definuje technické a procedurální požadavky na vytváření a ověřování digitálních podpisů pro potřeby nějaké třídy aplikací.

Některé TSP (např. CA, RA, AA, repositář) mohou plnit svoji funkci jak v rámci jedné organizace, tak i v různě uspořádaných globálních strukturách podle potřeb aplikací, které služeb TSP využívají. Mohou působit uvnitř organizace nebo vně organizace. CA působící uvnitř organizace vesměs vydávají digitální certifikáty používané pro řízení přístupu ke zdrojům organizace. CA působící vně organizace vesměs vydávají digitální certifikáty osobám, které potřebují provádět bezpečné on-line transakce a podepisovat elektronickou poštu a dokumenty, vyměňované mezi zúčastněnými stranami, působícími v různých doménách. Mezi CA, působícími vně organizací, může být zaveden takový vztah vzájemné důvěry, který umožňuje uplatňovat křížové uznávání certifikátů různých CA.

Pro implementaci repositáře (revokovaných) certifikátů se vesměs využívá některá z forem distribuovaných bází dat, např. systém adresářových služeb X.500 Directory. V poslední době se ukazuje, že služby typu X.500 jsou těžkopádně implementovatelné a repositáře bývají proto často implementovány nějakým již existujícím databázovým systémem a přístup k nim se řídí jednodušší verzí základního protokolu služeb X.500 označovanou jako *LDAP* (Lightweight Directory Access Protocol).

PKI je velmi vhodným prostředím pro implementaci silnější služby autentizace, než je služba autentizace založená na pouhém uvádění jména a hesla. Službu autentizace zpřístupňují otevřenější komunitě než speciální autentizační systémy typu Kerberos. Pokud se autentizace realizuje stejným komunikačním kanálem, jako odpovídající transakce, která autentizaci požaduje, hovoříme o „in-band" autentizaci (výměny autentizačních zpráv sdílí komunikační šířku pásma s výměnami transakčních zpráv). Autentizace na bázi tradičních metod realizovaná mimo komunikační kanál použitý vlastními transakcemi požadujícími autentizaci (např. telefonicky nebo osobní přítomností) se označuje jako „out-of-band" autentizace. Cílem každé PKI je potřebu „out-of-band" autentizace minimalizovat. Odstranit ji úplně z principiálních důvodů zřejmě nebude možné nikdy. Osoba, která chce PKI použít, musí mít svoji identitu a/nebo atributy počátečně prověřeny některou CA. Počáteční prověření nelze provádět prostřednictvím PKI, protože v ní neexistuje žádná CA, která by za identitu žadatele či atributy dala garance. „Zavlékací" (bootstrapping) proces důvěryhodného prověřování vždy požaduje nějakou formu „out-of-band" autentizace a jednotlivé typy PKI se odlišují požadovaným rozsahem „out-of-band" autentizace podle toho, jak silnou nevyvratitelnost certifikace provozovatelé PKI chtějí poskytovat. Problém dosažení požadované úrovně nevyvratitelnosti má mnoho právních, sociálních a technických důsledků včetně kladení požadavků na to, jak držitelé certifikátů musí se svými soukromými klíči zacházet.

3.2 Certifikační a registrační autorita

Jestliže CA současně vystupuje i v roli repositáře CRL, není vyloučena možnost provedení obtížně prokazatelné podvodné modifikace CRL takovou CA. Řešení uvedených problémů se usnadní, když se role v PKI oddělí a CA a RA a přijmou dodatečná opatření zabraňující zpětné manipulaci s již publikovanými CRL (např. veřejně dostupným a periodicky publi-

kovaným řetězením charakteristik postupně vydávaných verzí CRL získávaných aplikací kryptografických hašovacích funkcí).

Pokud registraci žadatele o certifikát neprovádí přímo CA, řešení požadavku na vydání certifikátu může zahájit některá RA podřízená dané CA, do ranku jejíž působnosti žadatel patří. RA se ustanovuje především tehdy, když je žádoucí oddělit odpovědnost za důvěryhodnost obsahu certifikátu a důvěryhodnost vydání vlastního certifikátu. RA může být reprezentována fyzickou osobou, úřadem, případně i nějakým automatizovaným procesem. Výsledkem registrace u RA bývá, kromě ověření identity a platnosti certifikovaných vlastností, vydání nějakého registračního tajemství, kterým se žadatel posléze prokazuje nadřazené CA. Požadavky na kvalitu a formu činnosti RA/CA stanovuje *certifikační politika CA*. O certifikačních politikách se podrobněji zmiňujeme níže.

Princip možné souhry CA, RA a autority odpovědné za udržování repositářů lze ilustrovat příkladem výčtu základních kroků prováděných při vyžádání šifrovací karty (příklad je převzat ze systému *Fortezza*). Jedná se o šifrovací kartu typu PCMCIA, která bezpečným způsobem uchovává privátní klíč uživatele, certifikát vydavatele karty, veřejné klíče potřebné pro kryptografii apod. Karta provádí digitální podepisování, generuje charakteristiky, šifruje a dešifruje a řeší protokoly výměny klíčů. Lze ji použít v součinnosti s celým systémem Fortezza pro přímé šifrování souborů a/nebo přenášených zpráv a obsahu médií, pro řízení přístupu, pro silnou autentizaci spojením principů „znám“ a „mám“. Kroky prováděné při vyžádání karty jsou následující:

1. Žadatel zašle svůj požadavek vhodné RA podléhající CA regionu žadatele. RA plní roli „notáře“, certifikáty uživatelů ani nepodepisuje, ani nevydává, pouze pomáhá své CA jednak při registraci uživatelů a posléze při distribuci karet.
2. RA žadateli přidělí ve spolupráci s autoritou zabezpečující provoz repositářů identifikaci (rozlišitelné symbolické jméno podle uplatněné metodiky identifikace). V repositáři jsou uloženy certifikáty (splňující doporučení X.509) a CRL. Repositář je připojen k Internetu pomocí silného autentizačního systému.
3. Autorita zabezpečující provoz repositářů vytvoří v repositáři potřebný databázový záznam.
4. RA předá kompletní prověřený požadavek na vydání certifikátu své CA
5. CA vygeneruje klíče (kryptografický materiál) a certifikát.
6. CA zašle certifikát do repositáře
7. CA doručí kartu Fortezza RA a její PIN zašle žadateli přímo.
8. Kartu doručí žadateli RA.

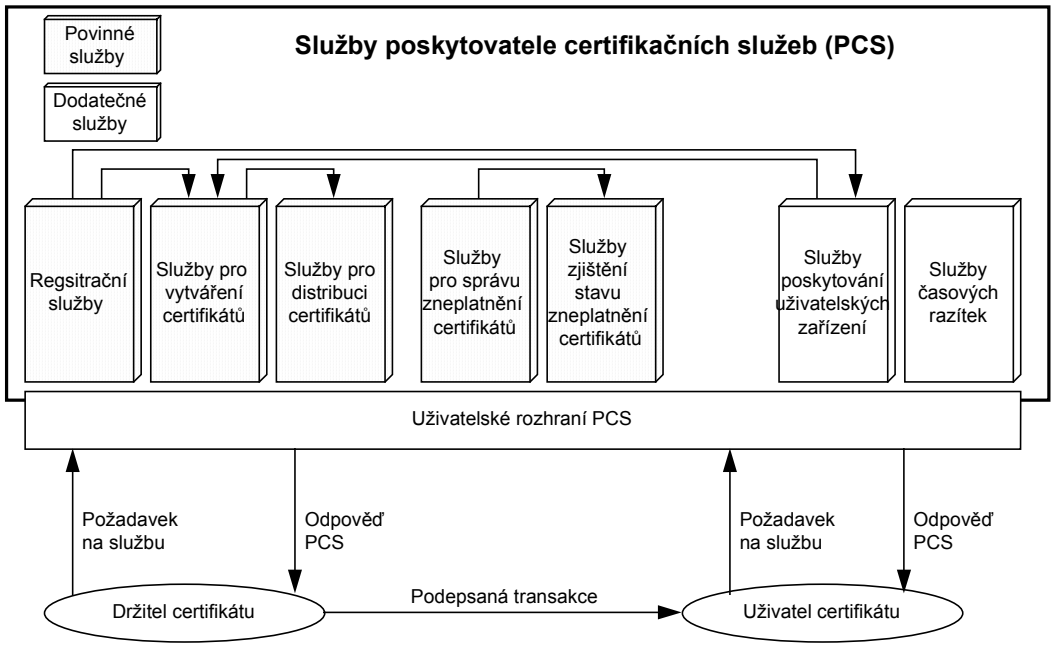
Na vybavenost CA (na její pracovní stanici) jsou kladeny nadřazeným PMA vyšší požadavky na bezpečnost – např. použitý OS musí splňovat (podle TCSEC) požadavky třídy B1 (např. SCO/Secureware CMW Trusted OS). Při implementaci na procesorech typu Motorola se cena celého systému pohybuje na hladině cca 15 až 20000 USD. CA zajišťuje rovněž službu odvolání platnosti certifikátů. CA podléhají společnému PMA, který jednotlivé CA zřizuje a navíc poskytuje službu správy kompromitovaných klíčů (v případech, kdy uživatel ztratil kontrolu nad PIN nebo kartu a stal se hrozbou pro bezpečnost systému). Na činnost PMA dohlíží nadřazený PAA.

Uplatnění zásady nevyvratitelnosti certifikace nesmí přitom zamezit používání PKI aplikacemi, které požadují zachování požadované úrovně anonymity (způsobilost používat PKI při odhalování pouze informací relevantních pro dané použití). PKI musí podporovat jak přísnou nevyvratitelnou autentizaci, tak i možnost ochrany soukromí prostřednictvím služeb zachovávajících anonymitu. Způsob poskytování služeb se zachováním anonymity držitele certifikátu při udržení potřebné úrovně nevyvratitelnosti má CA definován ve své politice poskytování certifikačních služeb.

3.3 Vnitřní struktura certifikační autority

Certifikační autorita (obecně poskytovatel certifikačních služeb, PCS) se skládá z několika služeb. Tyto služby se dělí na *povinné služby*, které musí implementovat každý PCS a *dodatečné služby*, které není nutno implementovat.

Povinné služby zahrnují registrační služby, služby pro vytváření certifikátů, služby pro distribuci certifikátů, služby pro správu zneplatnění certifikátů a služby zjištění stavu zneplatnění certifikátů. Dodatečné služby obsahují služby poskytování uživatelských zařízení a služby časových razítek. Struktura služeb PCS a jejich vazby jsou znázorněny na Obr. 4.



Obr. 4 Služby poskytovatele certifikačních služeb

4 Dokumentová základna CA

Základními formami vyjádření politiky činnosti CA jsou *certifikační politika, CP* (Certificate Policy) a *certifikační prováděcí směrnice, CPS* (Certificate Practice Statement). Tyto dokumenty tvoří bázi pro zavedení důvěry mezi různými CA a následně bázi pro křížové uznávání certifikátů vydaných různými CA.

Vztah důvěry mezi všemi třemi účastníky PKI (CA, držitel certifikátu a uživatel certifikátu), kteří jsou samostatnými entitami, se přirozeně zavádí jinak v případech, kdy je CA, na kterou se žadatel o certifikát obrací, současně i žadatelovým zaměstnavatelem a potenciální uživatelé certifikátů jsou zaměstnanci téže organizace, a jinak v případech, kdy nějaká CA vydává široce používané certifikáty komukoliv. Mimo jiné jde i o to, aby mohla jedna CA upřesnit svoji důvěru v jinou CA např. tak, že jí důvěřuje jen z hlediska certifikací jistého druhu – „důvěřuji jen těm certifikátům vydaným CA_N, které vážou hodnotu veřejného klíče s adresou elektronické pošty“. Navíc, toto upřesnění by mělo být vyjádřeno tak, aby konformitu vůči takové politice bylo možné potvrzovat automaticky.

Politiky činnosti CA proto musí být vyjadřovány explicitně, aby mohly být auditovatelné a hodnotitelné, a to pokud možno co nejformálnějším způsobem, aby mohly být prověřovány automaticky. Při jejich vytváření je potřeba mít na paměti, že PKI není nástroj pro

ustanovení a dosažení plné vzájemné důvěry mezi entitami, PKI je pouze nástroj pro vyjádření existujících vztahů důvěry.

4.1 Iniciativa NIST – Protection Profile CIMS

Stanovení politik TSP je v současné době předmětem intenzivního vývoje. Například v rámci vývoje NIST PKI (Certificate Issuing and Management Components, Protection Profile, NIST PKI Project Team, 5/5/00) byl v květnu 2000 vydán návrh „Protection Profile“ (implementačně nezávislá definice požadavků na bezpečnost IT pro jistou kategorii produktů nebo systémů) autorit vydávajících digitální certifikáty splňující požadavky normy ISO/IEC 15408 (Common Criteria). Podle tohoto návrhu jsou vydávání, odvolávání platnosti a celková správa certifikátů a informací o stavu certifikátů předměty činnosti *systému pro vydávání a správu certifikátů, CIMS* (Certificate Issuing and Management System).

CIMS vždy obsahuje CA, jeho součástí mohou být i RA a některé další komponenty. CIMS je systém, je tvořen software, hardware a firmware. Zmíněný „Protection Profile“ se nezabývá ani definicí fyzického prostředí provozování (řízení přístupu, klimatizace, ...), ani definicí administrativních nebo procedurálních či personálních opatření. Definuje pouze požadavky na funkčnost CIMS a na zaručitelnost předem dané úrovně bezpečnosti CIMS. Implementace CIMS není předmětem této definice. Pro pochopení problematiky politik předpisujících účinnou činnost CA jsou ale zajímavé právě jeho definice možných úrovní záruky za bezpečnost. Na jejich dosažení se CP a CPS podílejí nepominutelným způsobem:

1. *CIMS bezpečnostní úrovně 1* poskytuje nejnižší úroveň bezpečnosti. Je určen pro provozování v prostředí s malým rizikem hrozeb zlomyslných činností. Není chráněn před odhalováním důvěrných informací zlomyslnými nebo neautorizovanými uživateli. Smí používat pouze standardní schválené kryptografické algoritmy. Použité kryptografické produkty musí být certifikované na nejnižší definované (1.) úrovni záruky za bezpečnosti. Musí mít definovány alespoň dvě samostatné role, jedna se zabývá správou účtů, generováním klíčů a auditem a druhá se stará o vydávání a odvolávání platnosti certifikátů. Pro implementaci lze použít běžně komerčně dostupné produkty.
2. *CIMS bezpečnostní úrovně 2* poskytuje základní úroveň bezpečnosti. Je určen pro provozování v prostředí, ve kterém nejsou signifikantní rizika a následné škody odhalením důvěrných informací. Musí být chráněn před většinou útoků vedených ze síťového prostředí. Smí používat pouze standardní schválené kryptografické algoritmy. Použité kryptografické produkty musí být certifikované na základní (1.) úrovni záruky za bezpečnosti. Musí mít definovány alespoň dvě samostatné role, jedna se zabývá správou účtů, generováním klíčů a auditem a druhá se stará o vydávání a odvolávání platnosti certifikátů. Pro implementaci lze použít produkty dodávané při splnění nejlepších komerčních praktik.
3. *CIMS bezpečnostní úrovně 3* poskytuje střední úroveň bezpečnosti. Je určen pro provozování v prostředí, ve kterém existují nepominutelná rizika a následné škody odhalením důvěrných informací a ztrátou integrity dat. CIMS bezpečnostní úrovně 3 musí provádět dodatečné integritní kontroly, aby se zajistila ochrana dat proti neautorizované modifikaci, musí používat opatření proti hrozbám plynoucím z fyzického přístupu ke komponentám CIMS a kladou se dodatečné požadavky na bezpečnost implementované funkcionality. Musí provozovat opatření proti zlomyslným autorizovaným uživatelům a proto musí mít definovány alespoň tři samostatné role – jedna se zabývá správou účtů, generováním klíčů a auditem, druhá se stará o vydávání a odvolávání platnosti certifikátů a třetí udržuje auditní záznamy. Všechny zprávy v rámci činnosti CIMS musí být podepisovány. Použité kryptografické produkty odpovědné za dlouhodobou ochranu soukromých klíčů, podepisování a odvolávání

platnosti certifikátů musí být certifikované na střední (2.) úrovni záruky za bezpečnosti. Pro implementaci lze použít požadovaným způsobem metodicky testované a kontrolované produkty a metodicky navrhované, testované a zkoumané produkty (podle CC kritérií). CIMS bezpečnostní úrovně 3 jsou zřejmě systémy vhodné pro implementaci PKI v nejbližších příštích letech.

4. Existuje ještě definice *CIMS bezpečnostní úrovně 4*, nepředpokládá se však, že by produkty této bezpečnostní úrovně byly v několika příštích letech dostupné. Jsou zamýšleny pro vysoce riziková „nepřátelská“ prostředí, ve kterých budou vystupovat „nepřátelští“ uživatelé. CIMS bezpečnostní úrovně 4 musí mít definovány 4 role, ke třem předchozím přistupuje další samostatná role odpovědná za zálohování. Auditní záznamy musí být podepisované třetí důvěryhodnou stranou časovým razítkem. Pro implementaci lze použít požadovaným způsobem metodicky navrhované, testované a zkoumané produkty a semi-formálně navrhované a testované produkty (podle CC kritérií).

4.2 Certifikační politika (CP)

Certifikační politika, CP je identifikovatelnou množinou pravidel určujících

1. účel, pro který lze certifikáty/certifikované veřejné klíče vydávané danou CA používat
2. podmínky za kterých lze tyto certifikáty a certifikované klíče používat
3. meze použití těchto certifikátů a klíčů
4. algoritmy, praktiky, metody, které CA při vydávání certifikátů používá (odkazem na CPS).

Použitou CP musí uznávat jak žadatelé o vydání certifikátu, tak uživatelé vydaných certifikátů. CP vymezuje třídu činností v rámci komunity distribuovaného systému, ve které se uplatňují shodné bezpečnostní požadavky (např. výměna klasifikovaných dat jisté klasifikační třídy nebo elektronický obchod se zbožím vymezené cenové kategorie). Uznávané CP musí být identifikovány a v certifikátu musí být uveden identifikátor CP, kterou CA při vydání certifikátu splňovala. Pokud se aplikace používající certifikáty musí chránit před chybným použitím certifikátu, musí mít možnost identifikátor CP prověřovat. Taková aplikace musí znát, kterou CP pro svoji činnost požaduje.

Standard X.509 umožňuje v certifikátech uvádět i způsoby vzájemného zobrazování CP, což usnadňuje implementaci procesu křížového uznávání certifikátů. CP lze kvalifikovat (detailně upřesňovat např. odkazy na CPS a na další dokumenty dokumentové základny, jakými jsou např. havarijní plán nebo systémová bezpečnostní politika použitého IS). V rámci dané komunity musí být množina akceptovaných CP definována veřejně. Pokud to účely používání certifikátů vyžadují, musí CP respektovat odpovídající právní normy.

Systém CP bývá uspořádán obvykle do vhodných (případně i hierarchických) soustav, např. *CP identifikačních certifikátů*, *CP šifrovacích certifikátů* atd.

Každou z uvedených kategorií CP lze dále členit podle síly záruky důvěryhodnosti certifikátu např. na

1. *elementární CP* – vydané certifikáty lze použít pro autentizaci WWW klientů na WWW serverech, neposkytuje se žádná podpora služby nepopiratelnosti
2. *CP se základní zárukou důvěryhodnosti* – podpora aplikací vystavených malým rizikům, vydaný certifikát je vhodný např. pro šifrování dat určených pouze pro vnitřní potřebu organizace, resp. pro podepisování finančních transakcí do výše 10 000 Kč; žadatel se ani nemusí registrovat u CA osobně a ani si nemusí osobně certifikát vyzvedávat; žádost o vystavení certifikátu může být podána elektronicky a CA si udané informace o totožnosti žadatele neověřuje, pouze všemi dostupnými prostředky zjišťuje platnost e-mailové adresy uvedené v on-line podané žádosti)
3. *CP se střední zárukou důvěryhodnosti* – podpora aplikací vystavených středním rizikům, vydaný certifikát je vhodný např. pro šifrování důvěrných dat organizace, resp.

pro podepisování finančních transakcí do výše 1 000 000 Kč; žadatel se musí registrovat osobně jako fyzická osoba, nikoli jako člen organizace, a osobně si musí certifikát vyzvedávat; CA si informace o totožnosti žadatele může ověřovat a musí je např. podepřeny dobrozdáním třetí nezávislé strany; CA musí používat certifikované softwarové kryptografické moduly

4. *CP s vysokou zárukou důvěryhodnosti* (podpora aplikací vystavených vysokým rizikům, vydaný certifikát je vhodný např. pro šifrování vysoce důvěrných dat organizace a pro finanční transakce bez omezení výše; uživatel se musí registrovat osobně jako fyzická osoba, ne jako člen organizace, a osobně si musí certifikát vyzvedávat; CA si informace ozřejmující totožnost žadatele může ověřit, musí být proto podepřeny dobrozdáním třetí nezávislé strany; žadatel musí předložit pro prokázání totožnosti alespoň 2 dokumenty, přičemž alespoň na jednom musí být fotografie žadatele; CA musí vést o provedených kontrolách identity auditovatelné záznamy; CA musí při podepisování používat certifikované autentizační kryptografické moduly a hardwarové kryptoprocesory).

Bez ohledu na to, zda certifikát obsahuje pouze identifikaci držitele klíče nebo nějaká jeho specifická autorizační data, CA musí žadatele o certifikát před vydáním certifikátu identifikovat. On-line vydávání certifikátů s vyšší zárukou důvěryhodnosti než představuje její základní úroveň je možná pouze tehdy, když CA s žadatelem sdílí nějaké tajemství a bezpečný kanál, kterým lze znalost tajemství prokázat (např. komunikací pomocí SSL). I když CA zajistí dostatečně důvěryhodné prověření identity žadatele, musí vyřešit další problém: je žadatel skutečně držitelem soukromého (podepisovacího) klíče, který odpovídá certifikovanému veřejnému klíči (řešení může spočívat např. v podepsání nějaké výzvy).

4.3 Certifikační prováděcí směrnice (CPS)

Certifikační prováděcí směrnice, CPS, říká, jak CA vede seznam uživatelů, kterým vydala certifikát a jak je CA řízena. Specifikuje praktiky, postupy, algoritmy, metody, které CA používá při vydávání certifikátů. CP, kterými se CA řídí, jsou přímo závislé na přísnosti, bezpečnosti jejích procesů. CPS obsahuje definici kritérií bezpečnosti nástrojů používaných CA, definici kritérií personální bezpečnosti (role, separace jejich povinností a odpovědností apod.) a specifikuje technická a procedurální bezpečnostní opatření CA.

CP je typicky vytvářena na abstraktnější úrovni než CPS. CPS je psána z hlediska perspektivy provádění správy certifikátů. Popisuje použité praktiky infrastruktury správy certifikátů, které podporují vytváření důvěryhodných certifikátů. Popisuje, jak je podporováno vytváření certifikátů z hlediska dosažení požadované záruky za integritu a důvěrnost. CA musí mít jednu CPS, ale může vyhovovat více CP. CA může CPS diferencovat podle požadovaných praktik jednotlivými CP. Různé CA mohou podporovat stejnou CP, mohou mít ale různé CPS. (To ovšem může způsobovat obtíže při křížovém uznávání certifikátů.) V rámci dané komunity, by měla být množina použitelných CPS definována explicitně.

Návrháři PKI musí při stanovování generických (někdy i závazných) vzorů CP/CPS stanovit základní charakteristiky PKI, mezi které, jak vyplývá z výše uvedeného výkladu, určitě patří definice:

1. Dat, která certifikát obsahuje (Je předmět certifikace definován nebo může certifikát obsahovat jakýkoliv typ informací?)
2. Typů certifikátů, které PKI podporuje (Identifikační, šifrovací, atributové?)
3. Uspořádání CA (Striktně hierarchicky, síťově nebo kombinovaně?)
4. Vztahů mezi držitelem certifikátu, CA a uživatelem certifikátu (Jedná se o různé entity? Jak dobře se vzájemně znají? Je nějaký konkrétní vztah mezi žadatelem o certifikát a CA vydávající certifikát obligatorní?)
5. Vztahů důvěry mezi držitelem certifikátu, CA a uživatelem certifikátu (Čím se vyjadřuje požadovaný stupeň vzájemné důvěry? Kdo přebírá odpovědnost za důvěryhodnost v různých situacích?)

6. Metody, která se použije při prokazování platnosti certifikátů (Jestliže se ověřuje on-line, pak při každém použití certifikátu nebo jen když certifikát definuje požadovanou minimální periodu ověřování? Jestliže off-line, jak budou vydávány odpovídající CRL?)
7. Metody, která se použije při odvolávání platnosti certifikátů (On-line nebo pomocí CRL? Pokud se použijí CRL, jak bude řešen problém časové granularity a problém rozměru CRL? V jakém vztahu bude doba platnosti CRL a doba platnosti certifikátu CRL?)
8. Úrovně nepopiratelnosti, kterou PKI z hlediska autentizace podporuje (Může PKI prokázat že daný podpis byl skutečně proveden konkrétním subjektem?)
9. Důvěryhodnosti prokázání identity a certifikovaných vlastností, jak je žadatel o certifikát musí prokázat (Jaký se požaduje rozsah a jaká je důvěryhodnost „out-of-band" autentizace žadatele? Podporuje PKI anonymitu?)

CP a CPS musí pokrýt oblasti, jejichž výčet zavádí např. široce uznávaný materiál RFC 2527, [2]. Definicí standardizovaných CP a CPS pro danou komunitu se obvykle zabývá odpovídající vydavatel certifikačních politik, PMA. Vydavatel certifikačních politik je přirozeně nadřazen všem CA, vč. případných kořenových CA, které v oblasti jeho působnosti provozují svoji činnost. Typicky se jedná o výbor reprezentantů zúčastněných stran, resp. nějaký úřad podléhající příslušnému ministerstvu, pokud se jedná o PKI státní správy. Do PMA bývají kooptování specialisté – experti z oblastí, se kterými PKI souvisí (právo, soukromí, technologie). PMA obvykle definuje vzorovou CP, CPS a CP pro křížové certifikace s PKI externích domén. Ve světě na úrovni státní správy PMA úzce spolupracují s poradními skupinami sdružujícími přední reprezentanty potřebných průmyslových odvětví (Netscape, Verisign, ...). PMA může reprezentovat několik problémových podokruhů, např. PMA v oblasti veřejné moci v ČR by měl být jeden s tím, že jeho roli z hlediska kompatibilního upřesňování CP a CPS pro jednotlivé podokruhy (armáda, zdravotnictví, vnitro) převezmou případné kořenové CA působící v daných oblastech. Tyto kořenové CA pak mohou např. přebrat i roli dlouhodobých skladišť (repositářů) certifikátů. PMA stanovuje povinnosti jemu podřízených CA. Typicky se jedná např. o stanovení úrovně klasifikace, na které smí CA vydávat certifikáty, maximální doby platnosti certifikátu, maximální doby platnosti klíčů, doby platnosti CRL atd. Politiky vypracované PMA mohou být v rámci působností dané PKI schvalovány nezávislým posuzovatelským orgánem, PAA. PAA mívá charakter sboru „starších" (bezpečnostních specialistů a zástupců vrcholových managementů organizací, kterých se použití PKI dotýká).

4.4 Příklad struktury CP a CPS

Certifikační politika modelové PKI musí vymezit kvalitu a způsob realizace poskytovaných služeb, při zachování možnosti křížové certifikace a potřebné dostupnosti, alespoň z oblastí

1. Generování klíčů, jejich skladování a obnovy
2. Generování a aktualizací certifikátů
3. Revokace certifikátů
4. Kontrola platnosti certifikátů
5. Správa repositářů
6. Řízení přístupu a všeobecná autorizace
7. Audit
8. Správa konfigurace
9. Archivování
10. Obnova po havárii

Pro zajištění bezpečnosti takových služeb musí CP stanovit požadavky na

1. Přípustné způsoby identifikace a autorizace žadatelů o certifikát
2. Použité počítače/operační systémy a kryptografické systémy
3. Provozování počítačů a kryptografických systémů
4. Používání certifikátů jejich držiteli a jejich uživateli
5. Pravidla vymezující odpovědnosti a podporující vysoký stupeň jistoty specifikovaná politika byla skutečně implementována.

Rámcové zadání úlohy vypracovat CP lze souhrnně vyjádřit následujícími body:

1. Ustanovený PMA musí stanovit metodiku hodnocení CP a cílové úrovně záruky za bezpečnost, které musí implementace CP pro jednotlivé typy autorit PKI dosáhnout
2. Vypracovaná CP musí konkrétně stanovit komunitu, pro kterou je CP závazná a kde a jak je CP možno uplatnit
3. CP stanoví role, autority PKI – PAA, PMA, CA, RA, případně auditoři a AA, a role koncových uživatelů – držitel certifikátu, uživatel certifikátu. Stanovením rolí se rozumí především definice povinností (CA, RA, žadatele, uživatele, repositářové autority apod.) a omezení kladených na přidělení rolí
4. CP musí ošetřit i případy vydávání certifikátů žadatelům z jiných sfér
5. CP musí stanovit formu publikací informací o CA (např. jejího certifikátu) a informací generovaných CA, periody korekcí takových publikací a pravidla řízení přístupu k těmto informacím
6. CP musí stanovit způsob provádění auditu (periodu, potřebnou kvalifikaci auditora, co se audituje, kdo a jak je seznamován s výsledky auditu)
7. CP musí deklarovat politiku ochrany důvěrných informací
8. CP může vymezit typ transakcí, pro které platí, že jimi používané certifikáty musí danou CP splňovat, případně vyjmenovat konkrétní celé aplikace. CP deklaruje úroveň záruky za bezpečnost vydávaných certifikátů, faktory vymezující použitelnost certifikátů, hodnoty informačních aktiv, se kterými lze pomocí certifikátů vydaných CA splňujících navrženou CP manipulovat, potenciální hrozby a rizika, akceptovatelné úrovně ochrany provozních prostředí a možné úrovně poskytované záruky podle požadavků odvozených z klasifikace manipulovaných dat.
9. Zvláště velkou pozornost musí CP věnovat problematice identifikace a autentizace. Musí specifikovat metodiku tvorby jmen a pravidla jejich interpretace. Musí stanovit jak se identifikuje a autentizuje jednotlivec a jak entita odpovídající nějaké organizační jednotce. CP stanovuje nástroje použitelné pro identifikaci a autentizaci.
10. CP musí explicitně definovat zacházení s certifikáty při jejich revokaci a při prověřování jejich platnosti.
11. CP musí specifikovat provozní podmínky provozování CA/RA: Jak se žadateli o certifikaci dodává certifikát? Jak se manipuluje s klíči zvláště v případě, kdy CA manipuluje i s tajemstvími žadatelů o certifikáty? Co musí udělat držitel certifikátu po obdržení certifikátu a před jeho prvním uplatněním? Jaké konkrétní postupy se uplatňují při manipulaci s certifikáty.
12. CP musí specifikovat procedury bezpečnostního auditu a procedury archivace.
13. Součástí CP musí být plán obnovy činnosti po havárii, resp. po detekovaném proniknutí. CP musí ošetřit případ ukončení činnosti certifikační autority
14. Od CP se očekává, že bude specifikovat požadovaná fyzická, procedurální (logická, organizační) a personální (požadovaná kvalifikace, zacvičování) bezpečnostní opatření.
15. Velmi významnou složkou certifikační politiky jsou specifikace technických bezpečnostních opatření (generování a instalace párů klíčů ASK, ochrana soukromých klíčů, jejich archivace apod.
16. Nedílnou součástí CP jsou profily certifikátů a seznamů certifikátů (např. CRL).

17. CP rovněž uvádí specifikace správních procedur pro manipulaci s CP, tj. jak se zveřejňuje, jak a kdo ji schvaluje apod.

Obsah dokumentů CP a CPS by měl odpovídat ve světě běžným zvyklostem a standardům pro vypracovávání těchto dokumentů. Základní osnova textů CP a CPS je stejná pro oba dokumenty a měla by být strukturována do následujících kapitol:

1. *Úvod* – definice TSP který provozuje a spravuje CA, kterým uživatelům CA slouží a jak ji lze kontaktovat
2. *Obecné požadavky na zúčastněné strany* – definice práv, povinností, zodpovědností, vztahu ke státní správě a zákonům a podobné požadavky. Tato kapitola se může skládat například z podkapitol: Povinnosti jednotlivých stran, Vydávání certifikátů externím žadatelům, Prosazení CP a řešení problémů, Zveřejnění certifikátů a repositář, Audit dodržování CP a CPS, Důvěrnost informací
3. *Identifikace a autentizace žadatelů* – jak jsou uživatelům přiřazována jména (identifikátory) a jak je ověřována jejich identita. Tato kapitola se může skládat například z podkapitol: Počáteční registrace žadatele o certifikát, Opětovné vydání certifikátu, Požadavek na zrušení certifikátu
4. *Provozní požadavky* – popis procesu vydávání a rušení certifikátů, záznamů, které je třeba vést, prováděného auditu a postupů zotavení po bezpečnostním incidentu. Tato kapitola se může skládat například z těchto podkapitol: Žádost o certifikát, Vydání certifikátu, Pozastavení a zrušení certifikátu, Procedury bezpečnostního auditu, Archivace záznamů, Změna klíčů CA, Zotavení po bezpečnostním incidentu, Ukončení činnosti CA
5. *Fyzické, procedurální a personální opatření* – popis bezpečnostních opatření implementovaných v CA a RA. Tato kapitola typicky zahrnuje podkapitoly: Fyzická bezpečnost, Procedurální bezpečnost, Personální bezpečnost
6. *Technická bezpečnostní opatření* – popis kryptografických mechanismů, generování klíčů, použitých algoritmů, ochrany kryptografických klíčů a technických bezpečnostních požadavků na CA, RA a na držitele certifikátů. Tato kapitola se může skládat například z podkapitol: Generování klíčů, Ochrana soukromých klíčů, Správa klíčů, Bezpečnost počítačového vybavení, Bezpečnost životního cyklu vybavení, Síťová bezpečnost, Bezpečnost kryptografických modulů
7. *Profily certifikátů a CRL* – definice použitých položek certifikátů a CRL, použitých rozšíření, jejich význam a způsob jejich využívání. Tato kapitola obsahuje dvě obvykle dvě podkapitoly: Profil certifikátu, Profil CRL
8. *Správa certifikační politiky / Správa CPS* – popis způsobu administrace a udržování CP a CPS.

5 Příklady vlastností vybraných typů PKI

5.1 PKI typu X.509

Standard X.509 byl původně navržen v polovině 80.let před bouřlivým rozvinutím Internetu. Byl navrhován k uplatnění v provozu v off-line prostředí, ve kterém se počítače spojovaly pouze občasně. Pro takové prostředí byly sice ve verzích X.509 1 a 2 navrženy např. i mechanismy odvolávání platnosti vydaných certifikátů, ale problémy rozložení participujících stran a problémy času však tyto verse dostatečně neřešily. Certifikáty X.509v1/2 byly navrhovány především pro použití v rámci jedné organizace. Typicky spoléhaly na existenci jedné hierarchické struktury CA, protože velké společnosti jsou takto organizovány. Organizace vydávaly certifikáty svým zaměstnancům a PKI organizací byly určeny především pro podporu vnitřní komunikace. Vnitřní PKI sledovaly vrozenou hierarchii organizace,

jejich cílem bylo umožnit definovat vztahy důvěry, zavést je a řídit jimi vnitřní komunikace. Předpokládalo se, že zaměstnanec své organizaci a jejím CA přirozeně důvěřuje.

Původním cílem normy X.509 byla definice autentizačního prostředí podporujícího poskytování adresářových služeb v rozsáhlých počítačových sítích při přístupu k distribuovaným bázím dat definovaným rodinou norem X.500. Norma X.509 popisuje PKI pro podporu autentizačních služeb pro služby definované rodinou norem X.500. Jedná se o normy ISO/ITU. PKI vybudované na bázi normy X.509 dodnes používá řada firem a systémů s celosvětovou působností. PKI založenou na normě X.509 umožňují používat mnohé WWW aplikace, např. prohlížeč Netscape.

Zkušenosti ze snah uvést do života PKI budované na bázi X.509v2, které vznikaly počátkem 90. let a snažily se plně převzít způsob identifikace z globální hierarchie jmen podle standardu X.500, ukazují, že tudy cesta zřejmě nevede. Systematické používání globálně jednoznačných jmen je pro většinu aplikací příliš složité. Pochybnosti o dlouhodobé perspektivnosti certifikací na bázi identity nakonec vedou ke snahám zvýšit účinnost atributově orientované certifikace ve spojení se zaváděním rolí, ve kterých uživatelé vystupují. Tímto směrem se ubírají iniciativy SDSI, resp. SPKI, o kterých se zmiňujeme níže.

5.2 PKI na bázi normy X.509v3 a certifikát X.509v3

V současné době je nejvíce podporovanou normou digitálních certifikátů a souvisejících PKI je norma *X.509v3*. Normu X.509v3 přijaly jako bázi pro implementaci platebního protokolu SET asociace Visa a MasterCard. PKI na bázi normy X.509v3 určila jako svoji PKI rovněž organizace NATO.

Verze 3 standardu X.509 potřebu hierarchického uspořádání vztahů důvěry eliminuje (sice ne plně dokonale, ale přece jen nějak). Cílem verze 3 je dosažení možnosti křížového uznávání certifikátů mezi různými hierarchiemi CA. Certifikáty předchozích verzí standardu X.509 jsou ve verzi 3 doplněny o „rozšíření“, která umožňují v certifikátu uvádět specifikace politik certifikace, atributy uživatele certifikátu a CA, omezení specifikující přípustné struktury certifikačních cest a identifikace cest potřebných k získání informací o případném odvolání platnosti certifikátu. Základním často kritizovaným nedostatkem standardu X.509v3 je potřeba, aby ve všech stýkajících se PKI byly některé participující objekty (např. podepisovací algoritmy nebo certifikační politiky) identifikovány jednoznačně. PKI založené na standardu X.509 jsou i ve verzi 3 orientovány především na certifikaci identity, certifikaci atributů podporují málo. Teprve připravovaná verze 4 standardu X.509 propracovává strukturu certifikátů označovaných jako atributové certifikáty. Základními informačními položkami certifikátu podle X.509v3 jsou:

1. *typové označení verze certifikátu* – verse 1, 2, 3 podle doporučení X.509
2. *pořadové číslo certifikátu* – jednoznačná identifikace certifikátu v rámci vydávající CA
3. *informace o CA, která digitální certifikát vydala* – jednoznačné jméno CA (vnější, rozlišitelné jméno a případně i identifikátor podporující jednoznačnost), identifikace použitého algoritmu pro podpis certifikátu (např. SHA-1 + RSA), podpis CA
4. *informace o držiteli certifikátu* – jednoznačné jméno držitele certifikátu (vnější, rozlišitelné jméno a případně i identifikátor podporující jednoznačnost), identifikace algoritmu použitého pro podpisování, hodnota veřejného (ověřovacího, šifrovacího) klíče
5. *doba platnosti certifikátu* – od ... do ....

Mnohé další položky mohou být obsaženy v tzv. *rozšířeních* (extensions).

Vlastnosti PKI založené na použití certifikátů podle normy X.509v3 lze přiblížit následujícím výčtem jejích základních charakteristik:

1. Certifikát X.509v3 je plně rozšiřitelný, jeho obsah není nijak omezován (předchozí verze X.509 omezovaly např. jména uživatelů, CA a uživatelů certifikátů na jména splňující požadavky normy X.500)
2. Certifikát X.509v3 je sice identifikačním certifikátem, ale formou svých rozšíření podporuje i atributově orientovanou funkcionalitu, formou rozšíření ho lze rozšířit na atributový certifikát
3. Podporuje se hierarchická struktura CA doplněná o možnost křížové certifikace na libovolných úrovních hierarchie
4. Uživatel, CA a držitel certifikátu jsou chápáni jako samostatné entity
5. Každý uživatel certifikátu plně důvěřuje alespoň jedné CA, certifikační autority mohou definovat způsob delegování důvěry vůči uživatelům (žadatelům o certifikát) a vůči ostatním certifikačním autoritám
6. Základní metodou prokazování platnosti certifikátu je off-line prokazování; pomocí rozšíření certifikátu lze implementovat i on-line prokazování platnosti certifikátu
7. Základní metodou odvolávání platnosti certifikátu je propracovaný mechanismus off-line práce s CRL; pomocí rozšíření certifikátu lze definovat i on-line odvolávání platnosti certifikátu
8. Za preciznost a věrnost procesu certifikace je odpovědná CA, připuštění nestandardizovaných jmen tuto odpovědnost zřejmě činní obtížnější
9. Žadatel o certifikát se musí alespoň jedné CA identifikovat „out-of-band“; tento typ komunikace je potřeba použít rovněž v případech, kdy se zavádějí nová rozšíření certifikátů, přinejmenším z důvodu rozsáhlého a značného používání jednoznačných identifikací objektů
10. Pomocí rozšíření v certifikátech lze podporovat službu zajištění plné anonymity držitele certifikátu

Použití X.509v3 pro budování PKI se zjevně setkává s úspěchem v případech, kdy odpovídající doména je homogenní. Pokud homogenní není, pak by v ní měly existovat alespoň potenciální snahy o konstruktivní spolupráci. V nejhorším případě v ní musí být k dispozici nástroje pro prosazování konstruktivní spolupráce. Ideální by bylo, kdyby se do takové fáze dostalo i řešení PKI státní správy, která příliš homogenní doménou není a očekávat existenci všudypřítomné plošné masové snahy o konstruktivní spolupráci od prvků státní správy je holý nesmysl.

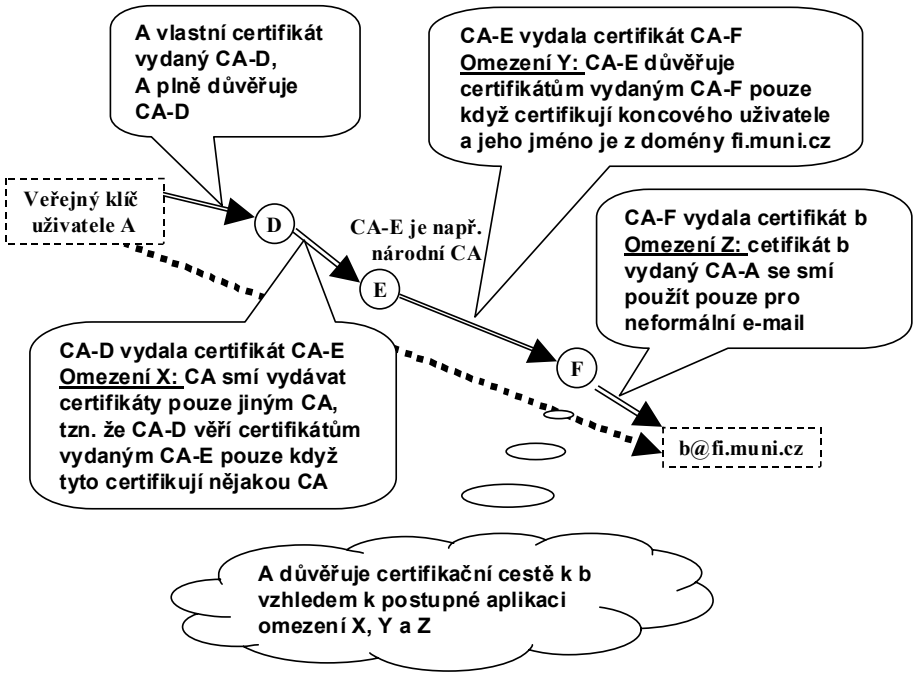
Z úzké souvislosti normy X.509 s normou X.500 plyne, že CA jsou standardně organizovány do hierarchických struktur, které poměrně těsně sledují hierarchické uspořádání adresáře typu X.500 – do tzv. *strom adresářových informací*, DIT (Directory Information Tree). Pojmenování uzlů na větvích takového stromu je nakonec základem jednoznačné identifikace objektů, které reprezentují listy DIT. Norma X.509 explicitně konkrétní uspořádání CA nepředpisuje, její veze 3 však hierarchické uspořádání doplněné o možnost křížových certifikací všestranně podporuje. X.509v3 se tak stala vhodnou platformou pro PKI pokrývající i heterogenní systémy, v nichž participuje mnoho více či méně nezávislých organizací. Předchozí verze X.509 byly de facto použitelné v rámci jedné organizace budované podle hierarchického modelu. Implementátorům PKI dovoluje norma X.509v3 definovat obsah certifikátu podle svých přestav, pro uvádění informací o klíčích, politikách, atributech, omezeních vymezujících možné certifikační cesty a pro zavedení propracované funkcionality prokazování platnosti a odvolávání platnosti certifikátů je definována řada *rozšíření*:

1. *CP a zobrazování CP.* CA může do certifikátu zahrnout seznam CP, které byly uplatněny při tvorbě certifikátu. Seznam pomáhá uživateli certifikátu při rozhodování, zda daný certifikát je či není vhodný pro nějaký konkrétní účel. CP může např. indikovat, že certifikát lze používat pro neformální komunikaci elektronickou poštou ale ne pro realizaci finančních transakcí. CP proto musí uvádět identifikaci používaných bezpečnostních opatření, způsobu identifikace žadatele o certifikát, právních závaz-

ků a předpisů apod. Mechanismus zobrazování politik CA umožňuje indikovat, zda některá z jejích CP je ekvivalentní některé CP jiné CA.

2. *Alternativní jména.* Držitel certifikátu i CA může mít i několik alternativních jmen, aby se PKI nemusela vázat na použití adresářové struktury X.500. Jako alternativní jména lze použít adresy elektronické pošty, URL známé z prostředí WWW apod. Alternativními jmény lze označovat rovněž vydavatele CRL.
3. *Atributy držitele certifikátu.* Certifikát může obsahovat hodnoty libovolných atributů, které byly původně ukládány do databázových záznamů distribuovaných bází dat X.500 a které reprezentují dodatečné identifikační informace doplňující jméno držitele certifikátu.

Omezení určující certifikační cesty. Tato rozšíření umožňují CA, aby se smysluplně zapojily do svých infrastruktur. CA může omezit typy certifikačních cest které lze tvořit z certifikátů, které vydává pro jiné CA. CA zde může určit, zda držitel certifikátu ve skutečnosti je či není nějaká CA (zabraňuje tím, aby koncový uživatel svévolně vystupoval jako CA). CA rovněž může omezit tvoření certifikačních cest z certifikátu na certifikační cesty k certifikátům vydaným v nějakém prostoru jmen (např. v nějaké internetovské doméně) a/nebo k certifikátům, které vyhovují nějak specifikované množiny politik. CA se tím umožňuje budovat ochrany před nekonečnými certifikačními cestami postupným uplatňováním omezení po certifikační cestě. Princip ilustruje obrázek Obr. 5. Když subjekt A z obrázku Obr. 5 získá certifikát b, ví, že b ho směl použít pouze pro neformální elektronickou poštu a dále ví, že může autentizaci b považovat za poměrně silnou autentizaci (silnější než je např. autentizace pavučinou důvěry PGP), poněvadž může sledovat postupná omezení důvěryhodnosti na certifikační cestě. Subjekt A tudíž nebude akceptovat ani certifikát b vydaný CA-E (nebo nějakému jinému uživateli), ani certifikáty vydané od jiné CA certifikované CA-F. Jestliže CA definuje co nejpřísnější praktické omezující podmínky při certifikaci jiných CA, pak platí, že čím je certifikační cesta delší, tím více je omezovaná, až nakonec nemůže dále růst.



Obr. 5 Postupné uplatňování omezení certifikačních cest

Pozornost je vhodné věnovat i rozšířením certifikátů X.509v3 určeným pro revokaci certifikátů a potvrzování jejich platnosti:

4. *Číslo CRL a kód důvodu revokace*. Každý CRL vydaný pro jistou populaci certifikátů má přidělené pořadové číslo z monotónně rostoucí posloupnosti celých čísel. To uživateli umožňuje zjišťovat, zda nějaký CRL nepropásl. Každý certifikát umístěný v CRL má v záznamu o jeho revokaci uveden důvod revokace
5. *Distribuční body CRL*. Toto rozšíření pomáhá omezovat rozměry CRL zpracovávané uživateli CA. CA může CRL dělit na části a jednotlivé části CRL vydávat na různých distribučních bodech, takže všichni uživatelé nemusí přijímat celé CRL. Například CA university může vydávat různé CRL jednotlivých fakult samostatně. Pokud chce profesor ověřit certifikát studenta z konkrétní fakulty, nemusí kontrolovat CRL celé university a může pracovat pouze s CRL odpovídající fakulty. CRL lze dělit rovněž podle důvodů revokace. Běžné revokační záznamy např. z důvodu změny jména (studentky po svatbě) se mohou publikovat v jiných CRL než revokační záznamy generované na základě oznámení kompromitace soukromého klíče učitele. Seznamy kompromitovaných certifikátů si pak uživatelé obnovují a kontrolují pravděpodobně častěji než seznamy běžných revokací.
6. *Delta-CRL*. Rozšíření, které podporuje další metodu omezování rozměru CRL. CA může pravidelně v jistých krátkých intervalech vydávat místo celého CRL nebo jeho částí pouze změny, které s v nich vyskytly od posledního vydání úplného CRL nebo jeho částí. Uživatel certifikátu si udržuje svoji kopii CRL a aktualizuje ji podle vydávaných delta-CRL. Významně se tak šetří komunikační kapacita.
7. *Nepřímé CRL*. Toto rozšíření umožňuje vydávání CRL jinou entitou než je CA, která vydala odpovídající certifikáty. Taková entita může fungovat jako společný repositář více CA, poskytuje jim službu distribučního bodu CRL.

Popsaná rozšíření neřeší fundamentální problém časové granularity. Ani dělení CRL na části, ani vydávání delta-CRL nezabrání časové prodlevě, po kterou lze používat neplatný certifikát. Tento problém řeší až propracované protokoly on-line revokace a potvrzování platnosti certifikátů. Teprve jejich plné zavedení umožní CRL plně eliminovat.

Posledním rysem PKI typu X.509v3, který je potřeba zmínit a rozumět mu, je způsob identifikace elementů (objektů) vytvářejících PKI typu X.509v3. Způsob, jakým X.509v3 podporuje rozšiřitelnost působnosti a pružnost PKI současně omezuje snadné globální používání rozšíření definovaných různými uživateli. Každý prvek PKI typu X.509v3 (algoritmus podpisu, certifikační politika, uživatelem definované alternativní jméno, uživatelem definované rozšíření,...) musí být označen mezinárodně definovaným mechanismem identifikace objektů. Každý objekt pak má svůj OID (Object Identifier). OID je numerická hodnota tvořená posloupností celých čísel, která je vůči ostatním OID jednoznačná.

OID jsou přidělovánu podle hierarchické struktury autorit přidělujících hodnoty OID. Takovou autoritou se může stát kterákoliv organizace nebo instituce. Taková instituce musí mít přidělený svůj OID, který uvádí jako prefix hodnot, které generuje. Strom hierarchie autorit přidělujících hodnoty OID objektů může začínat na nadnárodní úrovni (ISO, ITU, UN, ...), pokračovat na další úrovni definicí pozice pro státy, výbory nadnárodních organizací apod. Na další úrovni se státy mohou dělit na jednotlivé státní útvary, na další úrovni mohou OID vydávat instituce ve státu (státní správa, armáda, ...) atd. OID nějaké CP může mít hodnotu např. 2-16-840-1-45356-3-15. Problémy nastávají v okamžiku, kdy se OID začnou uvádět v certifikátech dříve, než dojde ke všeobecné dohodě na jejich významu. Jestliže chce nějaká CA zavést a označit svoji (novou) politiku, OID této politiky musí a priori znát všechny entity, které chtějí její certifikáty používat. Jinak neznalá entita nebude vědět jak takovou politiku interpretovat. Nejasnosti mohou vzniknout i v případech, kdy dvě nebo více CA přidělí stejnému objektu více jmen (např. hašovacímu algoritmu). Zbytečně si nerozumí, používají stejný objekt, jen o tom neví a zbytečně takto označený rys ignorují. Po propojení PKI křížovou certifikací může snadno dojít k tomu, že CA budou muset své uživatele informovat o ekvivalenci různých OID nebo u sebe a u svých uživatelů

OID změnit. Zavedení systematické propracované metody určování významu OID je základním předpokladem zavedení křížové certifikace mezi různými PKI. Problém OID je hlavní zábranou volné rozšiřitelnosti X.509v3 na rozlehlé domény.

5.3 PEM a PKIX, další typy PKI na bázi normy X.509

Pro síť Internet byla navržena PKI založená na normě X.509v1. Výsledkem její implementace se stal systém *Privacy Enhanced Mail, PEM* (RFC 1421, 1422 a 1423, 1993) poskytující služby důvěrnosti, autentizace, záruky za integritu a nepopiratelnosti originálu implementované pomocí ASK. Omezení PEM dané výše zmíněnými omezeními X.509v1 (především požadavek hierarchické struktury) způsobily, že internetovská komunita systém PEM nikdy za svůj nepřijala.

Ve druhé polovině 90. let vzniká v internetovské komunitě iniciativa *PKIX, Public Key Infrastructure using X.509*, (http://www.ietf.org/html.charters/pkix-charter.html), která vychází z normy X.509v3. Poněvadž na vývoji PKIX s podílí řada zdrojů, které stály za návrhem normy X.509v3, lze očekávat, že PKIX bude nakonec velmi blízká řešení původní PKI typu X.509v3. Je vhodné upozornit na některé výsledky této iniciativy, tj. na RFC, které upřesňují doporučení X.509v3 do konkrétních profilů zaručujících interoperabilitu cestou Internetu – RFC 2459 definuje certifikáty X.509v3 a CRL pro použití na Internetu, RFC 2510 definuje „Certificate Management Protocol“ (CMP), RFC 2560 definuje „Online Certificate Status Protocol“ (OCSP), RFC 2511 definuje „Certificate Management Request Format“ (CRMF), RFC 2587 popisuje použití protokolu LDAPv2, RFC 2585 popisuje použití FTP pro transport operací PKI, RFC 2527je neformálním návodem pro tvorbu CP a CPS, RFC 2528 se zabývá definicí *KEA* (Key Encryption Algorithm).

Stojí za zmínku, že používání PKIX neodpovídá původním konceptům X.509. Ukazuje se, že identifikace pomocí DN-jmen (DN, Distinguished Name) podle X.500 je použitelná pouze pro vnitřní pojmenovávání v rámci organizace. Prostor jmen X.500 de facto neexistuje a neexistuj žádné aplikační směrování zpráv na tato jména, koncové entity zjevně používají DN-jména pouze pro privátní pojmenovávání. Použitelným prostorem jmen je prostor jmen DNS (Domain Name System). Existence DNS ukazuje, že není politicky nemožné aby jedna entita ovládala uniformní prostor jmen. Dva takové prostory jmen udržovat nelze. To, že uspěla iniciativa DNS a ne politicky protláčený systém X.500 je dáno tím, že DNS byl navržen a implementován dříve, než si ho, resp. jeho důležitosti, silné politicky motivované loby všimly.

5.4 PGP PKI

Systém PGP je původně navržen jako systém kombinující použití symetrické a asymetrické kryptografie pro podepisování (důvěrných) elektronických dopisů. Vlastnosti PGP PKI lze přiblížit tímto výčtem základních charakteristik:

1. Certifikát PGP je jednoduchý, má pevně stanovenou strukturu, obsahuje veřejný klíč, adresu pro elektronickou poštu a atribut vyjadřující stupeň důvěryhodnosti; rozšiřovat ho nelze
2. PGP podporuje pouze identifikační certifikáty
3. CA jsou uspořádány do ploché pavučiny důvěry
4. Každý uživatel PGP je sám sobě kořenovou CA, a bezmezně si věří; CA mohou svým subjektům (jiným CA) přiřazovat stupeň jejich důvěryhodnosti
5. PGP PKI dobu platnosti certifikátu neomezuje, uživatel certifikátu se sám rozhoduje, zda bude či nebude považovat certifikát za platný
6. PGP PKI nepoužívá žádnou formu CRL, předpokládá, že informace o neplatných certifikátech se nějak šíří mimo sféru vlivu PGP
7. Autentizace zaručovaná PGP je velmi slabá, jediným identifikačním nástrojem je adresa pro elektronickou poštu

8. PGP se plně spoléhá na „out-of-band“ autentizaci
9. PGP žádnou nepodporuje přímou formu anonymity, anonymitu lze poskytnout jedině „falšováním“ adres elektronické pošty

PGP PKI je jednoduchá, je široce používaná, ale mimo oblast neformální komunikace prakticky použitelná není. Na druhé straně PGP PKI je vedle PKI typu X.509 druhým typem PKI, který se skutečně používá i v běžné praxi.

Uživatel PGP si udržuje „kroužek s klíči“, na kterém má „zavěšeny“ veřejné klíče partnerů. Podepsáním veřejného klíče partnera svým soukromým klíčem uživatel vyjádří důvěru, že daný klíč je platný, tj. že k tomuto klíči připojené uživatelské jméno odpovídá skutečnému vlastníkovi klíče. Když uživatel přidává takový klíč na svůj kroužek, říká tím, že vlastní platný klíč. Při práci s každým klíčem PGP uživatele upozorní, jestli je daný klíč platný nebo ne.

Uživatelé si mohou klíče na kroužku vzájemně vyměňovat. Podepsaný klíč lze vystavit na Internetu tak, aby ho mohli používat jiní partneři dané osoby a aby měli od dané osoby potvrzeno, že ona má v tento klíč důvěru. Jako platný klíč na kroužku se rovněž označuje klíč ke kterému uživatel získá dostatečný počet certifikátů od osob, kterým důvěřuje. Například Alice podepíše certifikát Bobova veřejného klíče, protože je přesvědčena o jeho autenticitě (např. na základě důvěryhodné „out-of-band“ komunikace). Alice je v terminologii PGP „introducer“ – zavádí nový certifikát veřejného klíče tím, že ho podepíše svým soukromým klíčem. Bob tento certifikát předá Karlovi, protože Karel s ním chce důvěrně komunikovat. Karel zná a důvěřuje Alici z hlediska její role „introducer-a“ a zjistí, že podepsala certifikát Bobova klíče. Karel proto důvěřuje autentičnosti Bobova veřejného klíče. Kdyby Karel Alici nedůvěřoval, nedůvěřoval by pak ani certifikátu, který dostal od Boba a Bob by si musel najít jiného „introducer-a“, kterému by Karel důvěřoval.

Jiný scénář: Bob v minulosti získal Karlův veřejný klíč a ověřil si jehoQplatnost. Alice si vygeneruje párové klíče ASK a s Karlem si vzájemně vymění bezpečným způsobem svoji identifikaci a veřejné klíče. Karel tudíž podepíše certifikát Alicina veřejného klíče a ten vrátí případně už Internetem Alici. Ta si ověří, zda certifikát nebyl narušen (zná svůj a Karlů veřejný klíč a může ověřený certifikát poskytnout Bobovi nebo někomu jinému, kdo případně již má ověřenou platnost Karlova klíče. Od tohoto okamžiku Alice může bezpečně komunikovat s takovými jedinci.

Míra důvěry v PGP se vyjadřuje mírou důvěry ve veřejný klíč, tj. nepřímo řečeno důvěry, jak vlastník veřejného klíče je kompetentní podepisovat jiné PGP certifikáty veřejných klíčů, lze vyjádřit jednou ze čtyř následujících hodnot:

1. *Plně důvěryhodný* – jestliže získá nějaký jiný (nový) klíč s certifikátem podepsaným vlastníkem plně důvěryhodného klíče, pak nový klíč přidá na kroužek jako platný a de facto tím říká, že vlastníkovi plně důvěryhodného klíče důvěřuje B z hlediska záruky za platnost jím podepsaných klíčů
2. *Omezeně důvěryhodný* – dříve než si přidá na kroužek jako platný nějaký nový klíč *K* s certifikátem podepsaným vlastníkem omezeně důvěryhodného klíče, musí získat alespoň jeden další certifikát klíč *K* podepsaný dalším vlastníkem omezeně důvěryhodného klíče
3. *Nedůvěryhodný* – vlastníka tohoto klíče nebude používat pro zjišťování, zda může přidat nový klíč na svůj kroužek; jeho záruce za nový klíč nevěří
4. *Neznámý* – prakticky totéž jako „nedůvěryhodný“.

Uživatel A tak může přidělovat stupeň důvěryhodnosti klíči získaného od uživatele B. Kriteria pro akceptování klíče může uživatel A upřesňovat, může např. říci, že klíč akceptuje pouze tehdy, pokud ho získá alespoň ze dvou (tří, ...) plně důvěryhodných zdrojů. Celý systém je založen na principu fungování plně důvěryhodné „out-of-band“ komunikace mezi zúčastněnými uživateli (Alice–Bob, Alice–Karel) při předávání klíčů (např. pomocí diskety).

Uživatel B např. předá svůj veřejný klíč uživateli A. Pak si vymění své veřejné klíče s uživatelem C. Uživatel C získá klíč uživatele E. Uživatel B má na svém kroužku platných klíčů

klíč uživatele C, uživatel C má na kroužku klíče uživatelů B a E. Nyní uživatel B kontaktuje e-mailem uživatele C a vymění si e-mailem kroužky s klíči. Poněvadž uživatelé B i C mají svoje kroužky podepsané a vzájemně znají svoje veřejné klíče, mohou výměnu Internetem chápat jako bezpečnou. Od uživatele A uživatel B kroužek e-mailem bezpečně obdržet nemůže, nezná veřejný klíč uživatele A. Svůj kroužek však uživatel B uživateli A bezpečně poslat může, poněvadž A zná jeho veřejný klíč. Takže uživatel A se může dozvědět veřejné klíče uživatelů C a E.

Meze pavučiny důvěry PGP jsou z příkladu zřejmé. Uživatel A může bezpečně komunikovat s uživatelem C poněvadž B dostal klíč od C nezprostředkovaně ještě před tím, než ho dal A. Když ale uživatel A posílá e-mail uživateli E, spoléhá se na někoho, s kým nebyl v přímém styku, tj. na uživatele C, že ten mu řekne jaký má klíč někdo, koho A rovněž vůbec nezná (E). Kdyby se A setkal s C, možná by mu nedůvěřoval, ale takto, protože věří B, věří de facto také C. Pokud to uživatel B uživateli A neřekne, pak A nemá šanci se dozvědět, který klíč pochází od B a který od C. Nakonec, pokud A někomu v pavučině věří, pak musí věřit celé pavučině. I když s tím bude A souhlasit, je stále zranitelný. Pokud se podaří podvodníkovi přesvědčit uživatele C, že je vlastně uživatelem E, pak podvádí každého, kdo C věří.

Certifikáty PGP se zjevně liší od certifikátů X.509 – vydávají je běžní uživatelé (v prostředí X.509 obvykle profesionální CA) a důvěryhodnost vydavatelů certifikátů je proto podporována alespoň „pavučinou důvěry“ uživatelskou komunitou. Nejsou vydávány ani žádnými CA, ani podle žádných komerčních pravidel dokumentovaných nějakými dokumenty typu CP/CPS. PGP PKI je nejjednodušší formou PKI. Tak jak si uživatelé budují kroužky s klíči, budují si pavučinu důvěry. Každý uživatel je v podstatě svojí kořenovou CA, která rozhoduje komu se má a komu nemá věřit. Jednoduchost PGP PKI je hlavní příčinou relativně širokého používání PGP. Pro aplikační systémy typu elektronického obchodu nebo pro systémy, které vyžadují silnou autentizaci, se PGP PKI nehodí.

Certifikát PGP obsahuje pouze adresu elektronické pošty, hodnotu veřejného klíče a stupeň důvěryhodnosti a nelze ho rozšiřovat. Silnou autentizaci zajistit nelze, adresa elektronické pošty na to nestačí. Rozšíření certifikátu nepřipadá do úvahy, takže PGP lze používat pouze pro elektronickou poštu (když uživatel A podpisuje klíč uživatele B pro bankovní operace, nemůže dodat, že se jedná klíč pro bankovní operace).

PGP PKI neumožňuje revokaci a potvrzování platnosti certifikátů, tyto funkce musí být zajištěny mimo komunikační prostředí. PGP se tudíž hodí pouze pro neformální elektronickou poštu.

Koexistence PKI PGP a PKI X.509(v3) v rámci jedné aplikace je prakticky nemožná, především z důvodu naprosto odlišného modelu důvěry.

5.5 Infrastruktura SDSI

SDSI (http://theory.lcs.mit.edu/~cis/sdsi.html, A Simple Distributed Security Infrastructure,) je iniciativním návrhem „otců-zakladatelů“ mnohého z bezpečnosti IT – pánů Rona Rivesta a Butlera Lampsona. Sympatické na PKI tohoto typu je perspektivní přístup k řešení PKI. Jedná se o exemplární projev úsilí odklonu od individuové certifikace k certifikaci založené na rolích a atributech. SDSI nepřiděluje klíč nějaké identifikované entitě, entitami podle SDSI jsou klíče (v SDSI se entita nazývá „principal“ – herec, který hraje hlavní roli). Klíč je vlastně „proxy“ koncové osoby, která má pod kontrolou odpovídající soukromý klíč. Vlastnosti SDSI lze přiblížit tímto výčtem základních charakteristik:

1. Certifikát SDSI má volně rozšiřitelný formát, může obsahovat popis atributů
2. SDSI podporuje certifikáty identity a společně s mechanismem definice skupin podporuje i atributové certifikáty
3. Principálové SDSI mohou být CA, SDSI nedefinuje žádné uspořádání svých CA
4. SDSI nerozlišuje mezi držitelem certifikátu, CA a uživatelem certifikátu, všichni „principálové“ mají stejnou autoritu a práva

5. Vztah důvěry zavádí SDSI podobným způsobem jako PGP
6. SDSI certifikáty se ověřují plně on-line, jejich platnost lze ověřovat opakovaně při každém jejich použití nebo po udaných intervalech
7. Platnost SDSI certifikátů se odvolává on-line, definovatelná perioda povinnosti opakovaného potvrzování platnosti certifikátů současně definuje horní mez intervalu možné doby šíření certifikátu
8. Autentizace zaručovaná SDSI vychází z lokálně přidělovaných jmen a se vzrůstem prostoru jmen se jejich autentizační síla zeslabuje; systém globálních jmen podle SDSI zaručuje dostatečnou autentizační sílu SDSI certifikátů pouze když obsahuje malý počet rozlišitelných „kořenů“.

Svůj „principál“ pro některý rozlišitelný kořen SDSI uživatel získává nějakou vhodnou „out-of-band“ formou, ten pak lze použít pro následné „in-band“ získávání informací. Anonymita principálů se v SDSI dosahuje na úkor jejich autentizační síly. Pro dosažení silné autentizace musí mít principál přiděleno nějaké globální jméno nebo musí být ostatním principálům, kteří s ním pracují, dobře znám.

SDSI je relativně mladá, v praxi dosud nevyzrálá technologie PKI z druhé poloviny 90. let. Jelikož jedním z jejích autorů je B. Lampson a ten je z Microsoftu, lze tak očekávat cokoliv.

5.6 Infrastruktura SPKI

SPKI (http://www.ietf.org/html.charters/spki-charter.html, Simple Public Key Infrastructure) je výsledkem iniciativy pracovní skupiny IETF formované ve druhé polovině 90. let (v r. 1996) s cílem navrhnout alternativní PKI k PKIX, založené na certifikaci X.509v3. Hodně se přebírá z návrhu SDSI, v návrhu se rovněž projevuje snaha založit PKI spíše na bázi atributových certifikátech než na certifikátech konkrétních individuí. Hlavním cílem SPKI a certifikátů vydávaných SPKI je podpora šíření přístupových práv včetně jejich delegace.

SPKI je relativně mladá, v praxi dosud nevyzrálá technologie PKI. Návrhy SDSI a SPKI jsou konkrétními projevy přesvědčení, že z hlediska dlouhodobých perspektiv potřeby plně universální PKI nejsou PKI založené pouze na certifikaci identity entity (tj. X.509, PGP) perspektivní. IETF v současné době práce na SPKI ukončila. Požadavky trhu na certifikáty SPKI jsou zanedbatelné a dodavatelé technologií CA a PKI proto vesměs necítí potřebu nabízet vedle certifikátů X.509v3 ještě další certifikáty s podstatně odlišnou syntaxí

Důvěryhodnost certifikátů SPKI/SDI je podporována podobně jako důvěryhodnost certifikátů X.509 deterministickými certifikačními řetězci, cestami. Předpokládá se, že ID certifikátu váže klíč s jeho vlastníkem nebo se skupinou vlastníků. Vlastník klíče je identifikován libovolným lokálním jménem, které má z hlediska vydavatele certifikátu nějaký význam. Explicitně se říká, že ostatní nemohou předpokládat nějakou vazbu mezi lokálním identifikátorem a konkrétní osobou na základě toho, jak toto jméno zní (Jestliže Karlovi přisuzuji jména Anna, je to moje věc). Vydavatel certifikátu je jedinou autoritou z hlediska vazby jména na osobu. Nikdo jiný do toho nemá co mluvit. Není potřeba žádná CPS. Ostatní identifikují vlastníky klíčů pomocí jejich klíčů. ID certifikátu slouží pouze pro usnadnění práce vydavatele certifikátu jako přezdívka (nickname) nebo jako jméno skupiny vlastníků klíčů. Pro ostatní je užitečné, když se lokální jméno konvertuje na globální jméno např. formou „name <key> <ID>“.

Bezejmenná SPKI

Původní certifikáty SPKI, tj. před sloučením iniciativ SPKI/SDSI identifikovaly vlastníky klíčů pouze jejich veřejnými klíči nebo jejich hashem. I po sloučení snah obou iniciativ autorizační certifikáty stále vážou autorizace přímo na veřejné klíče (atributové certifikáty vážou autorizace na jméno). Veřejný klíč (nebo jeho hash, jsou-li hashe bezkolizní) je glo-

bálně unikátní identifikátor soukromého klíče. Ve všech certifikačních systémech se oprávněně předpokládá, že soukromý klíč je asociován právě s jedním vlastníkem klíče. Veřejný klíč (nebo jeho hash) je tedy globálně unikátní identifikátor vlastníka klíče. Pokud by nějaký systém byl navržen tak, že klíče může společně vlastnit skupina vlastníků klíčů, pak je veřejný klíč identifikátorem takové skupiny a neexistuje možnost další explicitní identifikace. Lze tímto způsobem např. podporovat anonymitu.

k-of-n subjekty SPKI/SDSI

V rámci rozvoje iniciativ SPKI/SDSI se posléze zavedl princip stanovení prahu „k-of-n subjektů"; k-of-n subjekt je takový seznam *n* subjektů (klíčů, jmen nebo jiných povolených konstrukcí) a hodnot *k* a *n*, že ověřovatel potřebuje *k* úplných cest mezi tímto certifikátem (nebo záznamem v ACL, Access Control List) a některým koncovým subjektem. Tím se dosahuje odolnosti proti výpadku podobně jako v pavučině důvěry PGP, s jedním významným rozdílem. V SPKI/SDSI o požadované míře tolerance v odolnosti proti výpadku rozhoduje vydavatel certifikátu nebo editor ACL. Tato strana také vybírá klíče známe předem a může si být tudíž jistá, že se jedná o klíče kontrolované různými vlastníky klíčů.

Vzájemné porovnání vlastností certifikátů z hlediska identifikace v hlavních dosud zmíněných PKI ilustruje následující tabulka:

PKI	Charakteristika CA	Typ identifikace
X.509	Hierarchie autorit odpovědných za identifikaci, vzájemná certifikace, CP/CPS	Definitoricky globální (Distinguished Name, X.500), prakticky lokální, volená vydávající CA se snahou o unikátnost
PGP	Pavučina důvěry – násobné cesty certifikace s cílem zajistit přijatelnou důvěryhodnost amatérských vydavatelů certifikátů	Globální – globálně unikátní e-mail adresa (díky „Domain Name Systém"), nemusí být však perzistentní
SPKI/SDSI	Jedna identifikační autorita, Není nutná CPS	Lokální (cokoliv)
SPKI bez jmen	Hierarchie autorizačních autorit, volitelně princip „k-of-n"	Globální – veřejný klíč nebo jeho globálně unikátní (díky matematice) a perzistentní hash

5.7 PKI DNS

DNS (Domain Name Service) je distribuovaná databáze zabezpečeně zobrazující symbolická jména uzlů Internetu na jejich internetovské (IP) adresy. DNS lze navíc použít i pro poskytování služby distribuce veřejných klíčů i pro jiné protokoly (minimálně je definováno rozšíření DNS pro zabezpečování internetovské elektronické pošty). Vlastnosti DNS PKI lze přiblížit tímto výčtem základních charakteristik:

1. certifikát DNS může obsahovat kterýkoliv typ záznamu o zdroji (resource record)

2. DNS certifikát identifikuje vlastníka veřejného klíče přiřazením veřejného klíče DNS-jménu, atributové certifikáty se nepodporují, lze však budovat systémy budované na bázi vyhodnocování atributů nad zabezpečeným DNS
3. každá DNS CA odpovídá nějaké DNS-doméně, takže DNS CA jsou vlastně uspořádány do hierarchie podle hierarchie DNS-domén; každá DNS CA ale může certifikovat kteroukoliv jinou DNS CA, takže lze vytvářet kombinované topologie
4. držitelem DNS-certifikátu je entita, která má DNS-jméno, její DNS CA je DNS CA odpovídající za příslušnou doménu nebo sama vystupuje roli DNS CA
5. předpokládá se, každý uživatel plně důvěřuje alespoň jedné CA
6. DNS certifikáty se ověřují on-line, certifikáty mají definovanou dobu platnosti, po jejím uplynutí se musí její platnost ověřit znovu
7. platnost DNS certifikátů se odvolává v okamžiku, kdy jeho držitel CA sdělí, že se změnil nějaký informační zdroj (např. změnil svůj šifrovací klíč); změna se musí rozšířit celým systémem za dobu kratší než je doba platnosti změny
8. autentizace zaručovaná DNS je silná pouze tehdy, když se mapování DNS-jmen řeší v rámci bezpečné zóny
9. v každé doméně se musí alespoň jeden klíč získat osobně, „out-of-band“, ten pak lze použít pro automatickou správu klíčů ostatních entit
10. cílem bezpečného DNS není podpora anonymity, není však problém požadavek anonymity uspokojit.

DNS lze principiálně použít jako univerzální praktickou PKI dostačující pro mnohé aplikace, eliminace omezení kladených počátečním návrhem DNS je řešitelná.

6 Bezpečnostní a správní služby a PKI

Při řešení základních problémů PKI je potřeba znát odpovědi především na následující otázky:

1. které bezpečnostní služby se musí poskytovat pro ochranu každého toku dat
2. jakou politiku je potřeba implementovat pro každou službu, resp. provozování každého prvku infrastruktury
3. co se stane, když dojde k narušení bezpečnostní služby nebo když je některý prvek infrastruktury kompromitován
4. které procedury je potřeba implementovat pro službu/provozování prvku infrastruktury
5. kdo odpovídá za službu nebo prvek infrastruktury
6. které požadavky si vynucuje zajištění interoperability
7. jak silné bezpečnostní mechanismy je potřeba použít
8. jaká je cena služby/prvku infrastruktury.

PKI podporuje plnění uživatelských bezpečnostních služeb, sama takové služby využívá a zajišťuje správu obou uvedených kategorií služeb. Požadavky kladené na PKI jsou jednak technického charakteru (např. generování certifikátů) a jednak administrativně správního (např. jak ustanovit oblast vztahu důvěry), provozního nebo i legislativního charakteru. Pro splnění takových požadavků je potřeba řešit související problémy jak během návrhu PKI, tak i během zavádění a provozování struktury a podstruktur PKI. Nelze je řešit isolovaně, mnohá rozhodnutí o způsobu plnění jedné kategorie služeb ovlivňuje způsob plnění mnohých dalších služeb.

6.1 Bezpečnostní služby podporované na uživatelské úrovni PKI

Jedná se především o podporu zajištění důvěrnosti, zajištění integrity dat, autentizace, nepopiratelnost, autorizace a řízení přístupu, notarizace, časové razítkování. Orientačně lze upozornit, že na řešení problematiky podpory těchto služeb mají dopad místa v architektuře systému, kde se služby poskytují, nároky kladené na zachování soukromí, potřeby podpory ze strany PKI při generování klíčů, požadavky na obnovu dat, požadavky dané potřebnou interoperabilitou, požadavky kladené potřebnou sílou bezpečnostních mechanismů, použité protokoly pro správu služeb, stanovení profilu odpovídajícího druhu certifikátu, politiky partnerů a nadřazených složek, dostupné technologie pro generování klíčů, požadavky na obnovu klíčů po jejich kompromitaci, exportní politiky případných zahraničních partnerů a požadavky na národní suverenitu při spolupráci se zahraničními partnery, požadavky na zaručitelnost bezpečnosti respektující výsledky provedených analýz rizik požadavky dané prosazováním práva a právní odpovědností, problematika rozhraní mezi partnerskými PKI zvláště na mezinárodní úrovni, způsoby řízení toku informací mezi různými klasifikačními úrovněmi, požadovaná granularita daná schopností identifikace zdroje podepsaných zpráv, požadovaná granularita časově závislých služeb.

6.2 Vnitřní bezpečnostní služby PKI

Jedná se především o zajištění důvěrnosti a zajištění integrity dat (auditních, registračních, archivních, publikovaných, klíčových materiálů, ...), autorizace a řízení přístupu ke komponentám PKI, řízení opakovaného využívání objektů/zdrojů, dostupnost a podobně i jako v předchozí kategorii i o podporu služeb autentizace, nepopiratelnosti, notarizace a časového razítkování. Na řešení podpory těchto služeb mají dopad analogické problémy jako jsou uvedeny u předchozí kategorie služeb.

6.3 Služby správy PKI

Jedná se především o

- *správu politik* (off-line proces vývoje, vyhlašování, provozní správy a udržování vztahů důvěry v rámci jednotlivých domén PKI a mezi doménami, vývoj provozních postupů, poskytování mechanismů prosazování politik, proces změnových řízení),
- *správu činností souvisejících s řešení kompromitace* (jak se detekuje průnik, zpravodajství o průniku, obnova po průniku a kompromitaci prvku infrastruktury, resp. certifikátu, vše v kombinaci off-line manuálních procesů s aplikací on-line působících technických mechanismů),
- *účtování* (protokolování) a audit (obvykle služby definované v CPS),
- *generování a obnovu klíčů a/nebo dat* (proces, kterým autorizovaná entita – uživatel, organizace, reprezentant práva – může obnovit data šifrovaná klíčem, ke kterému nemá přímý přístup),
- *správu certifikátů*,
- *řízení přístupu* a služby *komunikace mezi prvky infrastruktury*,
- *publikační služby*,
- *služby zajišťující interoperabilitu*,
- *potřebnou technickou podporu* a *správu konfigurace* prvků infrastruktury.

Na řešení podpory těchto služeb mají dopad rozhodnutí o tom, kdo je (kdo jsou) autoritou pro vývoj a pro prosazování politik, rozhodnutí o požadované úrovni zaručitelnosti bezpečnosti, rozhodnutí o požadavcích na personální bezpečnost, rozhodnutí o požadavcích na fyzickou bezpečnost, požadované způsoby integrace politik zúčastněných partnerů v

rámci PKI, požadavky práva, požadovaná úroveň inter-operability, požadované formy dokumentování politik, rozhodnutí o použitých normách a standardech, požadovaná úroveň konektivity mimo sféry přímého působení aplikací využívajících danou PKI, způsoby identifikace a přidělování jmen entitám v rámci domén PKI, stanovení síly mechanismů potřebných pro správu řízení po kompromitování prvku infrastruktury, rozhodnutí o aplikaci off-line a on-line mechanismů reakcí na průnik a kompromitaci, rozhodnutí o požadavcích na obnovu dat a klíčů uživatelů a prvků infrastruktury, rozhodnutí o tom, kde se správa obnovy po průniku řeší a jak se deklaruje informace o kompromitování, stanovení odpovědností za nedokonalost identifikace kompromitovaného uživatele, resp. za ignorování dostupné informace o kompromitaci, způsoby správy kompromitovaných dat mezi doménami PKI, rozhodnutí o tom které materiály se musí archivovat a jak dlouho, rozhodnutí o tom, kdo a kde provádí protokolování a co se protokoluje, které protokoly se pro účtování (protokolování) a archivaci použijí, stanovení odpovědností za údržbu archivů, rozhodnutí o tom, co podléhá auditu a kdo audit provádí, rozhodnutí o procesu podpory generování klíčů (lokálně nebo globálně, jak silnými mechanismy, jak se bude proces generování klíčů certifikovat, jak se budou chránit privátní klíče a jak budou stanoveny odpovědnosti), rozhodnutí o tom, zda celá procedura obnovy klíčů (dat) bude prováděna v rámci infrastruktury PKI nebo mimo ni, veškeré požadavky zmíněné v paragrafech této správy popisující požadavky na CP z hlediska správy certifikátů (od žádosti po vydání, revokace, prokazování platnosti, publikování atd.), rozhodnutí o dostupnosti technické podpory z hlediska času (trvale, pouze v pracovní době atd.).

7 Závěr

O PKI se v mnohých publikací tvrdí, že je generickou nepominutelnou komponentou distribuovaných informačních systémů, ve kterých mezi sebou musí důvěryhodně komunikovat vzájemně nezávislé entity (takovým systémem je např. jak systém pro elektronické obchodování, tak i systém státní správy), protože prokazování jejich identity je založeno použití ASK. PKI se přitom mnohdy chápe jako nakupovaný produkt, jehož pořízením a zapojením do informačního systému se významně přispěje ke zaručení bezpečnosti transakcí. Je vhodné upozornit na skutečnost, že takové zjednodušené zevšeobecnění může být v konkrétních situacích nebezpečné. Bezpečnost v IS je proces, nikoli předmět, bezpečnost IS je dána celou škálou na sebe navazujících dynamických faktorů (vč. lidského faktoru) a jeho bezpečnost je dána bezpečnostní nejslabšího článku takového řetězu.

Zvláště důležitou roli hrají v PKI certifikáty – jak jsou bezpečné a pro jaké použití je lze považovat za bezpečné. PKI v současnosti přebraly „štafetový kolík“ protagonistického produktu bezpečnosti po firewallech, systémech detekce průniků a VPN. Rizika plynoucí z dále zmíněných problémů použití PKI lze snižovat (nikoli odstraňovat) vhodně volenou bezpečnostní politikou.

8 Reference

1. Adams Carlise, Lloyd Steve: *Understanding Public-Key Infrastructure*, New Riders, 1999, ISBN 1-57870-166-x
2. Chokhani S., CygnaCom Solutions, Inc., W. Ford, VeriSign, Inc., *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework,* ftp://ftp.isi.edu/in-notes/rfc2527.txt, March 1999
3. Haber S., Stornetta W.S., *How to time-stamp a digital document*, CRYPTO Q90 Springer-Verlag 1991, *Journal of Cryptology*, Vol. 3, No. 2, pp. 99-111, 1991.

4. Hanáček Petr, Staudek Jan: *Bezpečnost informačních systémů, Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*, ISBN 80-238-5400-3, Úřad pro státní informační systém, Praha, 2000.
5. Draft CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

9 Použité zkratky

ASK		asymetrická kryptografie
AA	Attribute Authority	
ARL	Attribute Certificate Revocation List	
CA	Certificate Authority,	certifikační autorita
CIMS	Certificate Issuing and Management System	
CP	Certificate Policy,	certifikační politika
CPS	Certificate Practice Statement,	certifikační prováděcí směrnice
CRL	Certificate Revocation List	
CSP	Common Security Protocol	
CKL	Compromised Key List	
DNS	Domain Name Service	
DIT	Directory Information Tree	
DSS	Digital Signature Standard	
EC	Electronic Commerce	
ECA		externí certifikační autorita
EDI	Electronic Data Interchange	
EE	End entities	
FQDN	Fully Qualified Domain Name	
IETF	Internet Engineering Task Force	
IT		informační technologie
KCA		kořenová certifikační autorita
KEA	Key Encryption Algorithm	
KEK	Key Encryption Key	
LDAP	Lightweight Directory Access Protocol	
LRA	Local Registration Authority	lokální registrační autorita
MAC	Message Authentication Code	
MIME	Multipurpose Internet Mail Extensions	
MSP	Message Security Protocol	
OCSP	On-line Certificate Status Provider	
	On-line Certificate Status Protocol	
OID	Object Identifier	
OSI	Open Systems Interconnection	
PAA	Policy Approving Authority	
PGP	Pretty Good Privacy	
PKI	Public Key Infrastructure	
PMA	Policy Management Authority	
RA	Registration Authority	registrační autorita
SDSI	Simple Distributed Security Infrastructure	
S/MIME	Secure MIME	
SPA	Signature Policy Authority	
SPKI	Simple Public Key Infrastructure	
SSL	Secure Socket Layer	
TEK	Traffic Encryption Key	
TRA	Threat Risk Assessment	
TSA	Time Stamping Authority	
TSP	Trusted Service Provider	
TTP	Third Trusted Party	
UBS	UNCLASIFIED but Sensitive	