Kment Consulting

Elektronický podpis v ČR

Kapitoly 1 – 2

Analýza technického a právního stavu a související doporučení pro používání elektronického podpisu v podmínkách České republiky – říjen 2006

*Vojtěch **KMENT CONSULTING***

Revize 4.01
Říjen 2006

1. Úvod

Tato kapitola pojednává o účelu a obsahu studie.

1.1 Účel studie

Elektronický podpis je snadno chápán v abstraktní rovině, je přijatelně srozumitelný v základech své teorie, avšak značně složitý při snaze o důvěryhodnou, bezpečnou a právně vyhovující implementaci.

Zákon moudře stanoví, že podepisující osoba má mít při podpisu „pod svou výhradní kontrolou“ prostředek, se kterým elekronický podpis vytváří. Příkaz můžeme v analogii vyložit ve dvou rovinách, buď jednodušeji jako „ovládání auta“ řidičem, nebo složitěji jako „podrobnou znalost“ konstruktéra, který provedení auta rozumí natolik dobře, že si při jeho pořizování, provozu i používání bude stále vědom valné většiny potenciálních slabin součástí, které by mohly oslabit jeho technickou nebo právní schopnost auto skutečně ovládat.

Tato studie svého uživatele vybavuje znalostmi pro „ovládání“ druhého uvedeného typu.

Obsahuje výklad z několika disciplin (kryptologie, právo, počítačové inženýrství, standardy, ekonomika), které jsou jednotlivě i všechny společně relevantní pro každého, kdo se pokouší kvalifikovaně provádět vývoj, nasazování nebo implementaci aplikace elektronického podpisu nebo řídit její pořizování.

Studie umožňuje seznámit se s problematikou a osvojit si potřebné znalosti v reálně zvládnutelném čase.

Pořizovatel elektronického podpisu je v jiné situaci než uživatel auta. Kryptologické algoritmy realizované výpočetními prostředky mají nehmotnou povahu. Nevyskytují se pouze vady, ale i aktivní útoky. Výrobní, dodací a provozní kontroly se proto nakonec formují do jiného způsobu provádění a organizace než jsme běžně zvyklí z tradičních oborů, ale i běžného používání informačních technologií.

Studie zprostředkovává informace z této nové oblasti. Jejím účelem je poskytnout vzdělání svým příjemcům, kteří si mohou vytvořit i přesnější představu o správné míře důvěry v různá řešení.

1.2 Adresáti studie

Studie je vytvořena a určena pro použití osobami v organizacích, firmách a společnostech, které zvažují použití nebo hledají aplikační oblast elektronického podpisu, připravují návrhy nebo projekty, provádějí implementaci projektů nebo rozhodují o použití elektronického podpisu.

Hlavní adresáti:

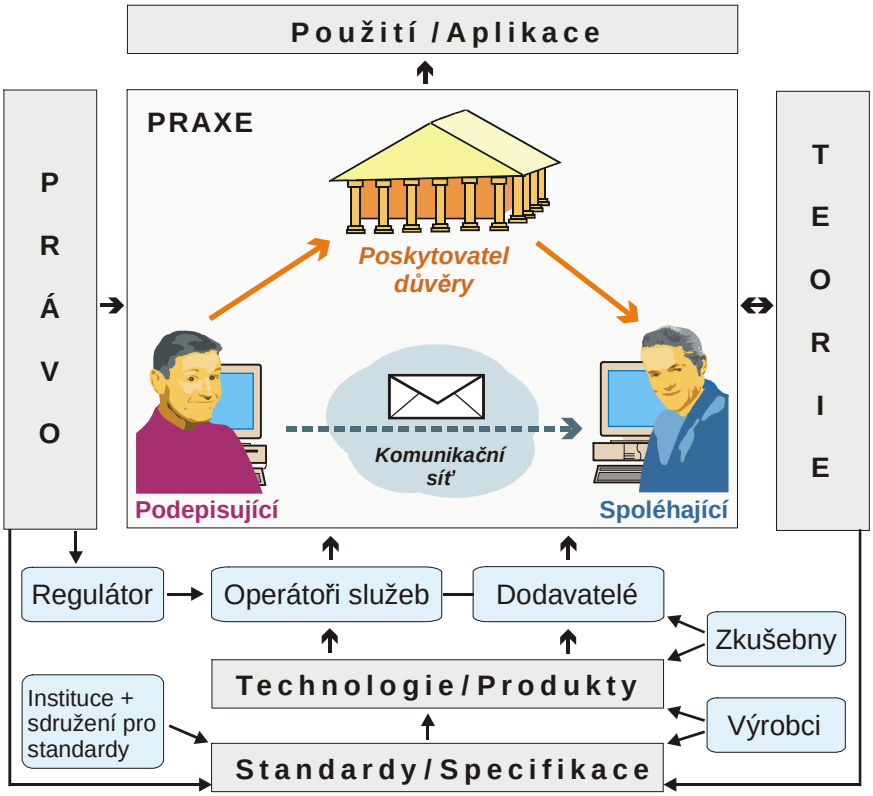
- Vedení oddělení IT (ICT).
- Manažeři projektů IT.
- Vývojáři SW popř. i HW aplikací.
- Analytici SW projektů.
- Konzultanti IT.
- Specialisté bezpečnosti IT.
- Pracovníci z firem dodavatelů produktů a služeb ICT.

Další adresáti:

- Management společností a firem.
- Vedení úřadů státní správy a veřejné samosprávy.
- Právníci, advokáti aj. osoby zabývající se právem, legislativou nebo vnitřními předpisy.
- Marketéři a obchodníci se zaměřením na strategii prodeje.
- Pracovníci logistiky a výroby.
- Další vážní zájemci o e-podpis.

1.3 Obsah studie podle hlavních struktur oblasti

Implementace elektronického podpisu potřebují multidisciplinární know-how. V oblasti zároveň působí řada různých druhů subjektů, je v ní poskytováno více druhů služeb a produktů, které jsou vázány na technické standardy i právní předpisy. Studie poskytuje systematický výklad o všech těchto strukturách.



Obr. 1-1 Elektronický podpis: doména mezi více obory a více subjekty

Teorie. Teoretický rámec poskytuje kryptologie. Studie se jí zabývá nejprve na úrovni zcela přístupné laikům v kapitole 2. Znalosti prohlubuje v kapitole 10, ve které seznamuje se základními odbornými pojmy pro další orientaci čtenáře v odborné literatuře, poskytuje odkazy na normativní dokumenty a seznámení se s podstatou a podrobnostmi vybraných kryptografických algoritmů. Studie podává rovněž výklad jazyka ASN.1 (kapitola 11), který se používá pro popis mnoha kryptografických struktur.

Právo. Ačkoliv principy stanoví kryptologie, je to právo, které je zastřešujícím normativním systémem společnosti a které rozhoduje o použitelnosti elektronického podpisu. Právo upravuje požadované vlastnosti právními předpisy a z nich vedoucími odkazy na technické standardy a specifikace. Studie obsahuje výklad evropského rámce, českých zákonů a dalších předpisů, včetně reflexe důsledků interpretace zpět až na technickou nebo teoretickou rovinu. Zabírá téměř třetinu obsahu, kapitoly 6 a 7.

Standardy / Specifikace. Těžiště druhu informací studie zabírající asi 43% obsahu. Ze standardů vycházejí technologie a produkty, ve kterých se potřebujete vyznat pro vlastní vyvoj i při pořizování od dodavatelů. Standardy pokrývají mnoho různých oblastí, jsou nezbytné pro funkčnost, kompatibilitu, bezpečnost a záruky bezpečnosti. Standardy a specifikacemi se zabývají kapitoly 8, 9, 12 - 17.

Organizační rámec. Uvedené právní předpisy a technické standardy jsou i zdrojem informací o druzích subjektů a organizačních vztahů mezi nimi. Zvláštní přehled významných organizací podává kapitola 18.

Ekonomie a aplikace. Ekonomické argumenty pro nasazování elektronického podpisu. V jakých druzích aplikací se elektronický podpis nejvíce prosazuje a proč. Hlavní druhy ekonomických přínosů při použití. Typické náklady. Druhy rizik a jejich eliminace. Zejména kapitoly 5 a 4.

Neutrálnost pohledu. Konkrétním produktům, technologiím nebo výrobcům se studie věnuje v nezbytné míře pro nabytí rychlé praktické zkušenosti a přehledu, v kapitolách 3, 4 a 16.

Zaostřenost na obecné organizace a potřeby. Malá míra pozornosti je záměrně věnována úpravám řešení vztahů mezi regulátorem a poskytovateli certifikačních aj. služeb, a vnitřnímu chodu provozovatelů těchto služeb, neboť tyto záležitosti jsou současně velmi komplexní a týkající se jen několik subjektů. Ve studii však jsou probrány ty záležitosti poskytovatelů, které mají přesah vůči uživatelům jejich služeb (zejména kapitoly 3, 4, 6, 7), např. odpovědnost.

1.4 Obsah studie podle kapitol

1. ÚVOD

Tato úvodní kapitola o účelu a obsahu studie.

2. ÚVOD DO ELEKTRONICKÉHO PODPISU

Úvod do tématiky digitálního a elektronického podpisu na obecné úrovni, dostupné všem čtenářům. Seznámí s principy, koncepty a základní terminologií výkladem od jednoduššího ke složitějšímu.

3. PRAKTICKÝ POSTUP PŘI POUŽITÍ ELEKTRONICKÉHO PODPISU

Vhodné zásady bezpečnosti pro vyzkoušení nebo používání elektronického podpisu, podrobně rozepsané krok za krokem formou „Best Practice“. Obecné postupy nezávislé na konkrétním produktu. Rozdělení na stranu podpisující a na stranu spoléhající (ověřující), rozčlenění do hlavních fází, ty do kroků.

4. TRŽNÍ SUBJEKTY V OBLASTI ELEKTRONICKÉHO PODPISU V ČR

Rychlá orientace na trhu služeb a produktů elektronického podpisu v ČR. Členění podle kategorie produktů a služeb. Přehled tří akreditovaných certifikačních autorit, hierarchie jejich certifikátů, základů služeb a certifikačních politik. Přehled dalších kategorií a firem v těchto kategoriích v ČR působících.

5. EKONOMIE APLIKACÍ A POUŽITÍ ELEKTRONICKÉHO PODPISU

Manažerský a ekonomický pohled na vývoj a pořizování aplikací s elektronickým podpisem. Určení hlavních trhů, na nichž se elektronický podpis využívá, příčiny a popis. Hlavní výhody nasazení elektronického podpisu a jejich měření. Typické náklady. Rizika falsifikace elektronického podpisu. Hrozby při komunikaci, které elektronický podpis odstraňuje.

6. PRÁVNÍ RÁMEC ELEKTRONICKÉHO PODPISU V EVROPSKÉ UNII

Právní rámec přijatý Evropským společenstvím pro harmonizaci práva členských států. Výklad pojmů a především hlavních principů evropské směrnice 1999/93/EC, která tvoří pojmový i metodologický základ, který se transponuje do právního řádu České republiky. Přehled dalších platných předpisů ES. Srovnání evropského pojetí s bezpečnostními službami a mechanismy v mezinárodních normách.

7. ELEKTRONICKÝ PODPIS V PRÁVNÍM ŘÁDU ČESKÉ REPUBLIKY

Právní řád jako zastřešující normativní systém, s rozhodným účinkem pro posuzování přípustnosti použití elektronického podpisu, jeho vlastností a použití jako důkaz v právním řízení. Podrobný výklad zákona č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů, včetně jeho prováděcích předpisů. Soukromoprávní použití elektronického podpisu v otevřených systémech. Veřejnoprávní použití elektronického podpisu podle dalších devíti zákonů a prováděcích předpisů.

8. VYBRANÉ EVROPSKÉ NORMY A DOPORUČENÍ

Popis hlavních standardů a doporučení přijatých evropskými normalizačními institucemi a pracovními skupinami. Tyto dokumenty obsahují řadu velmi užitečných profilací existujících standardů nebo nástinů řešení mnohých závažných problematik. Vhodná struktura formátů pro elektronické podpisy různých druhů. Popis doby latence při zneplatňování certifikátů. Profil pro zařízení pro bezpečné vytváření elektronického podpisu. Struktura aplikace vytvářející podpis a aplikace ověřující podpis.

9. HODNOCENÍ ZÁRUKY BEZPEČNOSTI PROSTŘEDKŮ A NÁSTROJŮ

Metodologie hodnocení prostředků a nástrojů elektronického podpisu, která umožňuje stanovit záruky bezpečnosti implementací. Metodologie Common Criteria (ISO 15408) a FIPS 140. Hodnocení záruk

bezpečnosti na úrovni EAL 4+. Možnosti vedení útoků na implementace kryptografických modulů a poučení z toho plynoucí pro jejich nasazení a používání.

10. ALGORITMY PKI PRO ELEKTRONICKÝ PODPIS V ČR

Rozvinutí teorii elektronického podpisu z kapitoly 2. Podává podrobnější výklad kryptologických pojmů, se kterými se lze v oblasti elektronického podpisu setkat. Provádí přehled kryptografických algoritmů a funkcí stanovených vyhláškami č. 366/2001 Sb, č. 496/2004 Sb. a č. 378/2006 Sb. a udává jejich normativní zdroje. Přibližuje principy vybraných kryptografických algoritmů RSA(bližší podrobnosti o formátování jsou v kapitole 13 o PKCS #1), DSA a hašovacích funkcí SHA-1 a některých dalších.

11. ASN.1 – ABSTRAKTNÍ SYNTAXOVÁ NOTACE JEDNA

Seznámení s účelem a výklad jazyka ASN.1, s jehož pomocí jsou definovány datové struktury zejména ve standardech X.509 a PKCS #, odkud jsou přebírány do internetových aj. specifikací. Existující kódovací pravidla. Výčet standardů. Základní metody vývoje aplikací se strukturami v ASN.1.

12. FORMÁTY PODEPISOVANÉHO OBSAHU

Zjištění nároků na formáty obsahu dat, aby byly vhodné pro elektronický podpis. Přehled požadavků na formáty obsahu v předpisech ČR a SR. Podrobné vlastnosti formátů: TXT, MIME plain/text, RTF, MIME text/enriched, PDF, HTML a XML. Podpisový formát XML Signature. Hlavní existující kódování znaků a jejich trendy.

13. STANDARDY PKCS

Popis PKCS #1 až PKCS #15. Podrobný popis standardu PKCS #1, který je základem využití nejpoužívanějšího asymetrického kryptografického algoritmu RSA. Kryptografie pro použití hesel, syntaxe žádosti o certifikát, programovací rozhraní tokenu (Cryptoki), formát pro výměnu klíčů a certifikátů, formát obsahu kryptografického tokenu aj. Způsob použití standardů a jejich perspektivy.

14. INTERNETOVÉ STANDARDY

Úvod do systému organizace a postupů vytváření úspěšných internetových specifikací. Vývoj specifikací RFC pro elektronický podpis a jejich hlavní druhy. Struktura kryptografické zprávy CMS. Formáty internetové elektronické pošty od RFC 822 přes MIME až k S/MIME. Formát OpenPGP a jeho slabina. Pracovní skupina PKIX. Slepá vývojová větev PEM. Formát pro časové razítko.

15. CERTIFIKÁTY X.509

Průvodce spletitou historií a významem součástí certifikátů X.509. Orientace ve standardizačních variantách standardu X.509. Přípravný výklad pojmů, používaných v rodině X.500 a X.509, jejichž pochopení je jinak obtížné. Formát certifikátů X.509 v3 – základní obsah a rozšíření podle hlavních internetových profilů. Formát CRL v2. Protokol OCSP pro on-line ověřování stavu platnosti certifikátu.

16. PRŮMYSLOVÉ STANDARDY

Znalosti o tržně prosazených průmyslových standardech. Architektura kryptografického systému v Microsoft Windows sestávající z CryptoAPI, subsystému čipových karet a rozhraní CAPICOM. Informace o dalších průmyslových standardech jako SET a EMV pro finančnictví, SSL, CEPS, JavaCard, MULTOS, OCF a ISO 7816.

17. PC/SC – PERSONAL COMPUTER / SMART CARD

Seznámení s vícevrstvou architekturou PC/SC pro kryptografické čipové karty. Podle ní je vytvořena kryptografická architektura čipových karet v Microsoft Windows. Revize PC/SC 2.0. Funkce a rozhraní. Párování ovladač – čtečka a CSP – karta. Implementace bezpečných čteček - bezpečné PIN.

18. VÝZNAMNÉ ORGANIZACE V OBLASTI E-PODPISU

Určení a orientace mezi několika desítkami organizací, jejich vztahy a vliv na rozvoj elektronického podpisu. Identifikace jejich dokumentů a hlavní vydané specifikace, doporučení a normy. Přehled a informace v rozčlenění na evropské, české, slovenské, americké a mezinárodní organizace.

1.5 Obsah studie podle dílčích potřeb

Právo a smlouvy. Práva a povinnosti podpisujících a spoléhajících. Viz zejména kapitolu 7 popř. též kapitolu 6.

Zákon o elektronickém podpisu (odst. 7.3) tvoří základní veřejnoprávní úpravu a též obecný rámec pro "otevřené" soukromoprávní systémy. Pro jiné soukromé systémy je možné si v souladu s občanským zákoníkem (odst. 7.4.1) sjednat smluvní podmínky.

Veřejnoprávní použití s úřady je dále upraveno v řadě dalších zákonů: správní řád (odst. 7.4.3), zákon o archivnictví a spisové službě (odst. 7.4.4), zákon o správě daní a poplatků (odst. 7.4.5), zákon o účetnictví (odst. 7.4.6), zákon o dani z přidané hodnoty (odst. 7.4.7), občanský soudní řád (odst. 7.4.8), soudní řád správní (odst. 7.4.9), trestní řád (odst. 7.4.10), trestní zákon (odst. 7.4.11) a v dalších předpisech.

Podpisové algoritmy. Obecný úvod je v kapitole 2. Teorie a termíny algoritmů jsou podrobněji rozebrány v odst. 10.1, vybrané algoritmy: RSA (odst. 10.5.1) + formáty PKCS #1 (odst. 13.1), DSA (odst. 10.5.2), SHA-1 (odst. 10.5.3) a další ve zbytku kapitoly 10.

Podpisové schema. Je kombinace asymetrického podpisového algoritmu a některé hašovací funkce, popř. dalších požadavků. Pro výklad podpisového schematu viz odst. 10.1.1. Přehledy předpisy požadovaných schemat jsou v odst. 10.2 až 10.4. Prakticky se prosazují pouze podpisová schemata s algoritmem RSA, z hašovacích funkcí nyní obsahující SHA-1, výhledově z rodiny SHA-2.

Podpisový formát. Je formát dat použitý pro spojení dat obsahu datové zprávy a dat elektronického podpisu z podpisového schematu. Do úvahy přichází čtyři základní možnosti:

- podpis v rámci obecné datové struktury CMS (odst. 14.2),
- podpis v rámci S/MIME (odst. 14.3), který vychází z CMS - hodí se pro poštovně orientované systémy, existuje používaná subvarianta s tzv. odloučeným podpisem,
- podpis v rámci XML Signature (odst. 12.6), hodí se pro formulářově strukturovaná data,
- podpis v rámci formátu PDF (odst. 12.5.5), kompaktní řešení,

nebo i další, méně obvyklá řešení:

- podpis v rámci OpenPGP (odst. 14.4),
- podpis v rámci EDIFACT (pouze odst. 5.2.3).

Formát obsahu, dokumentu. Při výběru formátů pro podpis je vhodné být opatrný a pokud možno vybírat jednoduché a jednoznačné formáty. Formáty obsahu se zabývá kapitola 12.

Bezpečný podpisový prostředek. Viz zejména odst. 8.5 a odst. 9.1. V ČR zatím nepovinný.

Praktické kryptografické tokeny a čtečky. Situace na českém trhu viz odst. 4.2 až 4.4, kryptografický systém Windows viz odst. 16.1, specifikace PC/SC viz kapitolu 17, rozhraní tokenu PKCS #11 / Cryptoki viz odst. 13.9.

Volba certifikační autority. Pro působící akreditované PCS v ČR viz odst. 4.1.

Formát žádosti o certifikát. Formát PKCS #10 (odst. 13.8). Viz též obsah certifikátu níže.

Obsah a druhy certifikátů. Certifikáty podle standardu X.509 se zabývá kapitola 15. Vzácně je možné využít alternativní certifikáty ve formátu OpenPGP (odst. 14.4).

Certifikační politika. Přehled předpisů pro certifikační autority viz odst. 8.2, dále viz odst. 15.1 až 15.4 pro obsah certifikátu X.509.

Podpisová politika. Prakticky i právně neprosazený přístup. Viz odst. 8.3.

Vytvoření podpisu. Vhodná struktura aplikace viz odst. 8.7, právní povinnosti podepisujícího viz odst. 7.3.5 a 7.3.6.

Ověření podpisu. Vhodná struktura aplikace viz odst. 8.7, potíže s dobou latence (odst.8.4), právní povinnosti spoléhajícího viz odst. 7.3.7, použití CRL (odst. 15.5), použití OCSP (odst. 15.6).

Vývoj aplikace s e-podpisem. Prakticky celá tato studie, zejména kapitoly 8, 11, 13, 14, 16.

Elektronická podatelna. Vnitřní chod elektronické podatelny podle předpisů je popsán v odst. 7.3.12, známí dodavatelé v ČR viz odst. 4.8.

Elektronická značka. Viz odst. 7.3.13.

Časová razítka. Viz odst. 7.3.14 a odst. 14.7.

Archivační podpisy. Viz odst. 8.1.3.vii a odst. 7.4.4.

Rizika. Viz odst. 5.5 a kapitolu 9, zejména odst. 9.3.

Průzkum trhu. Viz kapitolu 4.

Vyhodnocení přínosů. Viz kapitolu 5.

2. Úvod do elektronického podpisu

Elektronický podpis v současnosti spočívá v podstatě téměř výhradně na technologii tzv. digitálního podpisu, elektronicky implementovaného. Podklad jeho teorie se opírá o tzv. *kryptografii veřejného klíče* PKC (Public Key Cryptography, ještě častěji snad označovanou za *infrastrukturu veřejného klíče* PKI (Public Key Infrastructure); toto druhé označení preferuje i tento text.

Použití PKI pro elektronický podpis předepisují všechny relevantní evropské a tuzemské právní předpisy a technické standardy.

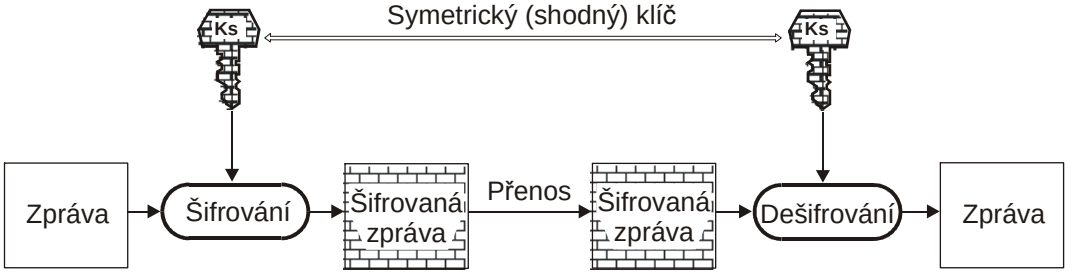
V této kapitole jsou vysvětleny principy PKI pro zcela laickou úroveň pochopení, s ohledem na použití PKI pro aplikaci elektronického podpisu. Úroveň popisu v této kapitole má zcela obecný charakter, bez přímého vztahu k právním předpisům nebo technickým standardům. Kapitola podává tematiku ve zjednodušené podobě pro konceptuální pochopení, na hlavní použitá zjednodušení je však upozorněno. V tematice zběhlí čtenáři mohou přejít na další části studie, v níž jsou součásti PKI vyloženy hlouběji.

2.1 Symetrické a asymetrické šifry

Metodika PKI se zrodila v kryptografii, což je odvětví matematiky a moderně též počítačových věd, které se historicky především zabývalo šifrováním informací, utajením obsahu nějaké zprávy. Ještě než se dostaneme k samotnému PKI, podíváme se na základní metodu šifrování zpráv, vůči nimž se PKI profiluje odlišně, avšak někdy se s ním též kombinuje.

Omezíme-li se na šifrování předem daných zpráv určité délky a obsahu, pak se pro tyto funkce v moderní době vyvinuly tzv. blokové šifry. Blokové se nazývají proto, že se dlouhá zpráva rozdělí do kratších bloků určité pevné délky a každý blok se šifruje zvlášť (s možným přenosem z předchozího bloku). Bloková šifra tak umožňuje bezpečně zašifrovat (téměř) libovolně dlouhou zprávu.

Pozn.: alternativou blokových šifer jsou šifry proudové, které v reálném čase šifrují určitou bitovou nebo znakovou posloupnost předem neznámé délky, bit po bitu nebo znak po znaku. Vzhledem k současnému paketovému pojetí většiny komunikace mají dnes podstatně menší význam než šifry blokové; pro tématiku elektronického podpisu se prakticky nepoužívají vůbec, neboť se předpokládá, že uživatel podepisuje kompletní zprávu, se kterou se předem seznámil, a nikoliv její vývoj za běhu.



Obr. 2-1 Symetrické šifrování

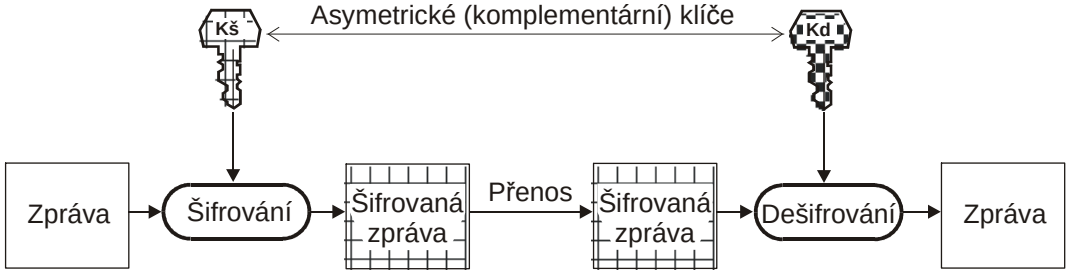
Rámcově je postup šifrování a dešifrování blokovou šifrou znázorněn výše. Podotkněme, že obrázek abstrahuje od vnitřní blokové organizace šifrovací i dešifrovací operace, zvýrazňuje však jinou záležitost, totiž přítomnost tajného klíče *Ks*. Rovněž se předpokládá, že šifrovací/dešifrovací algoritmus je veřejně znám. Tím se splňuje požadavek moderní kryptografie, aby utajení obsahu zprávy nespočívalo v tajnosti metody, kterou zpravidla lze dříve či později zjistit zpětným inženýrstvím nebo jinak, ale aby záviselo jen na tajnosti klíče a nemožnosti tento klíč zjistit, odvodit, nebo obsah zprávy dešifrovat jinak.

Obrázek má titulek „Symetrické šifrování“ neboť klíč *Ks* je shodný pro šifrovací i dešifrovací operaci. Takové klíče se pak též nazývají symetrické klíče, algoritmy se označují jako symetrické šifry. Mezi hlavní symetrické šifrovací algoritmy patří historicky DES, triple-DES a moderně AES. Úspěšnost šifrování spočívá tedy na schopnosti utajit šifrovací klíč *Ks*. S tím je spojen problém bezpečného předání (výměny) klíče mezi adresátem a odesilatelem. Zatímco zpráva je algoritmy zašifrována tak dokonale, že může být přenášena odposlouchávatelným kanálem, klíč musí být vyměněn nějak jinak, např. „z ruky do

ruky“, nebo bezpečným kanálem. Šifrování symetrickou šifrou též předpokládá vzájemnou důvěru mezi oběma komunikujícími stranami.

Zamyslíme-li se nad symetrickým šifrováním z hlediska požadavků, které se kladou na elektronický podpis, zejména tzv. nepopiratelnost původce zprávy, jasně prokazatelnou nezávislé třetí stráně, pak žádná symetrická šifra nemůže tento požadavek naplnit. Z pouhého předložení zašifrované a dešifrované zprávy nelze dokázat, která ze stran (odesilatel, adresát) zprávu vytvořila.

V sedmdesátých letech 20. století se proto rozvinulo nová kategorie šifrovacích algoritmů, které se, v kontrastu k symetrickým šifrám, označují jako asymetrické.



Obr. 2-2 Asymetrické šifrování

Ačkoliv situace vypadá na prvý pohled shodně, při pozorném pohledu se zjistí, že klíče jsou nyní dva! První klíč *Kš* je použit k zašifrování zprávy, druhý klíč *Kd* je použit k zpětnému dešifrování zprávy. Klíče *Kš* a *Kd* se používají vzájemně asymetricky, proto jsou tak nazývány. Oba klíče jsou navzájem různé, z hodnoty jednoho nelze odvodit hodnotu druhého klíče, hodnoty nicméně nejsou libovolné, ale jeden klíč musí komplementárně odpovídat hodnotě druhého. Též se proto někdy označují jako *klíčový pár* nebo *klíčová dvojice*.

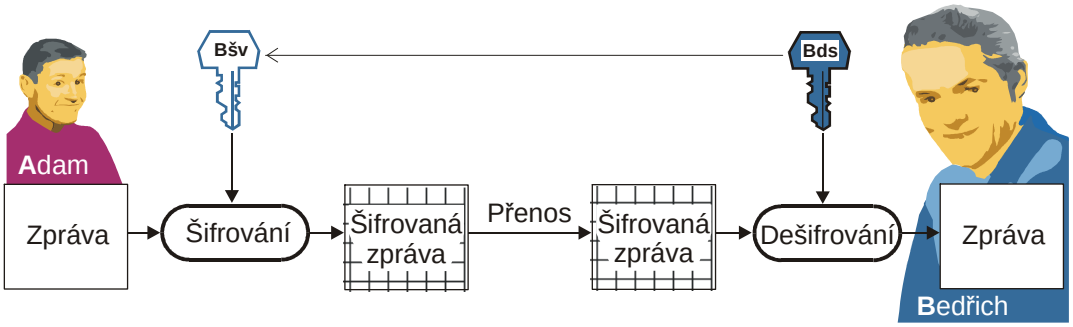
Mentální operace, kterou nyní s asymetrickými klíči můžeme učinit, je ta, že generaci klíčového páru (tj. obou klíčů) svěříme do rukou jen jedné ze stran, takže ta na počátku zná hodnoty obou klíčů. Následně jeden z klíčů z dvojice zveřejní. Tím se prvně dostáváme k pojmu „veřejného klíče“. Podle toho, který klíč zveřejní, je následně možné použít asymetrické šifrování k jedné ze dvou principiálních úloh:

- šifrování obsahu,
- digitální podpis obsahu,

popsaných v dalším odstavci.

2.2 Princip šifrování a elektronického podpisu s asymetrickou šifrou

Narozdíl od symetrického šifrování se u asymetrického nehovoří o tajném klíči, ale o klíčovém páru, z něhož utajovaný klíč bývá označován jako soukromý klíč (private key) a neutajovaný jako veřejný klíč (public key). Jak je avizováno výše, jsou v zásadě dvě možnosti, který klíč zveřejnit. Pro snazší orientaci je na dalších obrázcích veřejný klíč zobrazován vždy jako „bez výplně“.



Obr. 2-3 Šifrování s veřejným klíčem (pro Bedřicha)

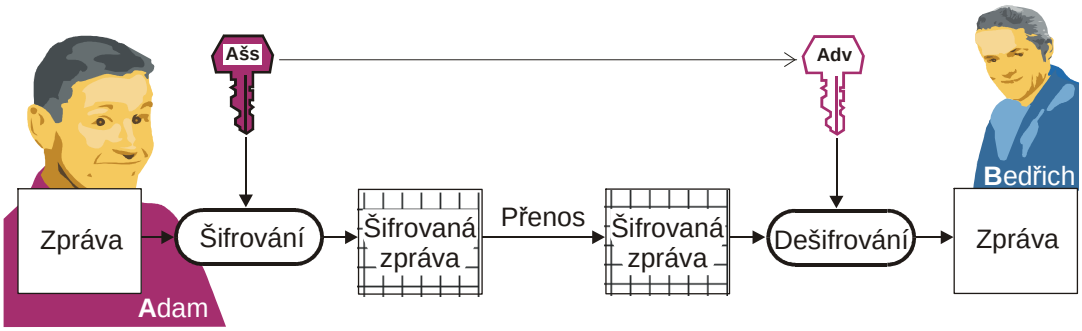
Pokud chce adresát (na obrázku výše Bedřich vpravo) přijímat zašifrované zprávy, vytvoří klíčový pár a jako svůj soukromý klíč si ponechá dešifrovací klíč *Bds* (Bedřich, klíč dešifrovací soukromý), zatímco

šifrovací klíč *Bšv* (Bedřich, klíč šifrovací veřejný) zveřejní a zašle všem svým protějškům (např. i zobrazenému Adamovi vlevo). Adam (ale i kdokoliv jiný) pomocí klíče *Bšv* zašifruje zprávu a zašle ji Bedřichovi. Ten ji svým soukromým klíčem *Bds* dešifruje.

Oproti obr. 2-1 (symetrické šifrování) má šifrování s veřejným klíčem dvě hlavní výhody:

- veřejný klíč může být odposlechnut, dostačuje zabezpečit integritu doručení klíče, tj. jeho nepozměnitelnost útokem muže uprostřed (tajný klíč nesmí být ani odposlechnut),
- pro šifrovanou komunikaci s mnoha (prakticky neomezeným počtem) protějšky dostačuje jediný klíčový pár, zatímco při symetrickém šifrování je zapotřebí zpravidla mít pro komunikaci s každým protějškem jeden zvláštní tajný klíč.

Asymetrické šifrování má i své nevýhody, zpravidla potřebu výrazně delších klíčů pro stejnou bezpečnost a zejména vyšší výpočetní náročnost. Proto je obrázek 2-3 idealizovaný. Kromě velmi krátkých zpráv se zasílání zpráv pomocí metod PKI provádí tak, že odesilatel vygeneruje náhodnou hodnotu pro tajný klíč, zpráva se tímto tajným klíčem zašifruje některou symetrickou šifrovací metodou, asymetrickou šifrovací metodou se zašifruje pouze tajný klíč, který se připojí ke zprávě. Adresát dešifruje nejprve hodnotu tajného klíče asymetrickou šifrou, s jeho pomocí pak dešifruje zbytek symetricky zašifrované zprávy. Dále obrázek též zanedbává různé otázky formátování všech dat zprávy.



Obr. 2-4 Digitální podpis (šifrování) s veřejným klíčem (od Adama)

Druhá principiální možnost je na obr. 2-4. Zde klíčový pár generuje vlevo Adam, tentokrát si jako soukromý ponechá šifrovací klíč *Ašs* (Adam, klíč šifrovací soukromý) a veřejný klíč *Adv* (Adam, klíč dešifrovací veřejný) rozšíří všem svým protějškům, např. i Bedřichovi.

Pokud pak klíčem *Ašs* zašifruje některou zprávu, pak příjemce je schopen klíčem *Adv* zprávu dešifrovat. Protože klíč *Adv* bývá veřejný a „dešifrování“ tak může provést kdokoliv, nelze zde vážně hovořit o tom, že by obsah zprávy byl šifrován. Z faktu, že „rozumnou zprávu“ lze dešifrovat právě klíčem *Adv*, který pochází od Adama a jenom Adam má v držení klíč *Ašs*, takže pouze Adam mohl takto „zašifrovat“ zprávu, lze tedy soudit, že zpráva je od Adama, tj. „Adam ji podepsal“.

Opět je zapotřebí dodržet zásadu integrity doručení veřejného klíče, aby si Bedřich mohl být jist tím, že mu nebyl podsunut mužem uprostřed klíč od někoho jiného.

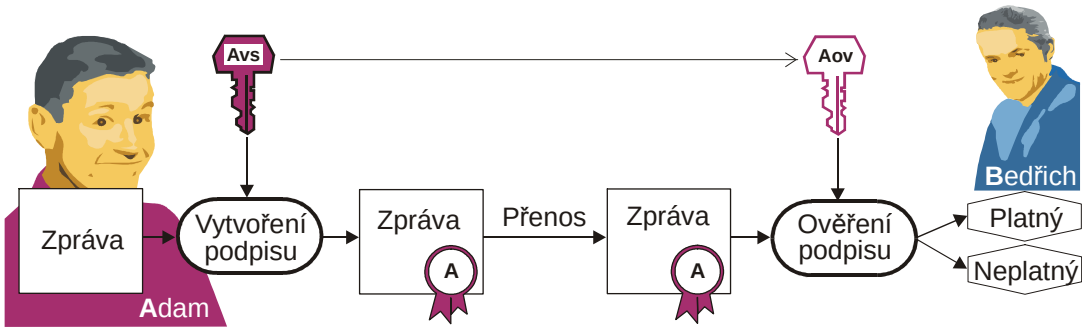
Narozdíl od symetrického šifrování nyní platí, že soukromý klíč je v dispozici pouze jediné osoby (zde Adama), takže Adam nemůže popírat, že zpráva je od něj.

Pozn.: Adam má v zásadě možnost popírat autorství podpisu dvěma způsoby: může namítnout únik klíče anebo podsunutí (vizuálně apod.) jiné zprávy než chtěl podepsat. Oběma těmto druhům námitek musí právní předpisy a technické standardy účinně bránit, jinak koncept podpisu v právní úrovni neobstojí.

Tak jako obr. 2-3 je i obr. 2-4 zjednodušen pro konceptuální pochopení. Opět chybí jakékoliv formátování podpisované zprávy, které je nutné. Uvedený způsob „podpisu“ by pak opět mohl být použit pouze u krátkých zpráv, v praxi se šifruje/dešifruje nikoliv samotná zpráva, ale její otisk (haš hodnota). Pro podrobnosti viz kapitolu 10.

Konečně, značné zjednodušení je též v tom, že se předkládá, že podpisový algoritmus má nativní šifrovací/dešifrovací schopnosti. Tak je tomu pouze u algoritmu RSA, který je sice nejrozšířenější

a nejznámnější, ale obecně s touto vlastností podpisové asymetrické algoritmy vytvářeny (většinou záměrně) nejsou.



Obr. 2-5 Operace digitální podpisu (od Adama): vytvoření a ověření podpisu

Na operace podpisu s pomocí asymetrických šifrovacích algoritmů je proto vhodnější nahlížet přes symboliku a názvy operací dle obr. 2-5. Adam si generuje dvojici klíčů pojmenovaných zde *Avs* (vytváření podpisu, soukromý) a *Aov* (ověřování podpisu, veřejný). Při operaci vytváření podpisu se typicky provádí získání otisku (haš) zprávy, na který se aplikuje asymetrická operace vytvoření podpisu, se vstupním parametrem soukromého klíče podpisujícího. Podpis se ke zprávě ve vhodném formátu přidá (symbolizováno pečetí s iniciálou A) a zašle protějšku (např. Bedřichovi). Bedřich musí mít nejpozději v okamžiku počátku ověřování k dispozici důvěryhodně získaný veřejný klíč *Aov* Adama. Operace ověření provede rozdělení na zprávu a podpis a určitým postupem, jehož vstupem je veřejný klíč, zjistí, zda podpis zprávě odpovídá. Výsledkem je nakonec rozhodnutí, zda podpis je platný nebo nikoliv.

Na závěr se lze zabývat tím, zda je možné zároveň šifrovat obsah a podepisovat zprávu kombinací výše uvedených metod. Je to možné, nicméně je dobře si být vědom několika záležitostí:

- šifrování obsahu není v souvislosti s elektronickým podpisem a komunikací vůči úřadům v ČR nijak upraveno právními předpisy,
- šifruje se veřejným klíčem adresáta, podepisuje se soukromým klíčem podpisujícího, dešifruje se soukromým klíčem adresáta, ověřuje se podpis veřejným klíčem podpisujícího,
- pro podpisování a šifrování by se ale měly používat odlišné párové dvojice, v praxi umožňuje použití jediné párové dvojice algoritmus RSA (tzn., že u RSA může být pro Adama *Ads=Ašs* a *Ašv=Adv*), nicméně ani zde to není metodicky správné,
- klíčová dvojice pro podpis by se neměla používat ani pro jiné účely jako je např. autentizace on-line sezení (např. pro SSL apod.).

Pro praxi je technicko-právně důležité zajistit i to, aby podpisující pokud možno nemohl uplatnit výše uvedené námitky úniku klíče nebo podsunutí zprávy.

2.3 Včlenění certifikační autority a vznik PKI

Ve výše uvedených obrázcích 2-3 až 2-5 jsme předpokládali, že každý má k dispozici veřejný klíč protějšku se zaručenou integritou klíče, klíč protějšku je důvěryhodný. Oproti přenosu symetrického klíče je u asymetrických šifer předávání klíče mnohem jednodušší, svůj veřejný klíč můžete zveřejnit třeba na svých webových stránkách a bude-li chtít někdo ověřit, že mu nebyly podsunuty jiné stránky, může ověřit otisk klíče např. telefonicky nebo jiným na internetu nezávislým kanálem.

Přesto by takové šíření klíčů bylo problematické a to ze dvou důvodů:

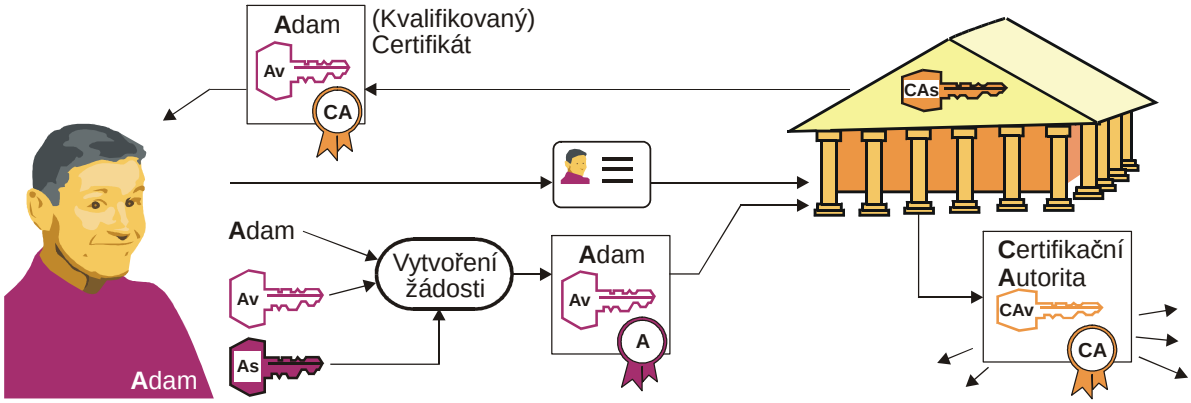
- při velkém počtu komunikujících partnerů obnáší individuální ověřování stále zátěž,
- při rozhodování třetí strany o nepopiratelnosti podpisu by tato rozhodčí třetí strana měla potíž rozhodnout jaký klíč podpisující ověřujícímu poskytl.

Tyto potíže se řeší tím, že se mezi vzájemně komunikující partnery včlení organizace běžně zvaná *certifikační autorita*. Tím se vytvoří méně či více složitá infrastruktura, která se označuje zkratkou PKI.

Znázornit plné schéma postupů je složité, proto je proces komunikace prostřednictvím certifikační autority (CA) rozložen do tří obrázků, znázorňujících samostatné a typické úlohy komunikace s CA.

2.3.1 Žádost o certifikát u certifikační autority

Každý podpisující, ještě předtím než se začne elektronicky podepisovat, musí napřed od některé certifikační autority získat elektronický certifikát. V případě zájmu o vyhovění právním předpisům bude mít zájem především o tzv. kvalifikovaný certifikát, který splňuje poměrně náročné požadavky na obsah, proceduru ověření údajů do certifikátu vkládaných i zázemí certifikační autority. Do certifikátu pro podpisujícího (i pro většinu jiných účelů v PKI) se vždy přinejmenším vkládá nějaký způsob identifikace osoby a veřejný klíč certifikované osoby. Hovoří se proto o tzv. certifikátech veřejného klíče.



Obr. 2-6 Žádost a získání (kvalifikovaného) certifikátu od certifikační autority

Požadované údaje do certifikátu (zde např. „Adam“) a veřejný klíč certifikovaného se proto napřed vkládají do elektronické žádosti, která je podepsána soukromým klíčem certifikovaného (pečeť s „A“). Certifikační autority udávají přesný formát a obsah žádostí, které přijímají, většinou přitom je nutné použít nějakou webovou nebo desktopovou aplikaci, připravenou certifikační autoritou. Vytváření žádosti bývá spojeno s těsně předchozí generací klíčů podpisujícího, dohromady jako tzv. enrollment. Soukromý klíč se přitom zpravidla vytváří na výpočetním prostředku, který má podepisující ve své moci, ideálně na kryptografické čipové kartě nebo tokenu, které jsou v přiměřeně zabezpečené platformě např. osobního počítače, PDA apod.

Poté, co je žádost vytvořena, se certifikovaná osoba musí, zpravidla fyzicky, dostavit na tzv. registrační místo (též nazývané registrační autorita), kde předloží vygenerovanou žádost v elektronické podobě, svůj identifikační průkaz (typicky dva nezávislé průkazy) a průkazní dokumenty, kterými dokládá pravdivost dalších případných údajů (nazývaných též atributy nebo znaky) uváděných do certifikátu.

Následně certifikační autorita vydá (kvalifikovaný) certifikát. Certifikát vždy předá do dispozice podepisujícího, např. poskytnutím na médiu nebo zasláním na adresu elektronické pošty. Podepisující tak má možnost zaslat svůj certifikát individuálně každému protějšku, se kterým chce komunikovat.

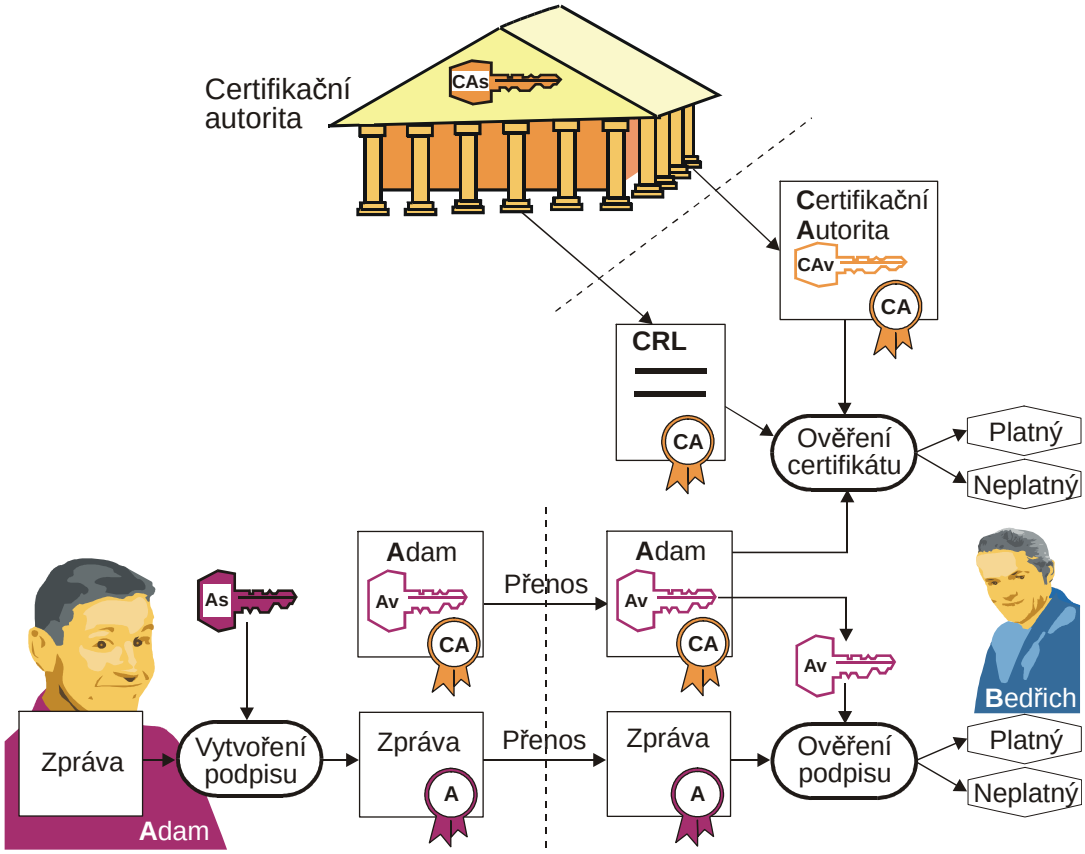
Certifikační autorita rovněž může vydaný certifikát zveřejnit sama, např. v seznamu certifikátů, v prohledávatelné databázi apod. To je užitečné, pokud se PKI používá pro šifrování zpráv pro adresáta, neboť adresátův certifikát a jeho veřejný klíč v něm, který použijete pro zaslání zašifrované zprávy pro adresáta, můžete získat od CA bez předchozí nešifrované komunikace s adresátem.

V případě elektronického podpisu je však zveřejňování zpravidla zbytečné, neboť podpisující může certifikát přiložit zároveň s podepsanou zprávou. Nezveřejněním certifikátu se pak chrání údaje v certifikátu uvedené, jako je např. e-mailová adresa, identifikátor aj. osobní údaje (atributy, znaky), které si podepisující nechal do certifikátu vložit.

Pozn.: certifikační autorita je v právních předpisech uváděna jako „poskytovatel certifikačních služeb“, v lokalizaci Windows pak jako „certifikační úřad“.

2.3.2 Vytvoření podpisu zprávy, přenos a ověření podpisu s PKI

Na dalším obrázku je znázorněno použití získaného certifikátu. Tak jako na obrázku 2-5 i na obr. 2-7 Adam vytvoří podpis ke zprávě. Zatímco na obr. 2-5 musel Bedřich věřit nebo nějak relativně složitě zajistit, že veřejný klíč, jímž podpis zprávy ověřuje, patří skutečně Adamovi, na obr. 2-7 Adam k podepsané zprávě prostě přiloží certifikát, vydaný předtím certifikační autoritou.



Obr. 2-7 Vytvoření a ověření elektronicky podepsané zprávy s připojeným certifikátem

Integrita veřejného klíče a identita jeho vlastníka je nyní zajištěna „elektronickým podpisem“ certifikátu veřejného klíče Adama (přenášená zpráva s pečetí „CA“). Bedřich se nyní proto může spolehnout na to, že veřejný klíč *Av* náleží Adamovi, že mu nebyl podsunut, a přímo jej použít pro ověření podpisu zprávy. Zbývá pouze ověřit platnost samotného certifikátu (tj. podpisu certifikátu), která se ověřuje vůči veřejnému klíči *CAv*. Ten je obsažen většinou v tzv. „samopodepsaném“ (self-signed) certifikátu, v němž certifikační autorita svým soukromým klíčem podepíše své identifikační údaje a svůj veřejný klíč (tento certifikát viz v pravém horním rohu obrázku 2-7). Alternativně může být certifikát potvrzen certifikátem certifikační autority o úroveň výše. Ověření certifikátu veřejného klíče CA provádí Bedřich pouze jedenkrát, když poprvé (a naposledy) provádí tzv. import certifikátu CA. Tomuto ověření by měl Bedřich věnovat o to větší pozornost, neboť na spolehlivosti tohoto ověření budou záviset všechna následná ověřování podpisů certifikátů od této certifikační autority.

Kromě ověření podpisu CA se ještě musí ověřit, zda certifikát veřejného klíče Adama nebyl zneplatněn, což se zpravidla činí přes seznam zneplatněných certifikátů, tzv. CRL (Certificate Revocation List), který vydává buď shodná CA, která vydala certifikát veřejného klíče, nebo jiný, CA pověřený subjekt. Pokud klíč v CRL není uveden a čas ověřování spadá do doby platnosti certifikátu veřejného klíče, pak je podpis zprávy platný.

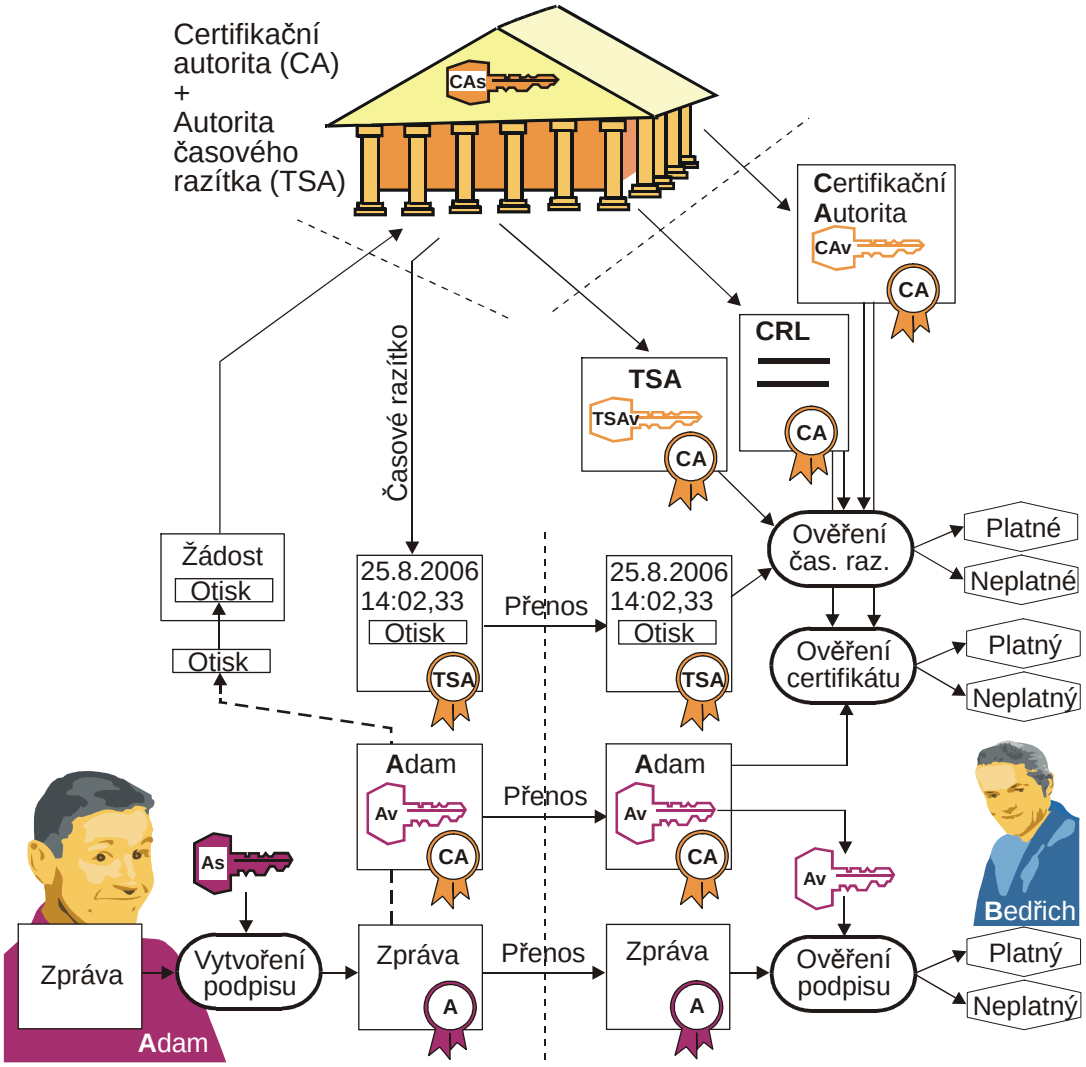
Pozn.: doba latence mezi podáním žádosti o zneplatnění vlastníkem certifikátu a časem zveřejnění v CRL může být právně-technicky definována různě a výše uvedené úvahy o platnosti podpisu zprávy s ohledem na čas ověření podpisu zprávy a kontroly výskytu certifikátu v CRL může komplikovat.

Na první pohled se zlepšení nezdá podstatné. Bedřich stále musí ověřit veřejný klíč a jeho podpis v jedné zprávě, k níž již žádný certifikát nenáleží. Včlenění CA přináší ale tato podstatné zlepšení:

- správně zavedená CA brání útoku muže uprostřed, podsouvání dat,
- úspora ověřování veřejného klíče se výrazně uplatní, pokud Bedřich komunikuje s více osobami, které mají vydán certifikát od shodné certifikační autority,
- ručně dostačuje ověřit „kořenový“ certifikát, ostatní podpisy v kaskádě se ověřují automaticky (nutné ale ověřit i právní účinky kaskády),
- CA poskytuje zpravidla poskytuje určité záruky za identitu osoby v certifikátě uvedené, tj. vnáší jistou míru důvěry do komunikace osob nebo subjektů, které se osobně předem vůbec nemusejí znát,
- CA vnáší do práce s klíči mechanismus tzv. zneplatnění (též revokace, odvolání), který chrání podpisujícího i spoléhajícího v případě nenadálých událostí se soukromým klíčem podpisujícího, změn údajů v certifikátu potvrzených apod.; v CRL se publikují certifikáty, které byly zneplatněny, čas jejich zneplatnění, popř. i kód důvodu.

2.3.3 Vytvoření podpisu s časovým razítkem

Ačkoliv se postup na obr. 2-7 zdá téměř dokonalý, Bedřichovi stále jedno riziko zbývá. Mohlo by se přihodit, že Bedřich postupem na obr. 2-7 zprávu i certifikát podpisujícího ověří, včetně kontroly CRL, podpis bude platný, avšak Adam svůj certifikát zneplatní o den nebo dva později. Stejný efekt bude mít, pokud samovolně vyprší platnost certifikátu Adama. Bedřich bude mít potíž prokázat, že ověření podpisu provedl ještě v čase platnosti certifikátu.



Obr. 2-8 Vytvoření a ověření elektronicky podepsané zprávy s připojeným časovým razítkem

K tomuto účelu byl do PKI zaveden nástroj tzv. časových razítek. Časová razítka mohou být použita více způsoby, ten základní však zobrazuje obr. 2-8.

Podpisující Adam ke zprávě připojí nejen svůj certifikát, ale navíc z podepsané zprávy, případně včetně certifikátu, nechá vytvořit časové razítko. Časové razítko poskytuje opět certifikační autorita, nyní spíše nazývána jako autorita časového razítka TSA (Time-Stamp Authority), popř. též obecně jako poskytovatel důvěry TSP (Trust Service Provider). TSA vytvoří časové razítko na základě žádosti. V žádosti se nevyskytuje originál časově razítkovaných dat, ale jen jejich otisk, vytvořený tzv. haš-funkcí. To umožňuje používat tuto službu naprosto důvěryhodně bez svěřování se s vlastními daty vůči TSP. Ve vystaveném časovém razítku je otisk zkopírován, je uveden čas vystavení razítka a razítko je podepsáno za pomoci soukromého klíče TSA. Časové razítko dosvědčuje, že razítkovaná data existovala **před** časem uvedeným v časovém razítku.

Razítkuje-li se elektronicky podepsaná zpráva (pochopitelně aspoň včetně samotného podpisu), časové razítko dokazuje, že elektronický podpis vznikl před datem a časem v razítku uvedeném. Takové časové razítko pak může být též připojeno k podepsané zprávě a zasláno adresátovi. Na pozdější zneplatnění nebo vypršení certifikátu podpisujícího již nemusí být brán zřetel, neboť je dokázáno, kdy nejpozději podpis vznikl.

Adresát Bedřich při ověření zkontroluje nejen podpis zprávy a platnost certifikátu, ale i platnost časového razítka. Pokud jsou všechny kontroly platné, pak má k dispozici elektronický podpis, jehož platnost bude zachována i v případě ukončení platnosti certifikátu veřejného klíče.

Uvedený postup na obrázku předpokládá, že razítko ke zprávě vytváří již podpisující. V praxi někdy dostačuje, aby si časové razítko podepsané zprávy nechal vytvořit až po příjmu zprávy ověřující.

Časová razítka jsou též používána pro složitější formáty tzv. archivních podpisů, kdy má elektronický podpis mít dlouhodobou platnost v řádu let až desítek let.

Konečně, časové razítko může být použito i pro jiné účely dokazování času, např. v různých registračních systémech pracujících na principu fronty, pro dokazování prvenství ohledně duševních práv apod.

Naopak, v některých situacích lze dokazování platnosti podpisu v určitém čase rekonstruovat i jinými metodami než je časové razítko, např. spočívajícími na sekvencích žurnálu apod., nicméně časové razítko je nejobecnější a nejsilnější nástroj průkaznosti časové hranice provedení podpisu nebo jeho ověření.

