Y36BEZ – Bezpečnost přenosu a zpracování dat

Róbert Lórencz

9. přednáška

DSA, PKI a infrastruktura

http://service.felk.cvut.cz/courses/Y36BEZ
lorencz@fel.cvut.cz

Obsah přednášky

- Distribuce veřejných klíčů
- Digitální podpis, DSA
- Formáty certifikátů podle X.509
- Certifikační strom
- Distribuce tajných klíčů
- Digitální podpis
- DSA

Distribuce veřejných klíčů (1)

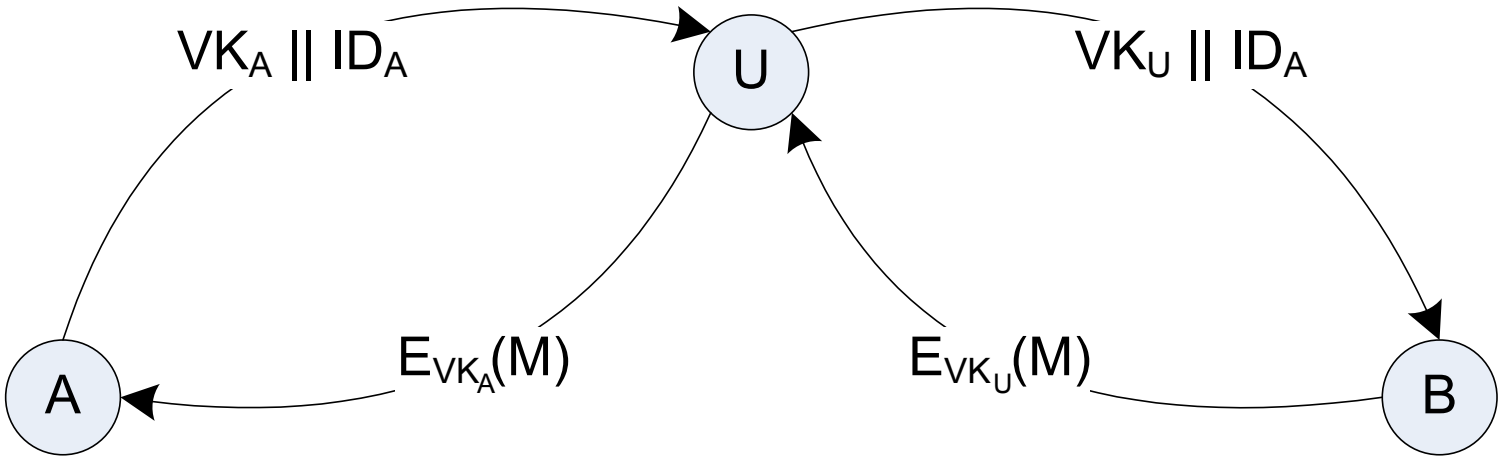
Úvod - distribuce tajných klíčů pomocí kryptografie VK

1. Distribuce veřejných klíčů.
2. Použití šifrování s VK pro distribuci tajných klíčů

Distribuce veřejných klíčů

- S distribucí VK souvisí hrozba podvržení veřejného klíče $\Rightarrow$
- ohrožení bezpečnosti kryptografických systémů s VK.

Podvržení veřejného klíče



Distribuce veřejných klíčů (2)

Způsob podvržení veřejného klíče

- Subjekt A pošle svůj VK_A a svůj identifikátor ID_A, tj zprávu $VK_A||ID_A$ subjektu B.
- Předpoklad: útočník U má aktivní přístup k veřejnému kanálu.
- U zachytí zprávu $VK_A||ID_A$ a vytvoří novou zprávu $VK_U||ID_A$ a odešle ji B - podvržení VK_U subjektu B.
- B se domnívá, že $VK_A = VK_U \Rightarrow$ B zašifruje každou zprávu M klíčem VK_U, tj vytvoří $E_{VK_U}(M)$ a odešle ji A.
- U zachytí $E_{VK_U}(M)$ a dešifruje ji SK_U a získavá zprávu M.
- U zná $VK_A \Rightarrow$ zašifruje $M \rightarrow E_{VK_A}(M)$ a pošle ji A.
- Důsledek: U čte korespondenci zaslanou sujektem A subjektu B!
- Tato činnost nemusí být vůbec subjektem B detekována.

Distribuce veřejných klíčů (3)

Distribuce veřejných klíčů lze realizovat technikou:

1. zveřejnění veřejných klíčů (public announcement)
2. veřejně dostupný adresář (public available directory)
3. autorita pro veřejné klíče (public-key authority)
4. certifikace veřejných klíčů (public-key certification)

Zveřejnění veřejných klíčů

- Zasíláním VK individuálně nebo hromadně v rámci nějaké komunity.
- Na internetu – připojením k emailu, vystavením na webu apod.
- Rychlý a jednoduchý způsob.
- Nízká bezpečnost! Není odolný proti podvržení VK –
- nepovolaný subjekt může číst zprávy dotčeného subjektu až do odhalení.

Distribuce veřejných klíčů (4)

Veřejně dostupný adresář

- Vyšší stupeň bezpečnosti.
- Distribuci VK zabezpečuje důvěryhodná autorita - zodpovídá za obsah, je správcem adresáře.
- Účastníci registrují svůj VK prostřednictvím autorizovaného správce adresáře.
- Bezpečná registrace: osobně nebo přes bezpečnou komunikaci.
- Položky v adresáři jsou tvořeny: [jmeno;*VK*].
- Účastníci mění VK podle potřeby - bezpečnost, velký objem dat jedním *VK*, zkompromitovaný VK atd.
- Správce periodicky aktualizuje adresář – elektronicky nebo fyzicky.
- Tento systém je bezpečnější než předchozí, má ale slabá místa:
- Pokud nepovolaný subjekt získá *SK* správce adresáře $\Rightarrow$
- může modifikovat adresář a provádět odposlech jako v předchozí metodě.

Distribuce veřejných klíčů (5)

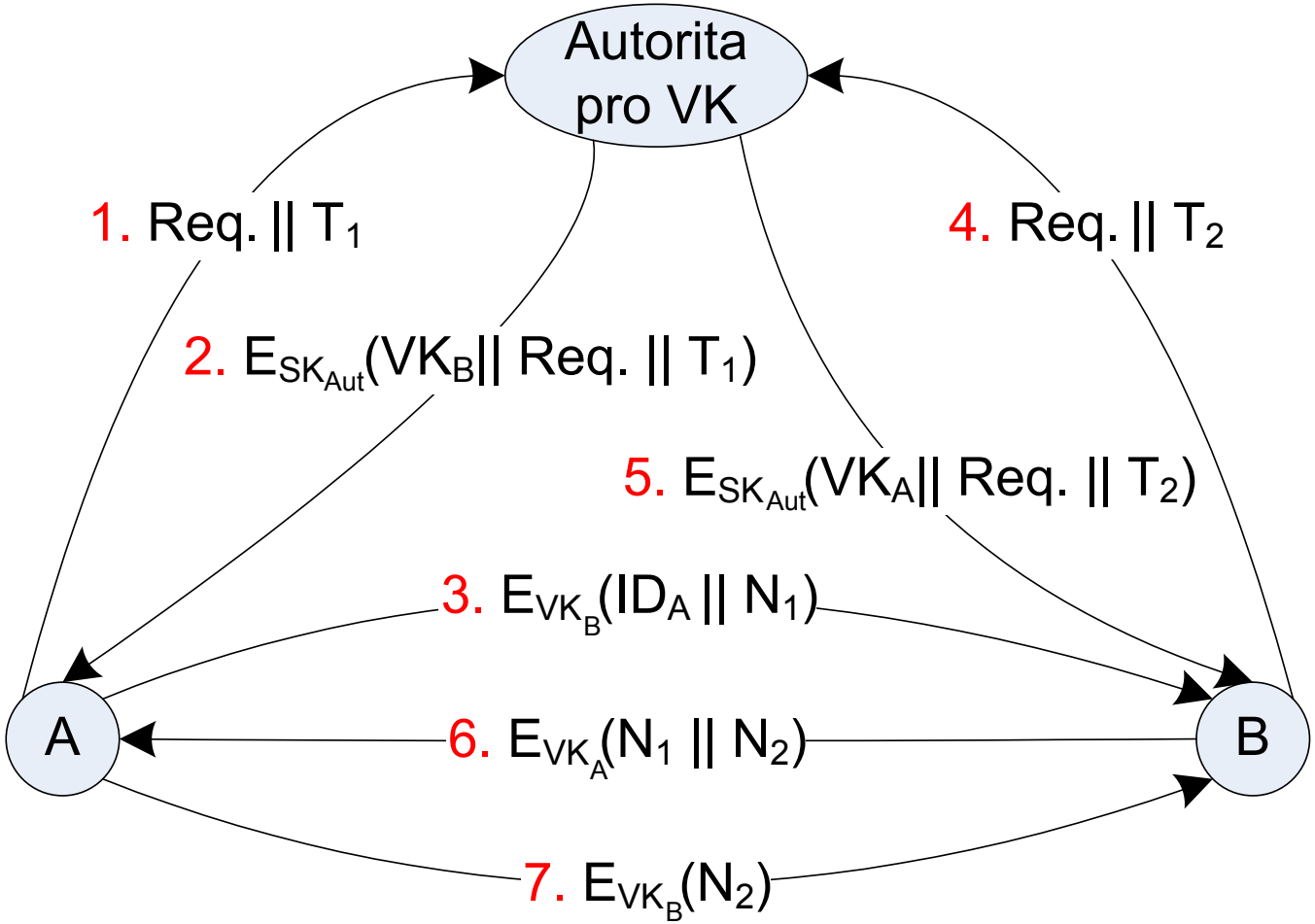
Princip veřejně dostupného adresáře

Autorita pro veřejné klíče

- Přísnější dohled na distribuci VK z adresáře znamená vyšší stupeň bezpečnosti.
- Autorita vykonává činnost správce adresáře VK.
- Každý účastník zná veřejný klíč autority VK_{Aut}, která vlastní odpovídající soukromý klíč SK_{Aut}.

Distribuce veřejných klíčů (6)

Distribuce veřejných klíčů pomocí autority pro veřejné klíče



Distribuce veřejných klíčů (7)

A chce inicializovat výměnu zprávy s B - scénař distribuce VK:

1. A ve zprávě Autoritě požaduje (*Req*.- Request) VK_B za účelem komunikace s B. Žádost je doplněná časovou značkou T_1 (Time).
2. Autorita odpoví zprávou zašifrovanou SK_{Aut}. A dešifruje zprávu VK_{Aut} - potvrzení, že zpráva je od Autority. Zpráva obsahuje:
   - VK_B - A může šifrovat zprávy pro B
   - kopii žádosti *Req*. od A – A může verifikovat kopii s vyslanpou žádostí, tj. zda žádost nebyla modifikována před přijetím Autoritou
   - kopii T_1 - umožňuje A verifikovat aktualitu žádosti.
3. A použije VK_B pro zašifrování zprávy pro B obsahující identifikátor A ID_A a náhodné číslo N_1 (potvrzuje jedinečnost výměny).
4. B po obdržení zprávy od A vyžádá od Autority VK_A (jako A v 1.).
5. B obdrží VK_A od Autority stejným způsobem jako A v bodě 2.
6. B zašle A zprávu $N_1||N_2$ zašifrovanou VK_A, N_2 generuje B.
7. A zašle B zprávu N_2 zašifrovanou VK_B.

Distribuce veřejných klíčů (8)

Zvýšení bezpečnosti předaných zpráv

- Postup v bode 6. a 7 zvyšuje bezpečnost výměny zpráv.
- B zasláním zprávy $N_1||N_2$ subjektu A, kde N_2 je náhodné číslo generované B, dá jistotu A, že autorem zprávy je B, protože obsahuje N_1 vygenerované A. Dešifrování na obou stranách je možné jen se znalostí přislušných SK A a B.
- V kroku 7. získá B jistotu, že zpráva pochází od A, protože obsahuje N_2.

- Distribuce VK pomocí Autority pro VK má své nevýhody. Autorita představuje "úzké hrdlo" této koncepce.
- Každý účastnik na získání VK adresáta musí nejdříve komunikovat s Autoritou pro VK.
- Alternativní přístup v distribuci VK představuje použití certifikátů.

Distribuce veřejných klíčů (9)

Certifikace veřejných klíčů

- Distribuce VK bez kontaktu s třetím důvěryhodným subjektem.
- Tento přístup vyžaduje definici certifikátu a certifikační autority.

Definice certifikátu

Certifikát je utajovaná struktura, ktera obsahuje:

- veřejný klíč žadatele/držitele certifikátu
- identifikační údaje držitele certifikátu
- dobu platnosti certifikátu
- další údaje vytvořené certifikační autoritou.

Tato struktura je podepsána soukromým klíčem certifikační autority SK_{Aut} a každý účasnik může verifikovat obsah certifikátu pomocí veřejného klíče certifikační autority VK_{Aut}.

Distribuce veřejných klíčů (10)

Definice certifikační autority

Certifikační autorita (CA) je důvěryhodná třetí strana, která na základě žádosti vydává a aktualizuje certifikáty. Každý účastník může verifikovat to, že certifikát byl vytvořen CA, pomocí jejího veřejného klíče VK_{Aut}.

- Žádost o vydání certifikátu lze CA doručit osobně nebo elektronicky s využitím bezpečné komunikace.
- Příjímaní žádostí, kontrola údajů v žádosti a odevzdávání certifikátů žadatelům se realizuje registrační autoritou

Princip výměny veřejných klíčů na bázi certifikátů

- Subjekt A před započetím jakékoliv komunikace požádá CA o vydání certifikátu na svůj veřejný klíč VK_A.

Distribuce veřejných klíčů (11)

- CA vydá certifikát C_A pro subjekt A, který obsahuje:
  - dobu platnosti - T_1
  - identifikační údaje A - ID_A
  - veřejný klíč - A - VK_A
- Tuto strukturu certifikátu podepíše svým soukromým klíčem SK_{Aut} a odešle A.
- Certifikát pro A má potom tvar:

$$C_A = E_{SK}(T_1, ID_A, VK_A)$$

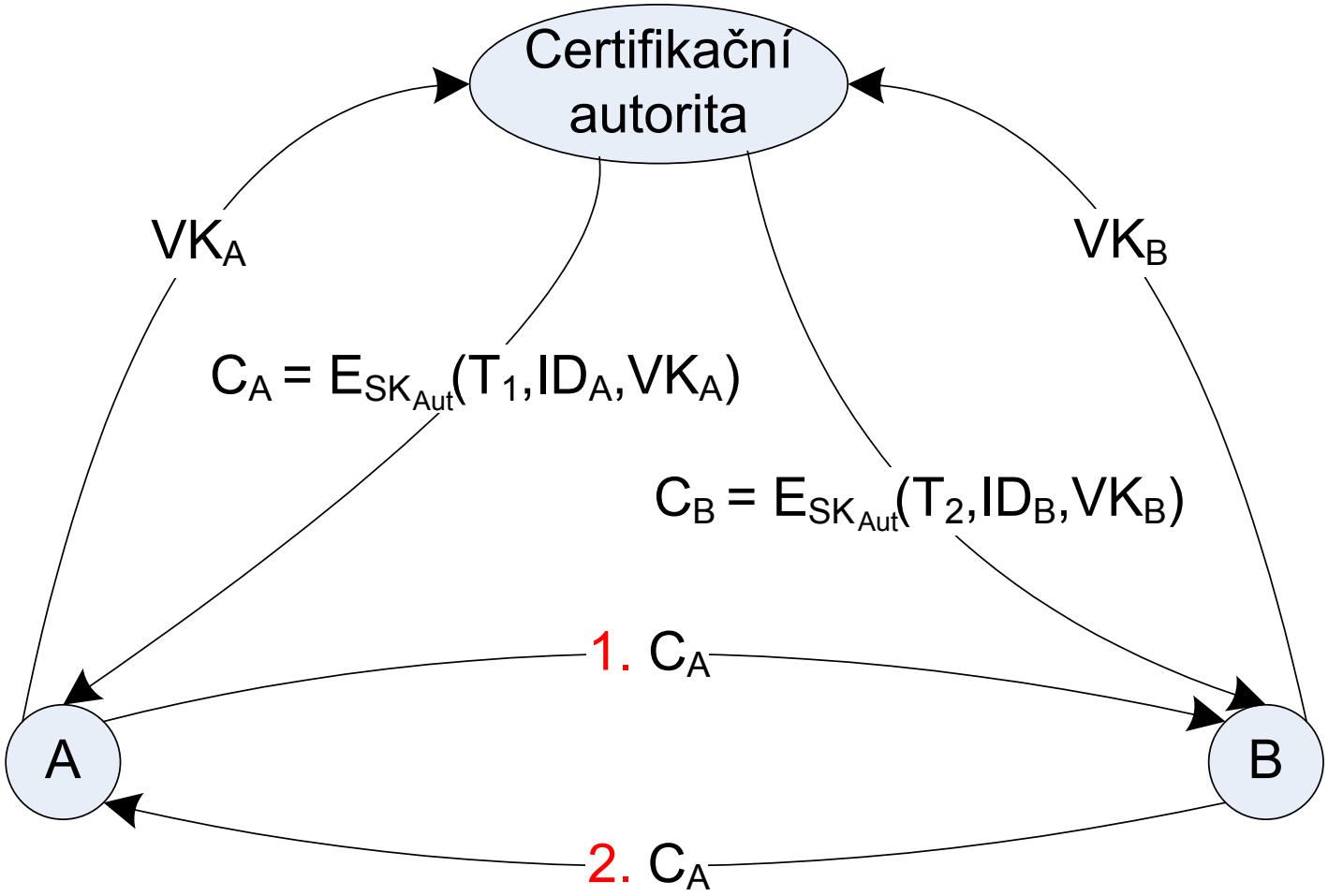
- Certifikát v této podobě lze poskytnout subjektu A, který ho může zveřejnit, protože ho lze číst/verifikovat pomocí veřejného klíče CA - VK_{Aut}:

$$D_{VK_{Aut}}(C_A) = D_{VK_{Aut}}(E_{SK_{Aut}}(T_1, ID_A, VK_A)) = (T_1, ID_A, VK_A)$$

- Tento proces dešifrování klíčem CA je současně ověřením toho, že certifikát byl vytvořen CA.

Distribuce veřejných klíčů (12)

Distribuce veřejných klíčů pomocí certifikátů



Distribuce veřejných klíčů (13)

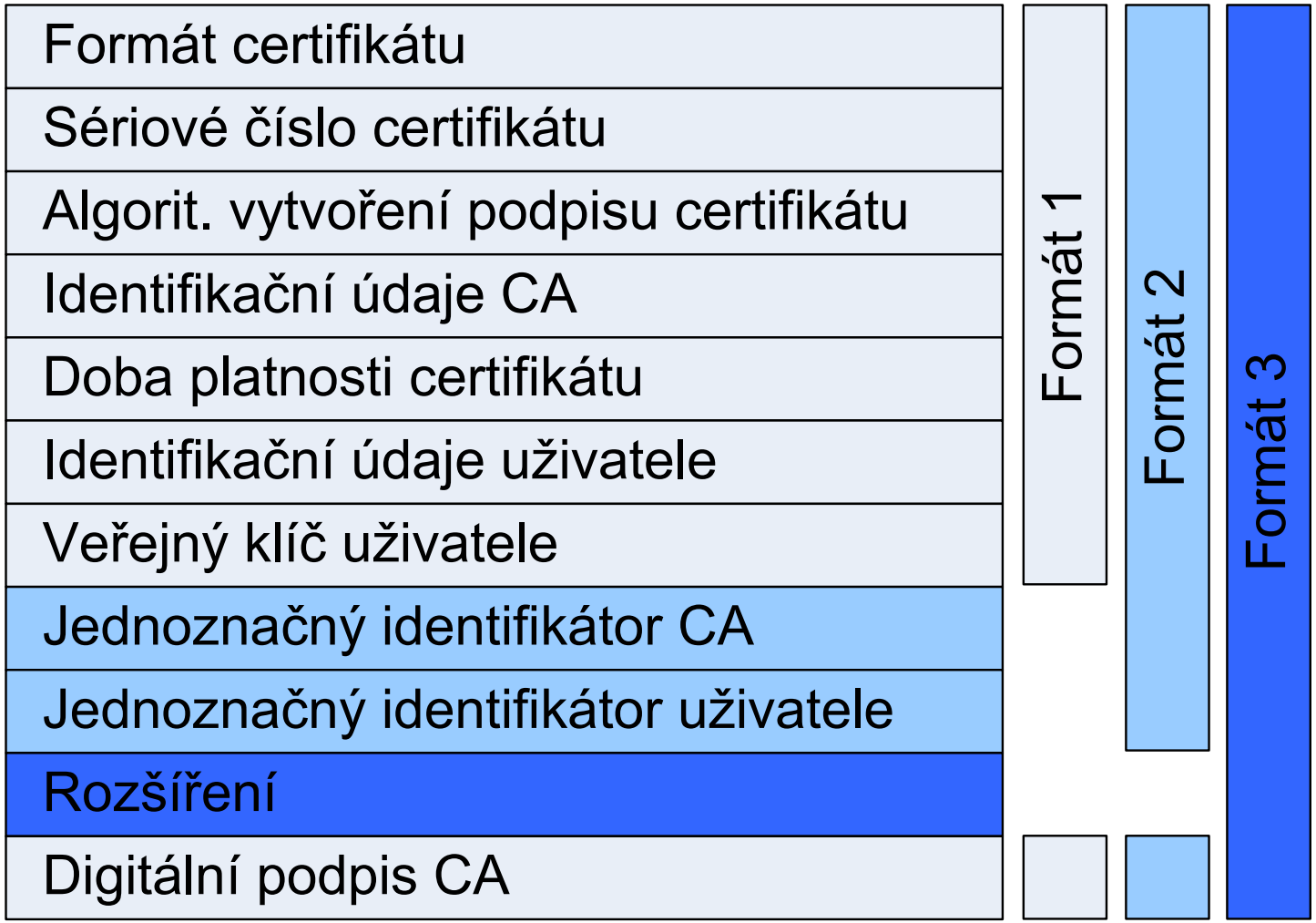
- Dešifrováním se získají jméno a veřejný klíč držitele certifikátu a také časový údaj o platnosti.
- Analogicky požádá o vydání certifikátu subjekt B.
- Certifikát C_B má analogickou strukturu jako C_A.
- Distribuce veřejných klíčů potom představuje výměnu certifikátů C_A a C_B mezi subjekty A a B (kroky 1. a 2. na obrázku).

Certifikáty podle doporučení X.509

- Formáty certifikátů určuje doporučení ITU-T X.509, které je částí doporučení X.500.
- Doporučení X.509 definuje také autentizační protokoly používané v různých typech sítí a aplikacích síťové bezpečnosti.
- Všeobecný formát podle X.509 je následující:

Formáty certifikátů podle X.509 (1)

X.509 - formáty certifikátů



Certifikační strom (1)

Vlastnosti certifikátů vydávaných CA:

- Kterýkoliv subjekt prostřednictvím veřejného klíče CA může verifikovat veřejné klíče jiných subjektů.
- Žádný jiný subjekt než CA nemůže modifikovat vydané certifikáty
- Certifikáty jsou nefalšovatelné $\Rightarrow$ jsou umístněny v adresáři CA přístupném všem subjektům bez nutnosti zvláštni ochrany.

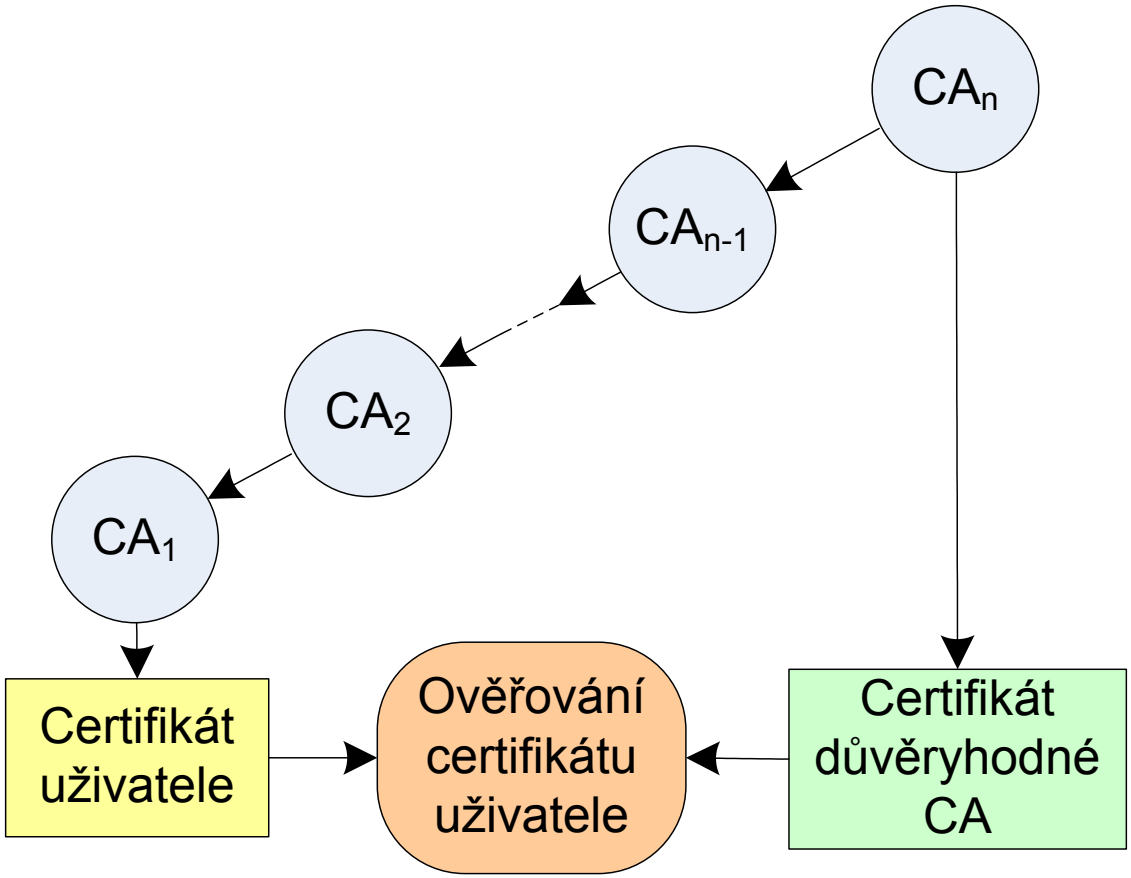
- Uvedená koncepce má nevýhodu při velkém počtů uživatelů.
- Každý uživatel musí mít kopii veřejného klíče CA.
- Výhodnější je vytvořit více CA pro různé okruhy uživatelů.

- Vytvoření více CA předpokládá vzájemné propojení mezi CA například ve formě stromové struktury – certifikačního stromu.
- Každý strom reprezentuje kořenová CA, která vlastní kořenový certifikát.

Certifikační strom (2)

- Posloupnost certifikátů od certifikátu uživatele až k certifikátu kořenové CA se nazývá řetězec certifikátů

Řetězec certifikátů

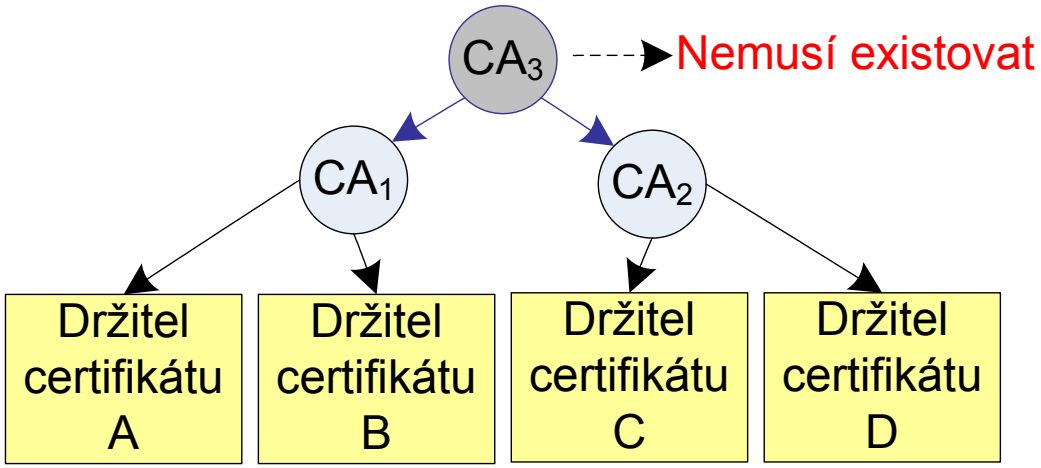


Certifikační strom (3)

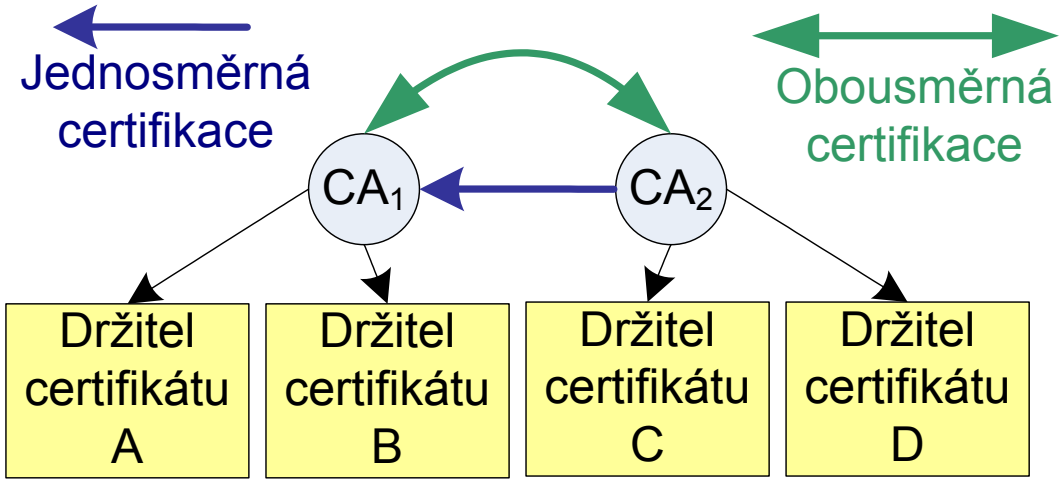
- Certifikát je platný $\Leftrightarrow$ platné všechny certifikáty v řetězci certifikátů.
- Kořenový certifikát musí být shodný s kořenovým certifikátem jiné důvěryhodné CA ověřený jinou bezpečnou cestou.
- Je možné prohlásit za důvěryhodný i certifikát v řetězci certifikátů $\Rightarrow$ se ověřovaní urychlí.
- Řetěz certifikátů předpokládá stromovou strukturu CA.
- Uživatelé mající certifikát jedné stromové struktury mohou získat v rámci této struktury certifikáty ostatních uživatelů.
- Prolém vzniká se získáním certifikátů uživatelů jiné stromové struktury.
- V tomto případě získaní certifikátů mezi uživateli dvou různych CA umožňuje křížová certifikace:
  - jednosměrná
  - obousměrná

Certifikační strom (4)

Stromová struktura certifikačních autorit



Křížová certifikace



Certifikační strom (5)

V případě, že C (obrazek Křížová certifikace) chce komunikovat s A, musí A poslat C množinu certifikátů:

- certifikát A, podepsaný CA_1
- certifikát CA_1 podepsaný CA_1, tj. kořenový certifikát CA_1
- certifikát CA_1 podepsaný CA_2, tj. křížový certifikát

Certifikát CA_2 podepsaný CA_2, tj. kořenový certifikát CA_2 subjekt C zná, protože patří do stromové struktury CA_2.

Touto křížovou certifikaci se CA_1 a její uživatelé stanou důvěryhodnými pro CA_2 a její uživatele, neplatí to naopak!

Aby tento vztah byl obousměrný, je nutné, aby i CA_2 si vyžádala křížový certifikát podepsaný CA_1.

Obousměrná křížová certifikace znamená, že CA_1 a CA_2 vlastní kromě kořenových certifikatů také křížové.

Certifikační strom (6)

Platnost certifikátu

- Každý certifikát má vymezenou dobu platnosti. Nový certifikát je vydaný těsně před uplynutím této doby platnosti.
- Na žádost držitele certifikátu může certifikát ztratit platnost – žádostí odvolání certifikátu podanou na CA. Motivace:
  - kompromitace soukromého klíče
  - uživatel chce změnit aktuální CA
  - kompromitace certifikátu vydaného CA
- CA zveřejňuje seznam odvolaných certifikátů.

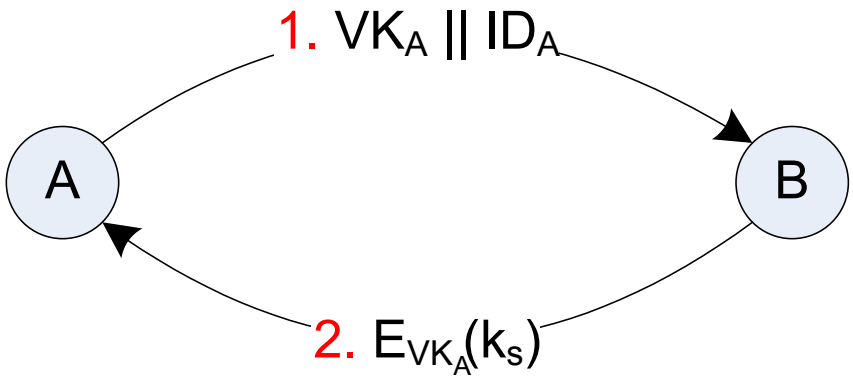
PKI (Public Key Infrastructure)

- Norma v sítí Internet vycházející z norem ITU-T X.500
- Specifikace technických a organizačních opatření pro vydávaní, správu, používaní a odvolávaní klíčů a certifikátů.
- Hlavní cíl – zabezpečení kompatibility SW pro Internet.

Distribuce tajných klíčů (1)

- Distribuce tajných klíčů existuje taktéž v kryptografických systémech s VK.
- Kryptografické systémy VK poskytují lepší možnosti pro tuto distribuci než klasická (symetrická) kryptografie.

Jednoduchá distribuce tajných klíčů

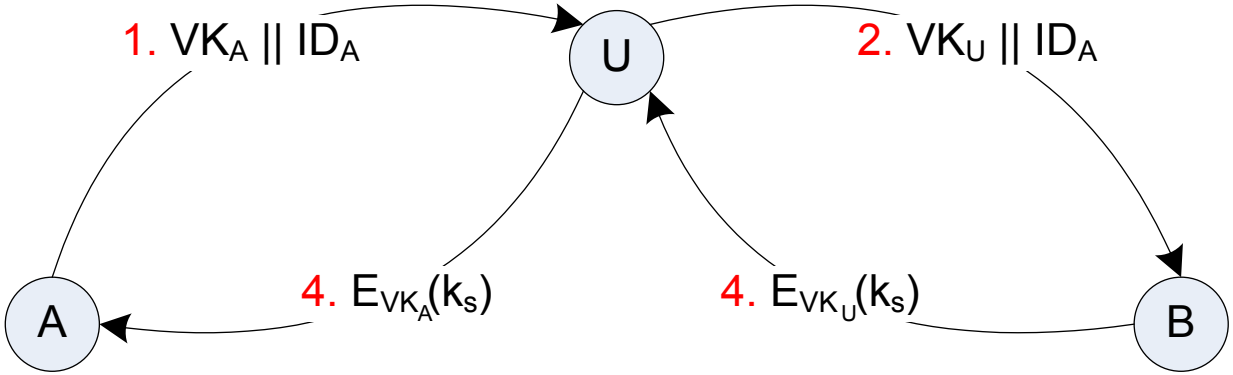


- Pokud A chce komunikovat s B, musí oba realizovat uvedené kroky.
- po vyslání subjektem A zprávu B obsahující VK_A a identifikátor ID_A obdrží A od B tajný klíč k_s zašifrovaný VK_A.

Distribuce tajných klíčů (2)

- Podvržením veřejného klíče aktivním útočníkem U lze získat tajný klíč k_s.
- Podvržení je provedeno stejným způsobem jako u podvržení veřejného klíče.

Získaní tajného klíče
podvržením veřejného klíče

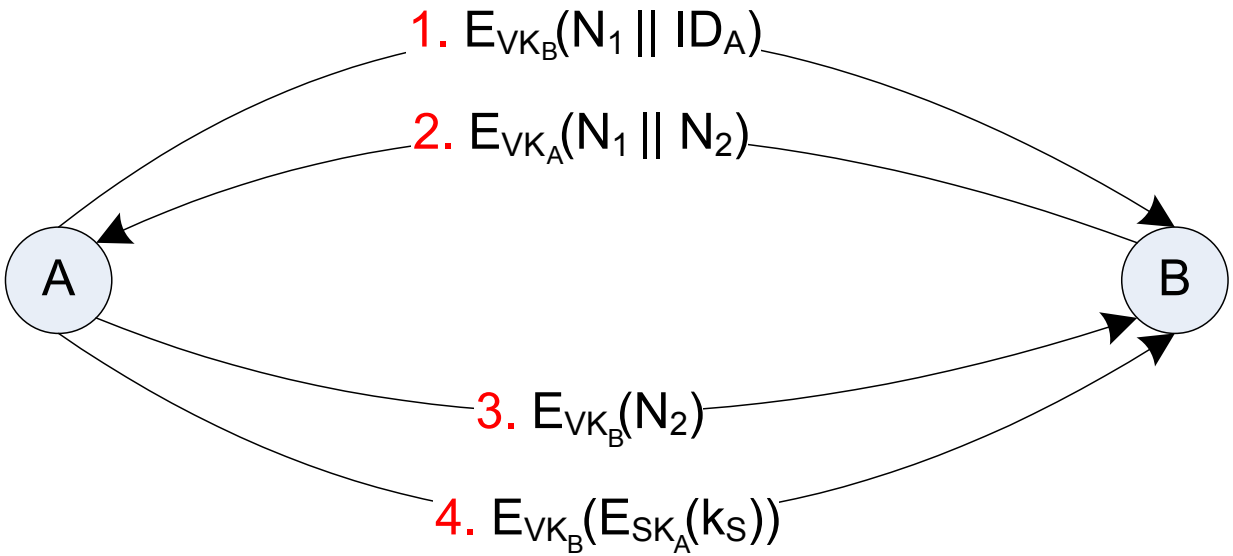


- Výsledek: tajný klíč k_s určený pro tajnou komunikaci mezi A a B zná také U, který může dešifrovat tajnou komunikaci mezi A a B.
- Jednoduchou koncepci distribuce tajných klíčů lze použít jen v prostředí s možností pasivních útoků.

Distribuce tajných klíčů (3)

- Distribuce tajných klíčů v prostředí s aktivními a pasivními útoky lze provést na bázi VK jen za předpokladu:
- A a B si bezpečným způsobem vyměnili svoje veřejné klíče.

Výměna tajných klíčů s utajením a autentizaci



- Tato koncepce zaručuje důvěrnost a autentizaci při výměně tajného klíče.

Digitální podpis (1)

Digitální podpis je obvykle formou asymetrického kryptografické schématu

- Soukromý klíč – podepsání
- Veřejný klíč – ověření

Vlastnosti digitálního podpisu

- Nezfalšovatelnost, autentizace – podpis se nedá napodobit jiným subjektem než podepisujícím
  - Ověřitelnost – příjemce dokumentu musí být schopen ověřit, že podpis je platný
- Integrita – podepsaná zpráva se nedá změnit, aniž by se zneplatnil podpis
- Nepopiratelnost – podepisující nesmí mít později možnost popřít, že dokument podepsal

Digitální podpis (2)

Další vlastnosti

- Skupina bitů, jejichž hodnoty závisí na celém podepisovaném dokumentu
- Využívá informaci, kterou zná jen podepisující (soukromý klíč)
- Implementace digitálního podpisu by měla být snadná, ale...
- falšování digitálního podpisu by mělo být výpočetně obtížné
  - neschůdné vyrobit falešný podpis pro existující zprávu
  - neschůdné vyrobit falešnou zprávu pro existující podpis

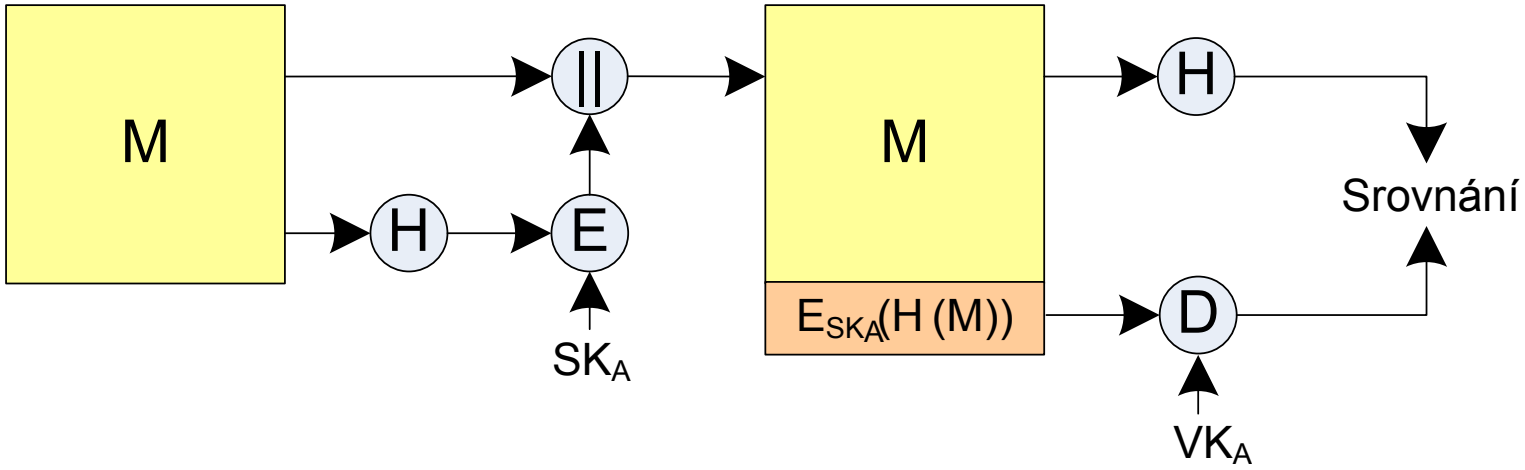
Kategorie digitálních podpisů

- Přímé digitální podpisy (direct digital signature)
  - Mezi dvěma subjekty, příjemce zná VK odesílatele
  - Problém s popiratelností
- Verifikované digitální podpisy (arbitrated digital signature)
  - Využívá důvětyhodnou třetí stranu (arbitra), který ověřuje podpisy všech zpráv

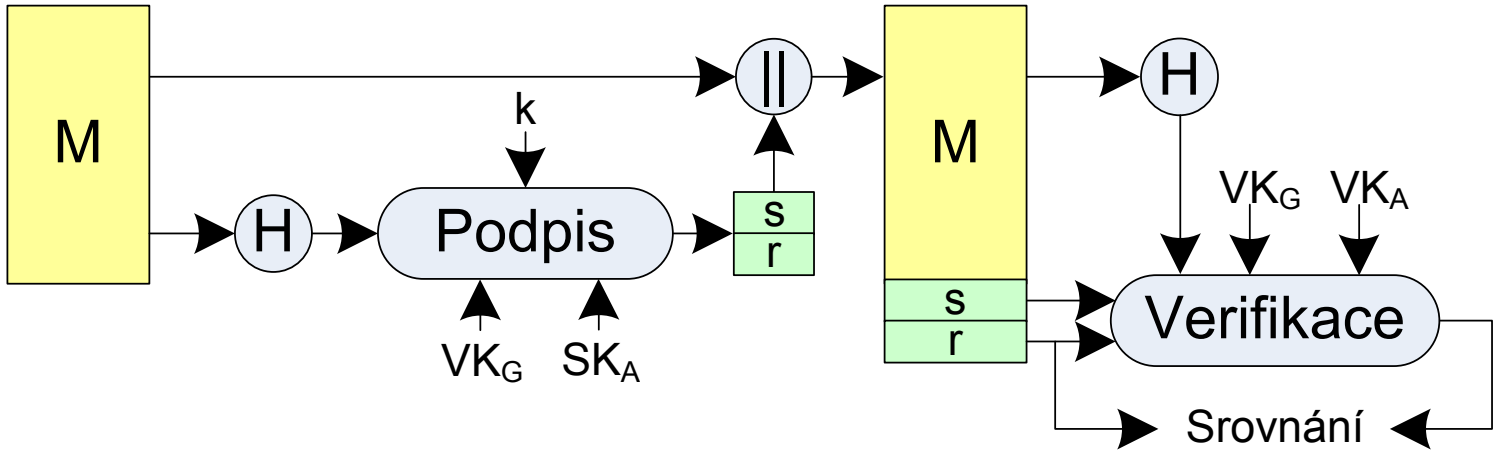
DSS (1)

Postupy v digitálních podpisech

RSA



DSS



DSA (1)

DSA - Inicializace schématu

- vygenerujeme náhodné prvočíslo q, $2^{159} < q < 2^{160}$
- vygenerujme náhodné prvočíslo p, $2^{1023} < p < 2^{1024}$, tak, aby $q|p-1$
- nalezneme generátor g podgrupy $G \subset Z_p^*$ řádu q, tj.

$$g = h^{\frac{(p-1)}{q}} \wedge 1 < h < (p-1) \wedge h^{\frac{(p-1)}{q}} \pmod{p} > 1.$$

- veřejné parametry schématu jsou (p, q, g)
- zvolíme privátní klíč x, $0 < x < q$
- nutno zajistit integritu čtveřice (p, q, g, x)
- nevhodné chránit jen x samostatně coby privátní klíč
- vypočteme veřejný klíč y, $y = g^x \bmod p$

DSA (2)

DSA - Podpis zprávy

- vstup: veřejné parametry (p, q, g), privátní klíč x, zpráva pro podpis m
- výpočet:
- vygenerujeme tajné náhodné číslo k, $0 < k < q$.
  - NONCE – Number used ONCE
  - k bývá označováno jako dočasný klíč zprávy
  - prozrazení k kompromituje privátní klíč
- vypočteme $r = (g^k \bmod p) \bmod q$
- vypočtěme $s = k^{-1}(h(m) + xr) \bmod q$, kde $kk^{-1} \equiv 1 \pmod{q}$
- kontrola, že $r \neq 0$ a $s \neq 0$, jinak se výpočet opakuje
- podpisem je dvojice (r, s)

DSA (3)

DSA - Ověření podpisu

- vstup: veřejné parametry (p, q, g), veřejný klíč y, zpráva m, ověřovaný podpis (r, s)
- výpočet:
- ověříme, že $0 < r < q$ a $0 < s < q$; jinak podpis odmítneme jako neplatný
- vypočteme $w = s^{-1} \bmod q$
- vypočteme $u_1 = wh(m) \bmod q$ a $u_2 = wr \bmod q$
- vypočteme $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$
- podpis je platný $\Leftrightarrow v = r$