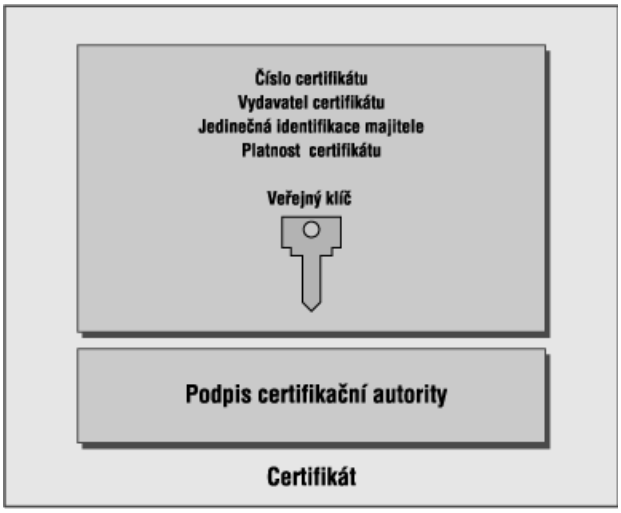
Certifikáty

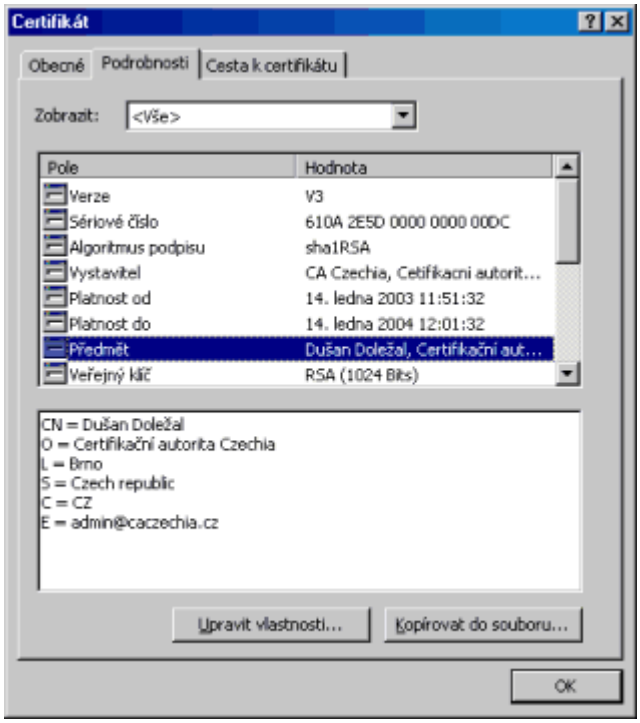
Problémem asymetrické kryptografie je způsob, jak ověřit pravost zveřejněných veřejných klíčů. K tomu slouží digitální či elektronický certifikát. Digitální certifikát je elektronická obdoba cestovního pasu nebo občanského průkazu. Jedná se v podstatě o uživatelův veřejný klíč plus další údaje popisující držitele certifikátu (jméno, bydliště, fotografie apod.) To vše je zašifrováno (elektronicky podepsáno) privátním klíčem, jehož veřejný klíč je znám a dostupný z nezaměnitelných zdrojů. Držitelem tohoto privátního klíče je tzv. certifikační autorita (v ČR např. PostSignum), tedy instituce nebo útvar, který tyto certifikáty neboli elektronické občanské průkazy vydává.
Každý může požádat certifikační autoritu o digitální certifikát.

Certifikační autorita a certifikáty

Řešením problému distribuce a uchování veřejných klíčů je tedy využití služeb certifikační autority (tzv. PKI - Public Key Infrastructure neboli Infrastruktura veřejného klíče). Instituce CA se podobají státním notářům, kteří při vzájemné komunikaci dvou subjektů vystupují jako třetí nezávislý důvěryhodný subjekt. Prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho veřejným klíčem a potažmo tedy i s jím vytvořeným digitálním podpisem. Certifikáty obsahují ve své nejjednodušší formě veřejný klíč, jméno a další údaje zajišťující nezaměnitelnost subjektů.



Běžně používané certifikáty též obsahují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu. To je zajištěno legislativními a technickými pravidly provozu instituce certifikační autority. Splnění těchto požadavků potvrdí certifikační autorita podepsáním dokumentu svým privátním klíčem a následným vydáním tohoto certifikátu.

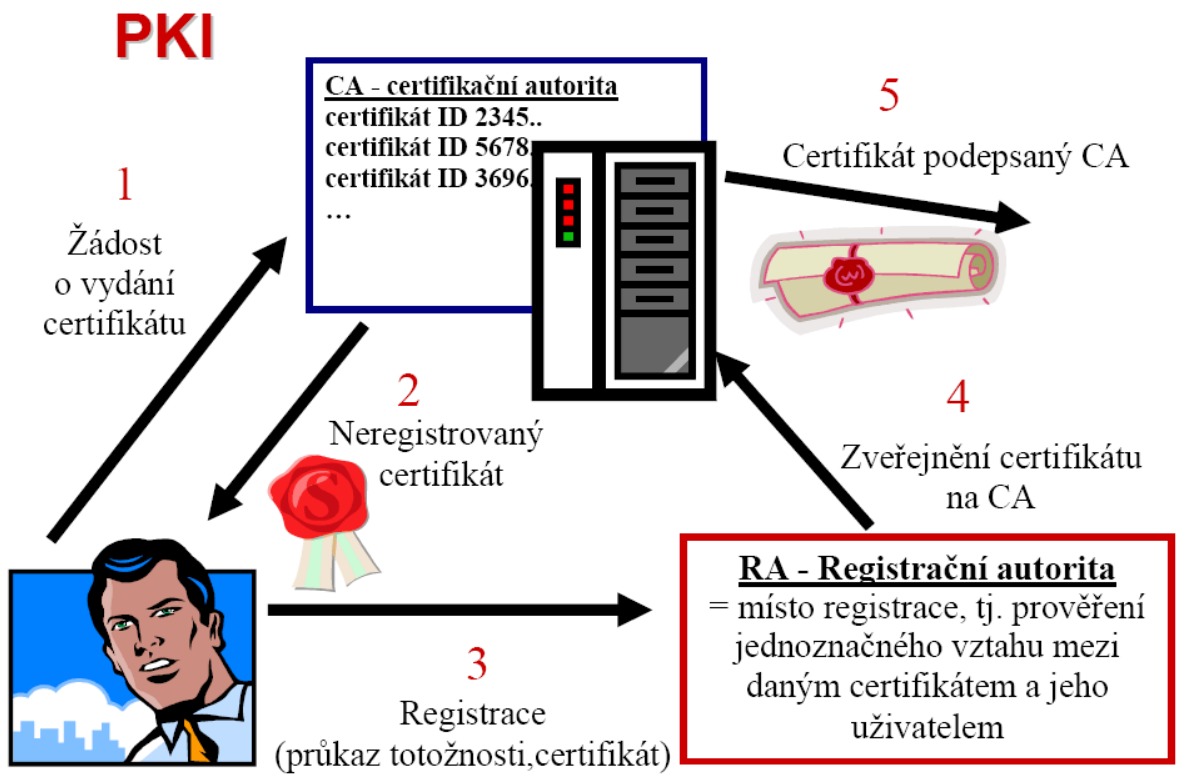


Znamená to, že certifikát je podepsaným dokumentem se všemi důsledky z toho plynoucími, tedy zejména autorizace (certifikační autorita jako garant pravosti dokumentu) a integrita dat (nelze zaměnit klíč nebo identitu klienta). Tím, že certifikační autorita zaručuje správnost jí vydaného certifikátu, odstraňuje nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty navzájem a jejich dohoda spočívá pouze v domluvě o společně uznávané certifikační autoritě. Důležité je, že se utajovaná data na straně klienta redukují pouze na bezpečné uchovávání privátního klíče, protože ostatní je řešeno certifikáty. Ty si můžeme kdykoliv ověřit se znalostí veřejného klíče certifikační autority, repektive jejího certifikátu. Existence certifikační autority také umožňuje důvěryhodnou komunikaci i subjektů, jenž se navzájem fyzicky nikdy nepotkali nebo neabsolvovali složitou proceduru vzájemné důvěryhodné výměny svých klíčů.

Tvorba a životnost certifikátů

Tvorba certifikátu má 6 kroků:

1. Generování klíčů. Každý potenciální žadatel o certifikát si nejprve sám pomocí dostupného SW vybavení vygeneruje dvojici klíčů pro použití v asymetrické kryptografii.
2. Příprava identifikačních dat. Žadatel o certifikát shromáždí podle požadavků certifikační autority osobní identifikační materiály nutné pro vydání certifikátu, jako IČ, DIČ, resp. číslo OP, rodné číslo a podobně.
3. Předání veřejných klíčů a identifikačních údajů certifikační autoritě. Žadatel předá certifikační autoritě data nutná pro vydání certifikátu spolu s doklady o jejich pravosti.
4. Ověření informací. Certifikační autorita si na příslušných místech ověří, že může vydat žadateli certifikát.
5. Tvorba certifikátu. Certifikační autorita vytvoří digitální dokument příslušného formátu a ten poté podepíše svým privátním klíčem.
6. Předání certifikátu. Podle dohody je certifikát žadateli předán na výměnném médiu, zaslán, nebo zveřejněn.



Doba platnosti certifikátů je omezená a je uvedena v každém certifikátu. Tato veličina je velmi důležitá. Pokrok ve zvyšování výkonnosti výpočetní techniky a možnost objevení mezer v protokolech nebo algoritmech by ve velkém časovém horizontu mohl způsobit, že by se certifikáty staly nespolehlivé. Běžné certifikáty jsou proto vydávány s platností 6 měsíců, nejvíce 1 rok. I během této doby je možné zrušit platnost certifikátu. Důvodem pro toto opatření může být například vyzrazení privátního klíče.

Klíče a certifikáty - kam s nimi?

Digitální podpis je ekvivalentem podpisu klasického a jeho výhodou je prakticky nulová možnost jeho napodobení. Riziko zneužití této technologie existuje především v nedodržovaní bezpečné manipulace s prostředky vedoucími k jeho vytvoření. Především je třeba zacházet velmi obezřetně s privátním klíčem, nejlépe jako s PINem platební karty či mobilního telefonu. Důležitým prvkem, který brání zneužití digitálního podpisu, je tedy uchovávání soukromého klíče na bezpečném místě.

Základní možností uložení klíčů je využít čistě softwarové řešení a svoje klíče skladovat přímo na pevném disku počítače v bezpečně zašifrovaném tvaru. Takto uložený klíč je odšifrován až bezprostředně před použitím na základě zadání správného hesla. Tato operace je z hlediska bezpečnosti kritická a klade velké nároky na zabezpečení vlastního počítače.

Lepším řešením je použít hardwarové zařízení umístěné mimo vlastní počítač. Typickým představitelem jsou čipové karty, jejichž mechanické provedení se může lišit. Ač se to na první pohled nezdá, čipové karty dnes najdeme takřka všude: telefonní karty, SIM-karty do mobilních telefonů, různé průkazkové karty sloužící k identifikaci jejich nositele, elektronická peněženka, atp.

Méně často už potkáme karty použité jako zabezpečovací. „Čistokrevné“ čipové karty bývají vybaveny buď kontaktní ploškou (s osmi kontakty) nebo mohou být bezkontaktní (s VF-přenosem dat).

Ať již je „balení“ jakékoliv, čipová karta se většinou skládá z těchto základních částí:

- paměť (ROM s firmwarem, RAM pro ukládání mezivýsledků, PROM pro nastavení některých nevratných parametrů karty, EEPROM pro další rozšiřující funkce karty)
- řadič nebo CryptoProcesor (včetně generátoru náhodných čísel)
- komunikační zařízení (kontakty nebo VF)

Karta s kryptografickým procesorem se hodí hlavně pro realizaci podpisu zde uloženým soukromým klíčem nebo k získání symetrického klíče použitého při hybridním šifrování rozsáhlého datového bloku. Důvodem je potřeba zajistit, aby soukromý klíč nemusel hardwarové zařízení nikdy opustit a dostat se do samotného počítače, kde by mohl být zneužit.
Přístup ke klíčům na čipové kartě bývá většinou chráněn PINem (PersonalIdentificationNumber). Toto není zbytečné obtěžování uživatele, ale rozumné opatření pro případ, že by se karta dostala mimo jeho přímou kontrolu.

Jiným typickým představitelem hardwarových zařízení jsou tzv. USB tokeny. Token iKey je identifikační předmět umožňující bezpečnou autentizaci uživatelů. Obecně bývá v IT využíván pro zabezpečení přístupu do počítačových sítí, VPN, intranetu nebo extranetu, pro uložení digitálních certifikátů, pro nasazení v aplikacích e-business, digitálního podpisu a PKI.

iKey podporuje (obdobně jako smart karty) zabezpečení pomocí PIN kódu, navíc ale nabízí pokročilé kryptografické funkce jako - hardwarovou podporu algoritmů MD5 a RSA, včetně možnosti vygenerování privátního klíče přímo v tokenu.

iKey na portu USB je jednoduchým, okamžitě použitelným bezpečnostním řešením na každém dnešním počítači bez nutnosti investice do speciálního čtecího zařízení.

Standardní formáty souborů certifikátů

Personal Information Exchange (PKCS #12)
Formát PFX (Personal Information Exchange) také nazývaný PKCS č. 12 podporuje bezpečné uložení certifikátů, privátních klíčů a všech certifikátů v certifikační cestě. Formát PKCS č. 12 je jediný formát souborů, který je možné použít k exportu certifikátu a příslušného privátního klíče. Soubory PKCS #7 typicky používají příponu .p12.

DER – binárně kódované X.509
Formát DER (Distinguished Encoding Rules) podporuje uložení jednoho certifikátu. Tento formát nepodporuje uložení privátního klíče nebo certifikační cesty. Soubory s certifikáty DER mají typicky příponu .der.

PEM - Base64 kódované X.509
Formát PEM je vlastně formát DER, který je pomocí tzv. base64 kódování převeden na obyčejný text. Formát PEM tak může být využit např. v textově orientované komunikaci, kde nelze přenášet binární data. Tento formát je díky výhradnímu použití ASCII znaků nezávislý na platformě. Soubory s certifikáty Base64 mají typicky příponu .pem.