Certifikační autorita

Certifikační autorita (zkratka **CA**) je v asymetrické kryptografii subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče), čímž usnadňuje využívání PKI (Public Key Infrastructure) tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Na základě *principu přenosu důvěry* (viz níže) tak můžeme důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že důvěřujeme samotné certifikační autoritě.

Na Internetu působí mnoho komerčních certifikačních autorit, které obvykle mají své veřejné klíče umístěny přímo ve webových prohlížečích a dalších programech, čímž mohou uživateli zjednodušit rozhodování o míře důvěry webových serverů, ke kterým se připojuje (ale též digitálně podepsaných e-mailů i jiných dat). Existují též bezplatné certifikační autority nebo takové, které se řídí zákony daného státu, vnitřními předpisy organizace a podobně.

Činnost certifikační autority

Certifikační autorita vydává digitální certifikáty, což jsou elektronicky podepsané veřejné šifrovací klíče, které obsahují identifikační údaje svého majitele, za jejichž správnost se certifikační autorita zaručila. Když certifikační autorita podepíše svůj vlastní klíč, jedná se o certifikát podepsaný sám sebou (*self-signed certificate*).

Majitel veřejného klíče musí proto při žádosti o vydání digitálního certifikátu důvěryhodným způsobem certifikační autoritu přesvědčit, že jím poskytnuté údaje odpovídají skutečnosti a tomu, co uvedl ve svém veřejném klíči. Může tak například učinit:

- fyzická osoba
  - přeložením občanského průkazu zástupci certifikační autority
  - vlastnictvím e-mailové schránky
- právnická osoba
  - předložením ověřeného výpisu z obchodního rejstříku
  - vlastnictvím internetové domény se stejnými údaji ve Whois databázi

Po ověření a porovnání výše uvedených údajů vydá certifikační autorita digitální certifikát, který ověřené údaje obsahuje. Důležitou součástí digitálního certifikátu je elektronický podpis, kterým lze snadno ověřit jeho autentičnost. Pokud by byly údaje v digitálním certifikátu změněny, kryptografické ověření digitálního podpisu by změnu odhalilo.

Důvěra v certifikační autoritu

Hodnota digitálního certifikátu je úměrná míře důvěry, kterou máme k údajům v něm uvedených. Proto je pro certifikační autoritu nejdůležitější důvěra, kterou vůči svému okolí vzbuzuje (tj. že nevydá digitální certifikát s nepravdivými údaji). Certifikační autorita proto musí adekvátním způsobem pečovat o svoji důvěryhodnost, jinak by nebylo možné využít principu přenosu důvěry (viz níže). Důvěryhodnost certifikační autority můžeme posoudit podle jejích webových stránek, použitého mechanismu ověření údajů, které žadatel o digitální certifikát předkládá a dalších znaků (články v tisku a elektronických médiích, kótované akcie a podobně). Cena vydaného certifikátu (resp. oblíbenosti certifikační autority) pak obvykle odpovídá této těžko exaktně definovatelné míře důvěry.

Placené certifikační autority získávají od svých klientů peníze, které používají jednak na zajištění vlastní činnosti, ale hlavně na platbu za zařazení vlastních kořenových certifikátů do software, který využívá přenosu důvěry (viz níže). Certifikační autority tak platí za distribuci svých kořenových certifikátů v Microsoft Windows, Firefoxu a dalších programech.

Přenos důvěry

Přenos důvěry se běžně využívá v reálném světě. Čteme časopisy, noviny, hovoříme s lidmi, sledujeme televizi. Pokud se dozvíme něco nového, přikládáme informaci váhu podle důvěryhodnosti zdroje informací. Přenášíme tak důvěryhodnost zdroje informací na jím poskytovanou informaci. Věříme více svým blízkým přátelům nebo autoritám (seriózní noviny, učitel ve škole, kvalitní kniha, odborný pořad v televizi). Naopak s rezervou obvykle přistupujeme k informacím „jedna paní povídala“ nebo k reklamě. Nevěříme řádně odsouzenému člověku nebo prokázanému falzifikátu.

Stejným způsobem se uplatňuje přenos důvěry u certifikační autority. Je-li certifikační autorita důvěryhodná, můžeme věřit informacím uvedených v digitálních certifikátech, které vydala (resp. digitálně podepsala). Věříme, že by certifikační autorita nevytvořila digitální certifikát s nepravdivými údaji.

V počítači jsou šifrovací klíče uloženy v úložišti certifikátů nebo v klíčence. Při ověřování autentičnosti veřejného klíče můžeme využít toho, že klíč je digitálně podepsán důvěryhodnou certifikační autoritou (jinou osobou atp.). Pokud je digitální podpis certifikátu platný a důvěřujeme certifikační autoritě, která klíč podepsala, přeneseme důvěru a věříme v důvěryhodnost neznámého veřejného klíče.

Pro usnadnění přenosu důvěry jsou v počítači obvykle předem přítomny kořenové klíče certifikačních autorit, které jsou distribuovány buď přímo s operačním systémem (Microsoft Windows) nebo s příslušnou aplikací (Firefox, Opera, Thunderbird atd.). Do úložiště je možné přidávat další certifikáty a následně důvěřovat certifikátům, které jsou jimi ověřitelné.

Kvalifikovaná certifikační autorita

Kvalifikovaná certifikační autorita je rámci České republiky definována *Zákonem o elektronickém podpisu* (zákon č. 227/2000 Sb.). Seznam akreditovaných certifikačních autorit, které mohou vydávat kvalifikované certifikáty, zveřejňuje Ministerstvo vnitra České republiky.

Akreditovaná certifikační autorita vydává (zpoplatněné) *kvalifikované certifikáty*, což jsou standardní digitální certifikáty, které však jsou výše zmíněným zákonem uznávány v rámci komunikace se státními institucemi České republiky. Kvalifikovaný certifikát je ze zákona akceptován stejně jako občanský průkaz, avšak možnost využití kvalifikovaného certifikátu je omezena na vyjmenované případy (státní instituce musí být připraveny a jejich zaměstnanci příslušně proškoleni):

- komunikace elektronickou cestou se státní správou pomocí emailu
- pro ověřování elektronických podpisů
- pro bezpečné ověřování elektronických podpisů
- zajištění neodmítnutelnosti odpovědnosti

Z hlediska právní platnosti je jedno, u které akreditované certifikační autority je certifikát vytvořen. Kvalifikované certifikáty se řídí RFC 3039, přičemž zákon dále nařizuje používání

položek *Key Usage* a *nonRepudiation* bitu. Problémem kvalifikovaných certifikátů je šifrování, protože elektronický podpis nezahrnuje důvěrnost (realizovanou šifrováním).

Kvalifikované certifikační autority stojí v současné době mimo klasické celosvětově působící certifikační autority a zákon ani jiný stav nepředpokládá. Před ověřením kvalifikovaného certifikátu si proto uživatel musí do příslušného programu (webový prohlížeč, e-mailový klient) sám nainstalovat certifikát příslušné kvalifikované certifikační autority (a sám ověřit jeho důvěryhodnost), což je v současné době pravděpodobně nejslabší místo kvalifikovaného certifikátu, protože důležitost jeho důvěryhodnosti kvalifikované certifikační autority nezdůrazňují a své certifikáty mají jednoduše vystaveny na svých webových stránkách.

Zneplatnění certifikátu

Digitální certifikát lze zneplatnit před ukončením jeho deklarované platnosti pomocí seznamu zneplatněných certifikátů (CLR), který je obvykle zpřístupněn na stránkách příslušné certifikační autority. Omezení doby platnosti certifikátu zabraňuje přetěžování CLR. Zpracování CLR může podporovat program, který s certifikáty pracuje (nejlépe automaticky a průběžně). Zneplatnění omezuje možné zneužití certifikátu a dochází k němu především ze dvou důvodů:

1. při změně údajů uvedených v certifikátu
2. při ohrožení soukromého klíče (zcizení klíče, prozrazení heslové fráze)