JAK NA INTERNET

Elektronický podpis

Velké množství komunikace dnes probíhá v elektronické formě. To má mnohé výhody, jako například pohodlnost či úspora času. Elektronická komunikace má ale i své nevýhody, mezi které patří i problém ověřit identitu protistrany.

V reálném světě máme několik možností, jak doložit svoji identitu. Mezi ty nejběžnější patří občanský průkaz a vlastnoruční podpis. Tyto metody jsou ale pro komunikaci po Internetu nevhodné. Jako náhradu máme takzvaný elektronický podpis.

Cíle

Elektronický podpis zajišťuje několik různých věcí. První z těch důležitějších je zajištění integrity dokumentu. Pokud dostaneme elektronicky podepsaný dokument, lze ověřit, že od jeho podpisu nebyl změněn. Pokud změněn byl, dozvíme se to a můžeme podniknout odpovídající kroky (například mu nevěřit, podobně jako smlouvě s propiskou opravenými některými pasážemi).

Další funkcí je jedinečnost elektronického podpisu. U běžného podpisu toto zajišťuje unikátnost písma, za elektronickým podpisem v tomto stojí kryptografie.

A nakonec, elektronický podpis lze použít i k tomu, aby příjemce dokázal ověřit, že odesílatel je opravdu tím, za koho se vydává. To se na první pohled zdá stejné, jako minulá funkce, ale není. Já se můžu pokaždé vlastnoručně podepsat jako Jan Novák a příjemce může ověřit, že jsem stále tatáž osoba (mám stejný podpis), ale Jana Nováka to ze mě neudělá. V reálném světě máme pro tento účel občanský průkaz vydávaný státní mocí.

Fungování

Elektronický podpis je soubor binárních dat, který lze připojit k dokumentu (například PDF dokumentu, e-mailu, či požadavku v internetovém bankovnictví). Nemá žádný speciální smysl, jen musí určitým způsobem odpovídat podepisující entitě a obsahu dokumentu.

K vytvoření podpisu potřebujeme podpisový klíč. Ten má dvě části – soukromou a veřejnou. Ty lze vytvořit zároveň, ale jednu z druhé nelze odvodit (jedině zkoušením všech možností, kterých je ale pro útok příliš mnoho).

Pomocí soukromé části a dokumentu lze spočítat ona binární data. Pomocí veřejné části a dokumentu lze zkontrolovat, že se jedná o stejný dokument jaký byl podepsán a že ona binární data byla vytvořena pomocí odpovídající soukromé části. Pokud tedy dokážeme udržet soukromou část v tajnosti a příjemci dáme naši veřejnou část, máme splněné první dva cíle.

Třetí cíl je po technické stránce také jednoduchý, avšak v praxi mírně problematický. V reálném světě k tomu máme občanský průkaz vydaný státní mocí. Obdoba vydavatele občanských průkazů pro podpisové klíče je certifikační autorita. Certifikační autorita je entita, které všichni věří a znají její veřejnou část klíče. Tato certifikační autorita poté může vytvářet dokumenty, které obsahují jak veřejnou část něčího klíče, tak jeho identifikační údaje (jako jméno). Takový dokument poté podepíše a předá majiteli. Tomuto dokumentu se říká certifikát.

Nyní tedy příjemce, který má certifikát, může ověřit, že podepisující má odpovídající soukromý klíč a že autorita ručí za to, že se jmenuje tak, jak nám tvrdí.

Samozřejmě, takový certifikát nemusí mít jen osoba. Mnoho webových serverů má svůj certifikát. Prohlížeč při přístupu na zabezpečené stránky (například internetové bankovnictví) zkontroluje, že server je ten, za který se vydává (a případně upozorní, pokud něco není v pořádku – když například nevěří té certifikační autoritě, kterou byl certifikát podepsán).

Praxe

Pokud si chceme pořídit klíč a certifikát, je důležité vědět, k čemu jej chceme používat. Vnitrofiremní komunikaci lze podepisovat certifikáty vydanými vedením firmy. Banky často vydávají certifikáty svým klientům, aby s nimi mohly bezpečně komunikovat. Pokud však chceme mít certifikát pro běžné používání, musíme si najít nějakou obecně uznávanou autoritu. Pro komunikaci s úřady potřebujeme dokonce kvalifikovaný certifikát, které u nás vydávají tyto autority:

- První certifikační autorita (I.CA)
- PostSignum (Česká pošta)
- Eldentity

Poté, co jsme si vybrali certifikační autoritu a pročetli si její podmínky a další dokumenty, vygenerujeme si obě poloviny klíče. K tomu existuje mnoho programů, většina autorit některý doporučí či přímo poskytne. Výsledkem tohoto procesu jsou dvě věci. Jednak soubor se soukromým klíčem a jednak soubor s požadavkem. Požadavek je jen veřejná polovina klíče, jméno a další identifikační údaje, podepsaná soukromou polovinou. Tento požadavek doneseme společně s občanským průkazem a administrativním poplatkem na pobočku autority, která nám vytvoří certifikát.

Nakonec dáme soukromý klíč a certifikát k dispozici programu, ve kterém chceme generovat podpisy (například emailový klient) a můžeme začít podepisovat dokumenty.

Bezpečnost

Samozřejmě je na místě se ptát, jak je tento způsob bezpečný. Přímé kryptografické útoky nejsou známy (například není znám jiný způsob zjištění soukromého klíče z veřejného, než vyzkoušet všechny možné soukromé klíče, což by dnešním počítačům zabralo čas v řádech tisíců až milionů let). To je rozhodně lepší, než u klasického podpisu, věrohodně napodobit něčí podpis je snazší.

Ale jsou jiné metody. Pokud se útočníkovi podaří získat něčí soukromý klíč, může se za jeho uživatele bez problémů vydávat. Proto je velmi důležité s ním zacházet opatrně – nepůjčovat nikomu flashdisk, na kterém je uložený, nikdy jej nepoužívat na neznámém počítači a podobně. Soukromý klíč je obvykle chráněn heslem, ale tato ochrana je jen tak silná, jak silné je ono heslo. V případě podezření, že se ke klíči mohl někdo dostat (například notebook, na kterém byl uložen, byl ukraden), je třeba neprodleně informovat certifikační autoritu, která jej přidá na seznam zakázaných certifikátů.

Druhou možnost, kterou útočník může zkusit, je přesvědčit certifikační autoritu k vystavení certifikátu na cizí jméno. Toto by nemělo být jednoduché (zvláště u kvalifikovaných certifikačních

autorit), ale například s falešným občanským průkazem by to pravděpodobně šlo (ale pokud někdo má občanský průkaz na vaše jméno, pak se za vás již vydávat může, takže tím mnoho nezíská).

Alternativní přístupy

Entita, které věří úplně všichni, je poněkud problematická věc a obvykle nevzniká přirozeně (lze ji vytvořit například zákonem a všichni jí budou věřit prostě z povinnosti). Proto existují i jiné přístupy.

Kupříkladu systém PGP umožňuje mít veřejný klíč podepsaný více než jedním soukromým. Každý se za vás může zaručit tím, že vám podepíše váš klíč – tím říká, že věří, že jste to vy. Pokud vám někdo bude tvrdit, že se jmenuje Franta a pět vašich známých vám to svými podpisy potvrdí, pak mu to můžete docela dobře věřit. Pokud to potvrzují jen dva vám neznámí lidé, pak je to již méně důvěryhodné.