

Elektronické podpisy

Rudolf Klusal

AdminIT

6. listopadu 2011



Běžné odeslání souboru

- Uložím soubor
- Otevřu mail
- Pošlu soubor



Běžné odeslání souboru

- Uložím soubor
- Otevřu mail
- Pošlu soubor

Běžný příjem souboru

- Otevřu mail
- Stáhnu soubor
- Otevřu soubor



Běžné odeslání souboru

- Uložím soubor
- Otevřu mail
- Pošlu soubor

Běžný příjem souboru

- Otevřu mail
- Stáhnou soubor
- Otevřu soubor

Problémy

- Mezi odesláním a příjmem mohou vznikat bezpečnostní incidenty.
- Jedná-li se o soubor obsahující např. fakturu, může útočník fakturu pozměnit a nám tak třeba přijde méně peněz.



Co můžeme dělat?

- Zašifrovat email
- Zašifrovat celou komunikaci
- Podepsat email



Co můžeme dělat?

- Zašifrovat email
- Zašifrovat celou komunikaci
- Podepsat email

Šifrování a podepsání

- **Šifrování** znemožní přečtení souboru tomu, kdo nezná heslo
- **Podepsání** neznemožní nic, soubor můžeme i upravit, ale dále se tak soubor stane neplatným – platný je pouze původní originál



Identifikace, autorizace, autentifikace. . . kdo se v tom má vyznat?

- **Identifikace** nám říká, čí podpis je použit.



Identifikace, autorizace, autentifikace. . . kdo se v tom má vyznat?

- **Identifikace** nám říká, čí podpis je použit.
- **Autentifikace** je proces, při kterém se ověří, jestli je identifikovaná osoba právě identifikovanou osobou a ne nikým jiným.



Identifikace, autorizace, autentifikace. . . kdo se v tom má vyznat?

- **Identifikace** nám říká, čí podpis je použit.
- **Autentifikace** je proces, při kterém se ověří, jestli je identifikovaná osoba právě identifikovanou osobou a ne nikým jiným.
- **Autorizace** se zase váže k osobě (např. identifikované a autentifikované) a říká, co všechno *smí* daná osoba dělat.



Identifikace, autorizace, autentifikace... kdo se v tom má vyznat?

- **Identifikace** nám říká, čí podpis je použit.
- **Autentifikace** je proces, při kterém se ověří, jestli je identifikovaná osoba právě identifikovanou osobou a ne nikým jiným.
- **Autorizace** se zase váže k osobě (např. identifikované a autentifikované) a říká, co všechno *smí* daná osoba dělat.
- **Autenticita** je vlastnost dokumentu, který podepisujeme. Je-li dokument autentický, znamená to, že je „věrohodný“.



O čem všem se vlastně budeme bavit?

■ Elektronický podpis

- „Běžný“
- Zaručený
- Uznávaný

■ Elektronická značka

- „Běžná“
- Uznávaná

■ Časové razítko

- „Běžné“
- Kvalifikované

Trocha kryptografie

Abychom mohli řešit, jak fungují EP, musíme znát alespoň základní principy **klíčů**.

Co klíč je?

- Číslo
- Náhodná hodnota

Co klíč není?

- Ultimátní šifrovací řešení
- Všelék na problémy s přenosem

Princip šifrování

Ve stručnosti se využívá matematických vlastností součinu dvou prvočísel:

- Udělat součin $123456789 \times 23456789$ je snadné
- Najít v součinu 2895899850190521 dva správné dělitele už tak snadné není.
- Asymetrická kryptografie staví právě na těchto vlastnostech velkých čísel – dodnes neexistuje stroj, který by byl schopen v reálném čase provést **faktorizaci velkých čísel** v reálném čase.



Symetrická kryptografie

- U symetrické kryptografie se využívá jednoho klíče
- Tento klíč je použit jak pro **zašifrování**, tak pro **rozšifrování**.
- Další variantou je odesílání s dvěma klíči:
 - Chci poslat druhé osobě šifrovanou zprávu.
 - Zašifruji svým kódem a odešlu příjemci.
 - Ten zašifruje navíc svým kódem a odešle mně zpět.
 - Odstráním svůj kód a pošlu zpět příjemci.
 - Ten odstraní svůj klíč a má původní zprávu.
- Nevýhod má toto řešení opravdu dost:
 - Šíleně pomalé
 - Posílám vlastně 3×, pokud někdo sleduje (odposlouchává) celou komunikaci, nejen, že zjistí oba naše klíče, ale na základě nich dokáže spočítat i původní zprávu



Asymetrická kryptografie

- Staví na funkci **veřejného** a **soukromého** klíče.
- Pokud chcete, aby vám někdo poslal šifrovanou zprávu, odesílatel použije váš **veřejný klíč**, aby zprávu zašifroval.
- Zašifrovaná zpráva nejde (triviálně) rozšifrovat, jen za pomoci **soukromého klíče**.
- **Veřejný klíč** můžete klidně vystavit na váš web nebo si ho dát do podpisu emailu, proto se jmenuje právě veřejný.
- **Soukromý** klíč však nikde neukazujeme, slouží jen pro naši potřebu.



A jak to souvisí s elektronickým podpisem?

- Při práci s podepisováním „dokumentu“ využíváme též dvojice privátního a veřejného klíče
- Akorát je to s klíči **přesně naopak**, než u šifrování.
 - Zprávu podepíšu svým **soukromým klíčem**
 - Příjemce může použít můj **veřejný klíč** k ověření **autenticity** dokumentu



A proč je to naopak?

- Jde o rozdílné požadavky na to, co chceme s dokumentem či zprávou dělat
- Při šifrování nechceme, aby byla zpráva čitelná pro nikoho dalšího, proto zašifrujeme zprávu **celou**.
- Při podepisování však nechceme zneprístupnit zprávu někomu, kdo nechce třeba podpis řešit. Nepodepisujeme tedy celou zprávu, ale pouze její **hash**. Ten připojíme k odesílanému souboru a pošleme příjemci.
- Ověření **autenticity** dokumentu probíhá tak, že si příjemce vytvoří na své straně **vlastní hash** z přijatého souboru a zašifruje ho svým **veřejným klíčem**. Pokud se výsledky rovnají, s **největší pravděpodobností** jsou ekvivalentní i odesílaný a přijmutý soubor.



Ověření

- Pokud tedy soubor odpovídá hashi, který byl zašifrován jak mým **soukromým klíčem** i mým **veřejným klíčem**, jedná se o nezměněný soubor.
 - Nic víc nezjistíme:
 - Buď že je původní, anebo změněný, ale už nezjistíme kde je změněný.



Ověření

- Pokud tedy soubor odpovídá hashi, který byl zašifrován jak mým **soukromým klíčem** i mým **veřejným klíčem**, jedná se o nezměněný soubor.
 - Nic víc nezjistíme:
 - Buď že je původní, anebo změněný, ale už nezjistíme kde je změněný.
- Ale samozřejmě se nabízí otázka: Jak může příjemce věřit tomu, že nabízený **veřejný klíč** je skutečně párový k **soukromému klíči**, kterým jsem podepsal svoji zprávu?



Ověření

- Pokud tedy soubor odpovídá hashi, který byl zašifrován jak mým **soukromým klíčem** i mým **veřejným klíčem**, jedná se o nezměněný soubor.
 - Nic víc nezjistíme:
 - Buď že je původní, anebo změněný, ale už nezjistíme kde je změněný.
- Ale samozřejmě se nabízí otázka: Jak může příjemce věřit tomu, že nabízený **veřejný klíč** je skutečně párový k **soukromému klíči**, kterým jsem podepsal svoji zprávu?
- Řešením je tzv. **certifikát**.



Co to je ten „certifikát“?

- **Certifikát** je vlastně soubor, který říká něco ve smyslu: „Ano, ten **veřejný klíč**, který máte v ruce, je opravdu párový k tomu **soukromému klíči**, kterým byl podepsán dokument.“



Co to je ten „certifikát“?

- **Certifikát** je vlastně soubor, který říká něco ve smyslu: „Ano, ten **veřejný klíč**, který máte v ruce, je opravdu párový k tomu **soukromému klíči**, kterým byl podepsán dokument.“
- Ale samozřejmě – a opět, nabízí se podobná otázka, jako před tím: „Kdo mi zaručí, že tento certifikát je pravý a není padělaný někým, kdo chce, abych si předchozí tvrzení jen myslel?“



Co to je ten „certifikát“?

- **Certifikát** je vlastně soubor, který říká něco ve smyslu: „Ano, ten **veřejný klíč**, který máte v ruce, je opravdu párový k tomu **soukromému klíči**, kterým byl podepsán dokument.“
- Ale samozřejmě – a opět, nabízí se podobná otázka, jako před tím: „Kdo mi zaručí, že tento certifikát je pravý a není padělaný někým, kdo chce, abych si předchozí tvrzení jen myslel?“

Certifikační autorita

- Nebo též CA



Co to je ten „certifikát“?

- **Certifikát** je vlastně soubor, který říká něco ve smyslu: „Ano, ten **veřejný klíč**, který máte v ruce, je opravdu párový k tomu **soukromému klíči**, kterým byl podepsán dokument.“
- Ale samozřejmě – a opět, nabízí se podobná otázka, jako před tím: „Kdo mi zaručí, že tento certifikát je pravý a není padělaný někým, kdo chce, abych si předchozí tvrzení jen myslel?“

Certifikační autorita

- Nebo též CA
- ... ale mohl bych se ptát: Kdo mi zaručí. . . , ale ptát se nebudu. Proč?



Rekurze...

- Na takové otázky bych se mohl ptát skoro pořád a nikdy bych nedospěl konci, vždy bych potřeboval nějakou nadřazenou buňku, která by zase musela být ověřena nadřazenou nad sebe.
- Jak z této rekurze ven?



Delegování autority

- Certifikační autorita může být certifikovaná výše, ale musíme dojít k nějakému stropu.
- Využíváme známých certifikačních autorit, kterým „se prostě věří“.
- Poté platí, že všechny autority, které jsou ověřeny touto autoritou, jsou též autoritami.
- Věříme tedy těmto „podautoritám“ stejně, jako bychom věřili té nejvyšší.
- V momentě, co se nějaká (v nejhorším případě ona nejvyšší) autorita prokáže jako nevěrohodná, jsou všechny certifikáty všech podřízených autorit bez důvěry.



Alternativní přístupy

Ne každému může takový princip vyhovovat, proto existují i další možnosti, jak něco (někoho) autentifikovat.



Alternativní přístupy

Ne každému může takový princip vyhovovat, proto existují i další možnosti, jak něco (někoho) autentifikovat.

Web of Trust

- Jedná se vlastně o téměř či úplně decentralizovanou síť uživatelů, kteří tím, že se u dané autority podepisují, jí předávají důvěryhodnost.
- Distribuovaná důvěra.



Alternativní přístupy

Ne každému může takový princip vyhovovat, proto existují i další možnosti, jak něco (někoho) autentifikovat.

Web of Trust

- Jedná se vlastně o téměř či úplně decentralizovanou síť uživatelů, kteří tím, že se u dané autority podepisují, jí předávají důvěryhodnost.
- Distribuovaná důvěra.

Biometrické podpisy

Mohou využívat otisku prstu či jiných těžko nahraditelných vlastností člověka (oční sítnice atd.) Nevýhodou je, že klíč se musí často aktualizovat – s tím, jak roste a vyvíjí se tělo, se mění i klíč.

Kde sehnat takový podpis?

- V ČR je asi nejznámějším Post Signum, který nabízí Česká pošta.
- Verisign.



Kde sehnat takový podpis?

- V ČR je asi nejznámějším Post Signum, který nabízí Česká pošta.
- Verisign.

PostSignum

- PostSignum Root QCA – kořenová autorita
 - PostSignum QCA – kvalifikované certifikáty
 - PostSignum VCA – komerční certifikáty
- PostSignum Root QCA 2 – kořenová autorita
 - PostSignum QCA 2 – kvalifikované certifikáty
 - PostSignum VCA 2 – komerční certifikáty
 - PostSignum TSA – poskytuje časová razítka



Kontaktní informace

Pokud byste mi chtěli napsat nebo se na něco zeptat, budu rád, když se ozvete na následující:

- jméno: Rudolf Klusal
- email: klusik@klusik.cz
- jabber: [klusik@jabber.cz](jabber:klusik@jabber.cz)
- web: <http://www.klusik.cz>



Kontaktní informace

Pokud byste mi chtěli napsat nebo se na něco zeptat, budu rád, když se ozvete na následující:

- jméno: Rudolf Klusal
- email: klusik@klusik.cz
- jabber: [klusik@jabber.cz](jabber:klusik@jabber.cz)
- web: <http://www.klusik.cz>

Dotazy z publika

Máte-li nějaké dotazy, ptejte se. Případně pokud je to „na déle“, můžete si mě tu někde odchytnout a rád si popovídám :-)



Díky za pozornost ;)

