Informace o SSL certifikátech v systému ISDS

Úvod

Do ISDS přistupují dva typy uživatelů:

1. Běžní uživatelé přistupující prostřednictvím webového prohlížeče na portál ISDS.
2. Aplikace třetích stran (např. spisové služby) přistupující k webovým službám ISDS.

Obě tyto skupiny přistupují do ISDS zabezpečeným SSL kanálem. Pro sestavení zabezpečeného SSL spojení se používá SSL certifikát, který poskytuje server na straně ISDS klientské aplikaci, kterou je buď webový prohlížeč nebo např. spisová služba.

Klientská aplikace musí důvěřovat SSL certifikátu, který ISDS poskytuje. Jinými slovy musí důvěřovat certifikační autoritě, která certifikát vydala – musí ji mít uloženu ve svém úložišti důvěryhodných kořenových certifikátů.

Webové prohlížeče mohou používat úložiště operačního systému (Internet Explorer ve Windows, Safari na Mac OS) nebo mít vlastní úložiště (Mozilla Firefox). U aplikací třetích stran záleží na způsobu jejich implementace; často však používají také vlastní úložiště důvěryhodných certifikátů uložené v souboru. Tento soubor se označuje termínem „truststore“.

Ověřování platnosti SSL certifikátu ISDS

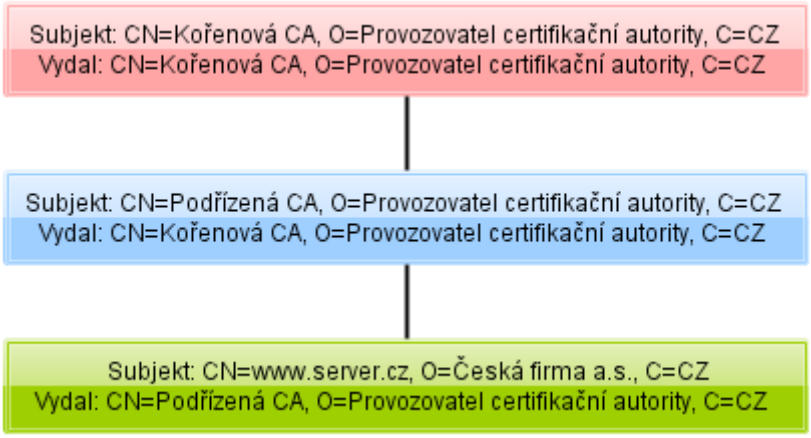
Při navazování SSL spojení musí klientská aplikace (webový prohlížeč, spisová služba, atd.) provést několik kontrol platnosti SSL certifikátu, který obdrží od ISDS.

Jednou z nich je sestavení řetězce certifikátů až k důvěryhodnému kořenovému certifikátu. Aplikace vyhledává certifikát certifikační autority (CA), který vydal SSL certifikát ISDS. K tomu používá úložiště důvěryhodných certifikátů, o němž byla řeč výše, případně řetězec certifikátů, který klientské aplikaci předává ISDS spolu s SSL certifikátem.

Vyhledání certifikátu CA probíhá na základě údajů o vystaviteli, uložených v SSL certifikátu, a také na základě rozšíření certifikátu „authorityKeyIdentifier“, které obsahuje SHA-1 otisk veřejného klíče v certifikátu CA. Aplikace tedy hledá takový certifikát, který má stejný otisk veřejného klíče (bývá uložen v rozšíření „subjectKeyIdentifier) a v subjektu certifikátu se nacházejí stejné údaje jako údaje o vystaviteli v SSL certifikátu.

Ale řetězec certifikátů nemusí být tvořen pouze SSL certifikátem a CA, která jej vydala. Certifikát samotné CA mohla vydat další, nadřízená CA, jejíž certifikát je opět nutné vyhledat a zařadit do řetězce certifikátů. Tímto způsobem pokračuje klientská aplikace až do okamžiku, kdy narazí na certifikát CA, který byl vydán stejnou CA (subjekt a vystavitel certifikátu jsou stejní). Toto je tzv. samopodepsaný certifikát a také kořenový certifikát, který tvoří „konec“ řetězce certifikátů.

Názornější představu o řetězci certifikátů si můžete udělat z následujícího obrázku:



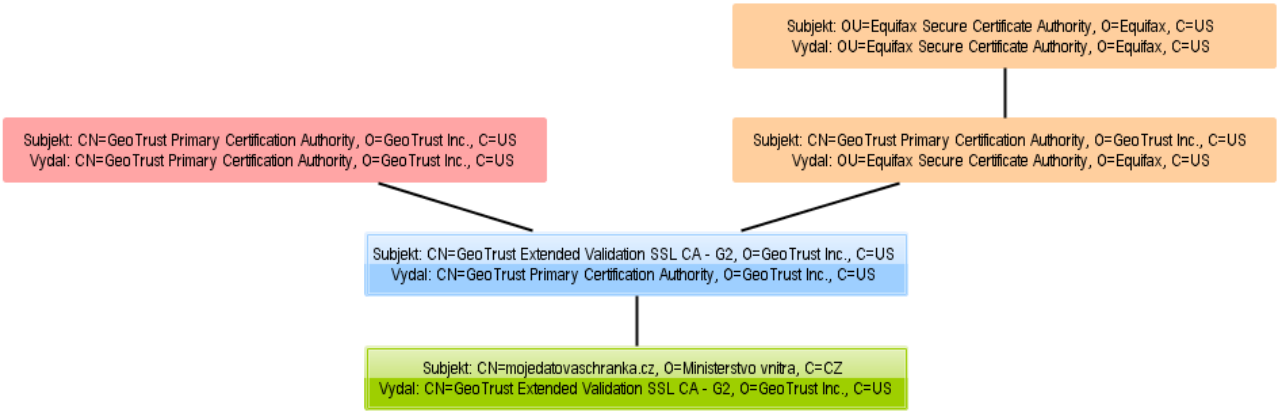
Certifikační autorita GeoTrust a její specifikum

SSL certifikáty systému ISDS pro zajištění bezpečné komunikace s „vnějším světem“ jsou vydány certifikační autoritou **GeoTrust**. Je to z toho důvodu, že GeoTrust patří do skupiny certifikačních autorit, jejichž certifikáty jsou standardní součástí výše zmiňovaných úložišť důvěryhodných certifikátů v operačních systémech nebo webových prohlížečích. V praxi to znamená, že uživatelé s webovým prohlížečem nemusí provádět žádné činnosti nezbytné pro zajištění důvěryhodnosti SSL certifikátu ISDS.

Dalším důvodem je použití tzv. Extended Validation (EV) certifikátů v ISDS. Tyto certifikáty mají tu vlastnost, že ve webovém prohlížeči se zobrazí zelený adresní řádek, případně jiný grafický prvek, který má signalizovat, že pro vydání tohoto certifikátu bylo provedeno přísnější ověření identity žadatele o certifikát (tedy provozovatele daného serveru či systému).

Certifikační autorita GoTrust má určité specifikum ve způsobu sestavení řetězce certifkátů. Pro SSL certifikát ISDS lze totiž sestavit dva řetězce certifikátů – jeden je zakončen kořenovou CA GeoTrust, druhý je zakončen kořenovou CA Equifax.

Pro nový SSL certifikát ISDS, který se bude nasazovat v červenci 2014, lze vytvořit tyto řetězce certifikátů:



Oba řetězce certifikátů mají společný SSL certifikát serveru a podřízenou CA „GeoTrust Extended Validation SSL CA – G2“. Na vyšší úrovni však již dochází k rozdělení na „levý“ a „pravý“ řetězec.

„Levý“ řetězec je zakončen kořenovým certifikátem CA GeoTrust s názvem „GeoTrust Primary Certification Authority“.

„Pravý“ řetězec pokračuje certifikátem, který má rovněž název „GeoTrust Primary Certification Authority“ (a obsahuje stejný veřejný klíč), ale byl vydán CA Equifax; nejedná se tedy o kořenový

certifikát. „Pravý“ řetězec je zakončen kořenovým certifikátem „Equifax Secure Certificate Authority“.

Co to znamená pro uživatele s webovým prohlížečem?

Nic zásadního. Nadále se budou pomocí webového prohlížeče přihlašovat korektně do portálu ISDS.

Z testování vyplynulo, že webové prohlížeče sestavují „levý“ řetězec certifikátů zakončený kořenovým certifikátem CA GeoTrust (viz obrázek výše). Nový SSL certifikát vydala podřízená CA „GeoTrust Extended Validation SSL CA - G2“. Může se stát, že v úložišti důvěryhodných certifikátů v operačním systému nebo ve webovém prohlížeči bude certifikát této CA chybět. ISDS ale předá tento certifikát v řetězci certifikátů spolu s SSL certifikátem, takže se uživatel nadále korektně připojí k ISDS, aniž by se zobrazila hláška o nedůvěryhodném certifikátu. To si ostatně můžete vyzkoušet na testovacím prostředí, kde je již nový SSL certifikát (vydaný „G2-kovou“ CA) nasazen. Do webového prohlížeče zadejte adresu: https://www.czebox.cz

Co to znamená pro uživatele a dodavatele aplikací třetích stran?

V tomto případě může dojít za určitých okolností k problému. Problém se týká „truststore“, který daná aplikace používá, případně způsobu implementace sestavování a ověřování řetězce certifikátů.

Pokud je aplikace naprogramována tak, že v „truststore“ má uložen pouze koncový SSL certifikát serveru ISDS, samozřejmě si musí do „truststore“ zařadit nový SSL certifikát, jinak přestane komunikace po nasazení nového SSL certifikátu fungovat.

Dále může dojít k této situaci. Server ISDS předává klientské aplikaci „pravý“ řetězec certifikátů zakončený kořenovým certifikátem CA Equifax (viz obrázek výše). Stejný řetězec bude předáván i po nasazení nového SSL certifikátu. Seznam certifikátů předávaných v rámci SSL spojení si můžete zobrazit např. pomocí aplikace Portecle (psaná v jazyce Java; http://portecle.sourceforge.net/) - volba „Examine SSL/TLS Connection“, nebo pomocí aplikace OpenSSL zadáním příkazu:

openssl s_client -showcerts -connect *hostname*:443

Místo „*hostname*“ zadejte jméno serveru (DNS jméno nebo IP adresa), na který přistupujete svou aplikací.

K problému může dojít v případě, pokud je v „trustore“ aplikace uložen jiný řetězec certifikátů – např. „levý“ řetězec z výše uvedeného obrázku. Aplikace může odmítnout SSL spojení z důvodu nedůvěryhodného SSL certifikátu. Problém byl zjištěn u aplikace CURL a je pravděpodobné, že se může týkat také dalších aplikací využívajících knihovny OpenSSL.

Řešením je do „truststore“ aplikace umístit „pravý“ řetězec certifikátů z výše uvedeného obrázku (zakončený kořenovým certifikátem CA Equifax). Mělo by dokonce stačit přidat pouze kořenový certifikát CA Equifax. Pokud potřebujete získat tento certifikát důvěryhodnou cestou, stáhnete jej z této webové stránky certifikační autority GeoTrust:

http://www.geotrust.com/resources/extended-validation-ssl/root-certificates.html

Soubor s certifikátem stáhněte z odkazu „Equifax Secure Certificate Authority (this root is included in all browser's root store)“.

Datum: 9.7.2014