Certifikační Autorita TrustCert

Certifikační autorita TrustCert, v České a Slovenské republice poskytující své služby přes společnost AEC, spol. s r.o. je jednou z prvních institucí, které se rozhodly přispět k bezpečné komunikaci svými zkušenostmi a znalostmi.

Jádro poskytovaných služeb spočívá v použití špičkové PKI technologie společnosti Norman Data Defense Systems a rovněž tak v detailně propracovaných prováděcích mechanismech, bez kterých nemůže kvalitní certifikační autorita existovat.

Certifikační autorita TrustCert vydává svým klientům osobní certifikáty, serverové certifikáty a certifikáty pro podepisování datových objektů.

Co je to digitální certifikát?

Digitální certifikát je digitální verzí Vaší identifikace. Je elektronickou obdobou identifikačního průkazu nebo dokladu o existenci právnické osoby. Digitální certifikát je používán k dokazování Vaší identity třetím stranám při elektronické komunikaci nebo při přístupu k informacím a službám on-line. Uživatel si vytvoří tzv. klíčový pár, který je unikátním pro každého uživatele. Skládá se ze dvou částí: soukromého klíče a veřejného klíče.

A Co musím udělat, abych obdržel digitální certifikát, vydaný certifikační autoritou TrustCert?

Nejjednodušší cestou je kontaktovat nás on-line, elektronickou poštou nebo nám zavolat o informace. Na webovské stránce http://www.trustcert.cz, si můžete rovněž vygenerovat klíčový pár a následně downloadovat DEMO certifikát. Pro obdržení detailního popisu certifikačních služeb, poskytovaných TrustCert, zavolejte naše pracovníky na tel. č.: +420-5-41235466

Certifikační autorita - nástroj bezpečné komunikace

V současné době, kdy potřeba komunikovat roste obrovským tempem a nadále již není možné všechny důležité kontakty „zaopatřit“ osobně, zabírá elektronická komunikace stále větší část celé komunikační „rodiny“. S tím roste přímo úměrně i potřeba tuto komunikaci zabezpečit a vnést do ní ovzduší důvěry. Spolu s masovým rozmachem datové komunikace může (a bude) přibývat datových pirátů a zločinců. Právě proto je budoucnost takové komunikace ve stále rozšiřovaném zavádění bezpečnostních mechanismů. Nejedná se přitom jen o šifrovanou komunikaci, ale především o masové zavádění autentizačních produktů, které zajišťují nepoškozenost a verifikaci původce jednotlivých informací, zpráv, či datových souborů. Mnoho lidí v současné době (z objektivních příčin) nedůvěřuje Internetové komunikaci a brání se proto svěřovat tomuto médiu privátní informace (např. čísla kreditních karet).

Široké zavádění asymetrické kryptografie v souvislosti s takovou bezpečností vede k nezbytnosti používání digitálních podpisů, digitálních Certifikátů a služeb Certifikačních a Registračních Autorit. Vysvětleme si tedy pár takových pojmů:

• Digitální podpis je ve své podstatě implementací určité matematické funkce prostřednictvím specializovaného programu, jejímž připojením k určitému dokumentu dochází k ověření jeho autentičnosti. Není to ovšem připojení pasivní (jako třeba pečeť na královské listině), ale aktivní - matematická funkce obsažená v digitálním podpisu nejprve provede výpočet kontrolních hodnot příslušného dokumentu až a poté se k němu připojí. (Pod pojmem „aktivní“ si ovšem nesmíme představovat, že dojde ke změně v podpisu při každé změně v dokumentu - podpis je jednou daný a nelze jej ani dokument modifikovat!).

• Digitální Certifikát je pak veřejným klíčem určitého uživatele, který je podepsán normou definovaným způsobem. Aby se však takovýto Certifikát stal důvěryhodným, je nezbytné, aby byl podepsán důvěryhodnou třetí stranou (Trusted Third Party). Právě takovými stranami se stávají Certifikační Autority.

Certifikáty a implementace Certifikačních Autorit do reálného života každého z nás se ve světle bezpečné komunikace jeví jako zásadní. Aby byla zabezpečena skutečná důvěryhodnost Certifikátů, vydaných jednotlivými Autoritami, pak je nutné, aby tyto Autority byly napojeny na další, vyšší Certifikační Autoritu (Root Certification Authority), která je celosvětově uznávána jako relevantní a věrohodná většinou společností. Takto vydané Certifikáty pak mají vysokou míru důvěryhodnosti. Je třeba dodat, že AEC je jednou z prvních společností, které tímto způsobem hodlají přispět k bezpečné komunikaci.

AEC se ve svém projektu zaměřeném na Certifikační Autoritu pochopitelně rozhodla jít cestou, která zabezpečí vysokou důvěryhodnost vydávaných Certifikátů. Aby byla zajištěna dostupnost těchto Certifikátů široké veřejnosti, je vždy nutné mít k dispozici řadu Registračních Autorit, které vydávají Certifikáty jménem Certifikační Autority, do jejíž sítě patří. V současné době proto probíhají intenzivní jednání s několika významnými společnostmi, které splňují ta nejnáročnější kritéria pro tento projekt.

Velkou výhodou spojení AEC a TrustCert je silná pozice na trzích v České i Slovenské republice, stejně tak, jako PKI řešení řady Norman® Security Suite, na kterém jsou služby TrustCert postaveny. Svým klientům tedy nenabízí „pouze“ jistotu, kterou přináší Digitální Certifikát, ale také možnost zavedení silného šifrování, které funguje jako jediný prostředek k úplnému zabezpečení dat.

NORMAN®

AEC, spol. s r.o.
Bayerova 30, 602 00 Brno
Tel.: 05/4123 5466-7
Fax: 05/4123 5038
e-mail: info@aec.cz
http://www.aec.cz

AEC
DATA SECURITY COMPANY