enterprise europe network

Podpora podnikania na dosah ruky

ELEKTRONICKÝ **PODPIS** A ELEKTRONICKÁ **IDENTIFIKÁCIA**

NÁRODNÁ AGENTÚRA PRE ROZVOJ MALÉHO A STREDNÉHO PODNIKANIA

Európska komisia
Podnikanie a priemysel

cip competitiveness and innovation framework programme 2007–2013

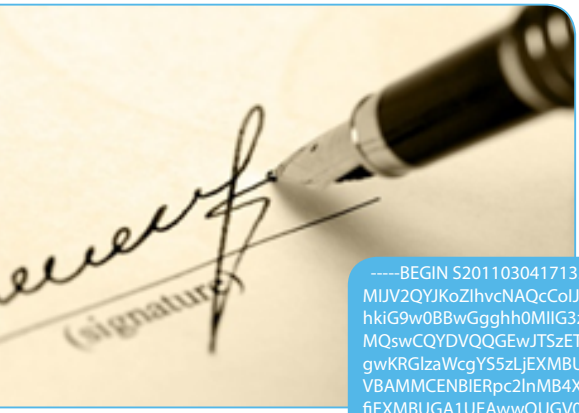
Dnešný moderný svet nám neustále prináša nové výzvy súvisiace s neuveriteľne rýchlym technickým pokrokom. Na konci uplynulého storočia a tisícročia, čo, ako by sa zdalo, nie je až tak dávno, sme všetci používali na vyjadrenie svojej slobodnej vôle a súhlasu vlastnoručný podpis s použitím pera a papiera. V banke si spoľahlivo chránili obrázok s našim naskenovaným podpisom, aby si pri každej operácii vyžadujúcej podpis overili, či je skutočne náš.

V tom čase nám ani nenapadlo, že v krátkom čase nastane doba, keď sa popri tom klasickom podpise, ktorý len tak mimochodom nemá žiadnu právnu úpravu, objaví podpis elektronický. Začiatkom nového tisícročia najskôr v podobe právnej úpravy, t.j. Zákona č. 215/2002 Z. z. o elektronickom podpise až po súčasnosť, keď sa elektronický podpis stáva súčasťou nášho každodenného života.

Že netušíte o čom to tu píšeme?

Ak patríte k tej časti populácie, ktorá sa snaží nepodľahnúť v plnej miere technologickému svetu súčasnosti, ktorý je plný počítačov, notebookov, mobilných zariadení všetkého druhu a aj napriek tomu chcete zostať informovaní, tak vám prinášame potrebné informácie týkajúce sa elektronického podpisu, jeho právnej úpravy, používaných typov a možnosti použitia v rámci elektronickej komunikácie.

Darmo by sme však hľadali nejakú právnu úpravu, ktorá definuje vlastnoručný podpis, ktorý sa používa už po stáročia. Je tomu tak aj napriek tomu, že z pohľadu ľudského správania vyvolávajúceho právne následky, ide o jeden z najvýznamnejších potvrdzovacích prejavov jednotlivca, ako aj iných právnych subjektov. Týmto je vytvorený priestor pre zdanlivo teoretické úvahy o tom, čo možno považovať za podpis vyvolávajúci právne účinky, a čo nie.



-----BEGIN S20110304171353Z.p7s-----
MIJV2QYJKoZIhvcNAQcCoIJVyjCCVcYCAQExDzANBglghkgBZQMEAgEFADALBgkq
hkiG9w0BBwGgghh0MIIG3zCCBMegAwIBAgIEAQAX+zANBgkqhkiG9w0BAQsFADBj
MQswCQYDVQQGEwJTSzETMBEGA1UEBwwKQnJhdGlzbGF2YTETMBEGA1UEC-
gwKRGlzaWcgYS5zLjEXMBUGA1UECwwOQUNBLTMwNy0yMDA3LTIxETAPBgN-
VBAMMCENBIERpc2InMB4XDTExMDExMDA5MTIyMVoXDTEzMDEwOTA5MTIyMVow-
fjEXMBUGA1UEAwwOUGV0ZXIgTWlza292aWMxDjAMBgNVBCoMBVBldGVyMREwD-
wYDVQQEDAhNaXNrb3ZpYzEYMBYGA1UEBwwPQmFuc2thIEJ5c3RyaWNhMQswC-
QYDVQQGEwJTSzEZMBcGA1UE

Legislatíva

Problematika elektronického podpisu v rámci Slovenskej republiky je legislatívne upravená zákonom č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, ktorého plné znenie bolo vyhlásené zákonom č. 76/2009 Z. z. Zákon o elektronickom podpise a súvisiacimi vyhláškami č. 131/2009 Z. z., 132/2009 Z. z., 133/2009 Z. z., 134/2009 Z. z., 135/2009 Z. z., 136/2009 Z. z. a 32/2010 Z. z.

Cieľom zákona č. 215/2002 Z. z. bolo umožniť zrovnoprávnenie elektronických dokumentov s dokumentmi v tlačenej podobe.

Zákon č. 215/2002 Z. z. je plne kompatibilný so Smernicou európskeho parlamentu a rady 1999/93/es z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy.

AKO JE VLASTNE PRÁVNE DEFINOVANÝ **ELEKTRONICKÝ PODPIS?**

Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,

b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie,

c) obsahuje údaj, ktorý identifikuje podpisovateľa.

Okrem elektronického podpisu definuje slovenská legislatíva ešte ďalší typ podpisu – **zaručený elektronický podpis** (**ZEP**).

ZEP musí spĺňať okrem vyššie uvedených požiadaviek ešte ďalšie 4 požiadavky:

a) je vyhotovený pomocou **súkromného kľúča**, ktorý je určený na vyhotovenie **zaručeného elektronického podpisu**,
b) možno ho vyhotoviť len s použitím **bezpečného zariadenia** na vyhotovovanie elektronického podpisu podľa § 2 písm. h),
c) spôsob jeho vyhotovovania umožňuje **spoľahlivo určiť**, ktorá **fyzická osoba** zaručený elektronický podpis vyhotovila,
d) na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu je vydaný **kvalifikovaný certifikát**.

Tieto ďalšie doplňujúce podmienky zaručujú vysokú úroveň bezpečnosti vytváraného ZEP v porovnaní s EP.
Definície EP a ZEP priniesli nové pojmy, ktoré sú vo svete elektronického podpisu veľmi dôležité a je potrebné si ich bližšie vysvetliť.

Súkromný kľúč a **verejný kľúč** tvoria systém, ktorý sa nazýva Infraštruktúra verejného kľúča (**Public Key Infrastructure – PKI**).

Tento systém umožňuje používateľovi, v podstate nezabezpečenej verejnej siete akou je napr. internet, bezpečnú a dôvernú výmenu informácií použitím práve kľúčového páru pozostávajúceho z verejného a súkromného kľúča, ktoré boli získané a sú zdieľané prostredníctvom dôveryhodnej autority.

PKI používa kľúčový pár na šifrovanie a rozšifrovanie. **Verejný kľúč** sa stáva verejným a **je publikovaný**, aby bol k dispozícii širokej verejnosti, zatiaľ čo **súkromný kľúč** nie je **nikdy poskytovaný ďalej** a musí zostať uchovávaný v bezpečí. Kľúčový pár má tú charakteristickú vlastnosť, že informácie zašifrované súkromným kľúčom je možné rozšifrovať len príslušným verejným kľúčom a naopak, informácie zašifrované verejným kľúčom je možné rozšifrovať len príslušným súkromným kľúčom. Tieto vlastnosti sú potom využívané na vytváranie elektronické podpisu a na zasielanie šifrovaných informácií nasledovne:

Elektronický podpis: elektronický dokument podpísaný súkromným kľúčom podpisovateľa je možné overiť kýmkoľvek, kto má k dispozícii verejný kľúč podpisovateľa. Na základe verejného kľúča sa dá totiž jednoznačne preukázať, že:

- podpisovateľ mal k dispozícii jemu prislúchajúci súkromný kľúč (kľúče tvoria jedinečnú dvojicu) t.j. je s veľkou pravdepodobnosťou, hraničiacou s istotou, autorom podpisu,
- elektronický dokument nebol zmenený.

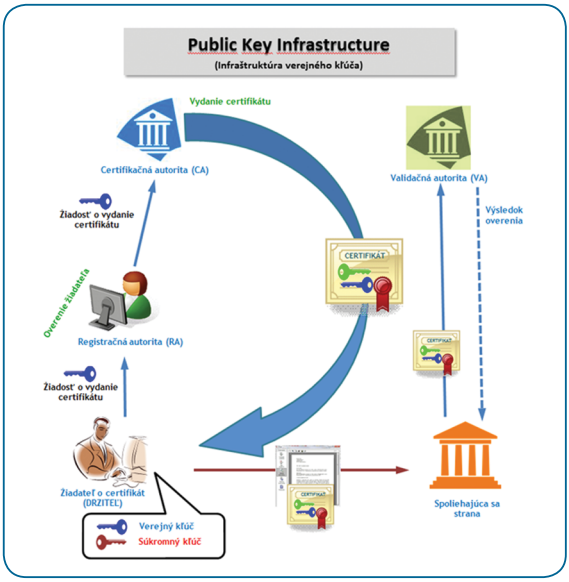
Šifrovanie verejným kľúčom: elektronický dokument zašifrovaný verejným kľúčom prijímateľa nemôže byť rozšifrovaný nikým iným okrem držiteľa príslušného súkromného kľúča – predpokladá sa, že ide o držiteľa kľúča a teda osobu zviazanú s použitým verejným kľúčom. Toto je využívané na zabezpečenie dôvernosti.

Infraštruktúra verejného kľúča (PKI): verejná infraštruktúra, ktorá spravuje, distribuuje a certifikuje elektronické kľúče a certifikáty, ktoré sú používané na overenie identity a šifrovanie informácií. Vo všeobecnosti je PKI systém elektronických certifikátov, certifikačných autorít, registračných autorít, ktoré potvrdzujú a overujú legálnosť všetkých strán zúčastňujúcich sa elektronickej výmeny údajov. (Richter & Roth, 2006)

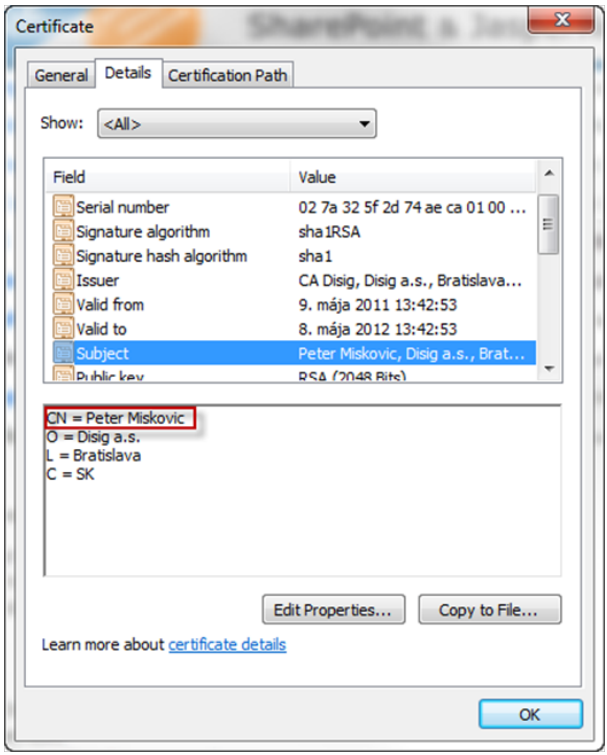
Zdroj: Dictionary of information science and technology / Mehdi Khosrow-Pour, editor (2007)

Infraštruktúra verejného kľúča (PKI) pozostáva z:

- certifikačnej autority (CA), ktorá vydáva a verifikuje certifikáty, ktoré obsahujú verejnú kľúč a informácie o ich držiteľovi
- registračnej autority (RA), ktorá koná v mene certifikačnej autority pri identifikácii autentifikácie žiadateľa o certifikát
- úložiska certifikátov, ktoré je verejne dostupné
- systému na správu certifikátov (vydávanie, rušenie)



Certifikát je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný (držiteľ certifikátu).



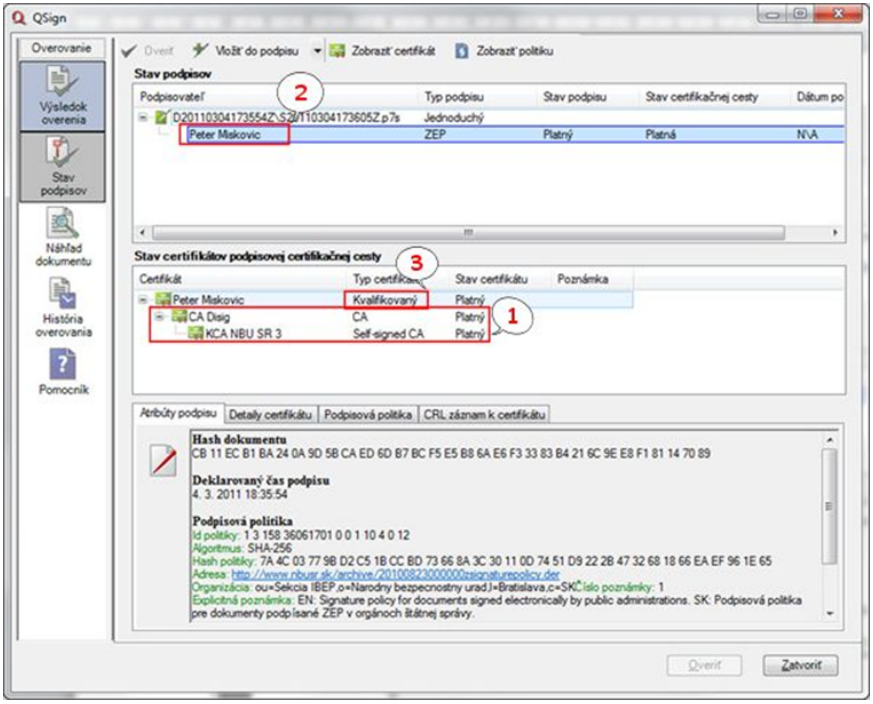
KVALIFIKOVANÝ CERTIFIKÁT JE CERTIFIKÁT FYZICKEJ OSOBY:

a) ktorý vydala akreditovaná certifikačná autorita (1 na obrázku nižšie) fyzickej osobe (2 na obrázku nižšie),

b) v ktorom je uvedené, že je kvalifikovaný (3 na obrázku nižšie),

c) v ktorom sú uvedené obmedzenia na jeho použitie, ak tretia strana také obmedzenia rozlišuje,

d) ktorý má telo certifikátu podpísané elektronickým podpisom akreditovanej certifikačnej autority (1 na obrázku nižšie), ktorý bol vyhotovený použitím súkromného kľúča určeného na tento účel.



Certifikačná autorita je poskytovateľ certifikačných služieb, ktorý spravuje certifikáty a vykonáva certifikačnú činnosť.

Akreditovaná certifikačná autorita je právnická alebo fyzická osoba – podnikateľ, ktorý má vytvorené materiálne, priestorové, technické, personálne, organizačné a právne podmienky na poskytovanie akreditovaných certifikačných služieb.

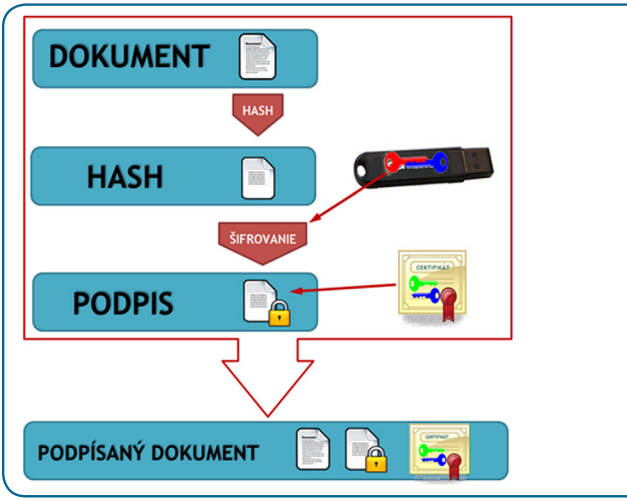
Bezpečné zariadenie na vyhotovenie elektronického podpisu je prostriedok na vyhotovenie elektronického podpisu, ktorý spĺňa požiadavky zákona č. 215/2002 Z. z., a ktorý slúži na vyhotovovanie zaručených elektronických podpisov.

Elektronický podpis a zaručený elektronický podpis

V zmysle Zákona č. 215/2002 Z. z. sa v styku s orgánmi verejnej moci používa elektronický podpis (EP) alebo zaručený elektronický podpis (ZEP). Ak sa v styku s orgánmi verejnej moci používa zaručený elektronický podpis, kvalifikovaný certifikát musí byť vydaný akreditovanou certifikačnou autoritou a musí obsahovať rodné číslo držiteľa certifikátu.

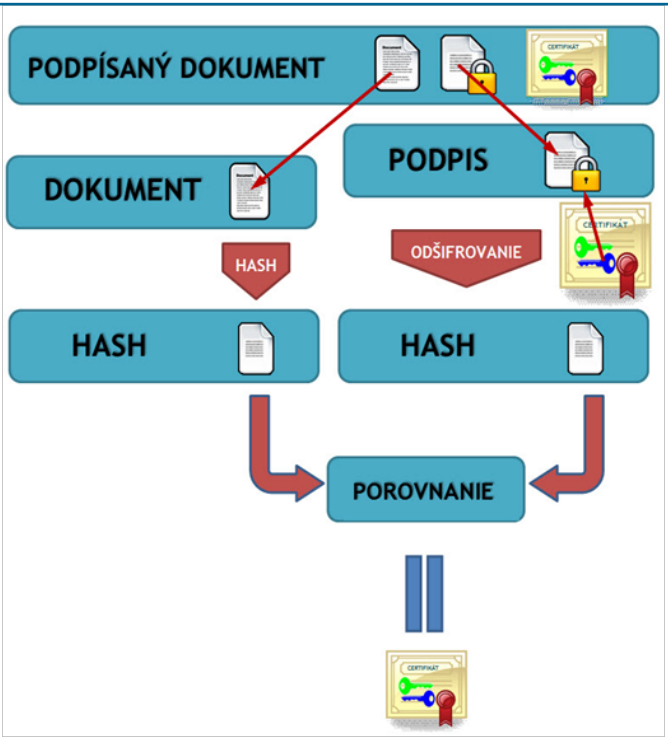
AKO SA VYTVÁRA **ELEKTRONICKÝ PODPIS**?

Z elektronického dokumentu sa prostredníctvom špeciálneho algoritmu (napr. SHA1 resp. SHA256) vytvorí odtlačok (angl. hash), ktorého dĺžka je pevne daná (pre ZEP je to v súčasnosti 256 bit). Získaný odtlačok sa zašifruje prostredníctvom známeho šifrovacieho algoritmu (napr. RSA) súkromným kľúčom podpisovateľa a k takto zašifrovanému odtlačku sa priloží certifikát resp. kvalifikovaný certifikát, vydaný podpisujúcej osobe certifikačnou autoritou. Priložením zašifrovaného odtlačku s certifikátom k elektronickému dokumentu vznikne podpísaný elektronický dokument.



Ako sa overuje **elektronický podpis?**

Pokiaľ máme k dispozícii podpísaný dokument, tak si môžeme overiť, či nebol od jeho popísania zmenený a na základe priloženého certifikátu zistiť, kto je jeho autorom. Postup overenia je nasledovný. Zoberieme zaslaný dokument a pomocou použitého hash algoritmu (SHA1 resp. SHA256) si vyrobíme z neho vlastný odtlačok. Potom zoberieme z podpisu zašifrovaný odtlačok a pomocou verejného kľúča podpisovateľa (je súčasťou certifikátu) ho rozšifrujeme. Potom nami vyrobený odtlačok a rozšifrovaný odtlačok navzájom porovnáme. Pokiaľ sa zhodujú, tak máme istotu, že elektronický dokument, ktorý bol podpísaný, nikto od podpísania nezmenil a keďže sa nám podarilo rozšifrovať odtlačok pomocou verejného kľúča podpisovateľa, tak z priloženého certifikátu vieme určiť, kto bol autorom.



Celé sa to javí zložité, ale je potrebné povedať, že podpisovanie i overovanie prebieha úplne automatizovane a popísanú funkcionalitu zabezpečuje príslušný softvér na podpisovanie a overovania elektronických dokumentov. V zmysle slovenskej legislatívy, pokiaľ sa vytvára ZEP, musí byť použitý podpisový softvér certifikovaný Národným bezpečnostným úradom SR (NBÚ SR).

Elektronický podpis zabezpečuje:

- integritu elektronického dokumentu
- identifikáciu a autentifikáciu podpisovateľa
- nepopierateľnosť vytvorenia (non-repudation)

Elektronický podpis nezabezpečuje:

- dôvernosť (privacy)

Kde dnes reálne môžeme **EP** a **ZEP** používať?

V súčasnosti existuje približne 28 slovenských právnych predpisov, ktoré sa zmieňujú o EP resp. ZEP. Z nich len niektoré sú aplikované v praxi tak, že ich využívanie zo strany fyzických resp. právnických osôb prerástlo do skutočnej elektronickej komunikácie s využitím EP resp. ZEP.

Najpoužívanejšie sú nasledovné:

Daňové riaditeľstvo SR
www.drsr.sk

Prostredníctvom portálu je možné predkladať všetky podania týkajúce sa daní fyzickej resp. právnickej osoby.

Podávajúca osoba potrebuje:
- Kvalifikovaný certifikát na bezpečnom zariadení certifikovanom NBÚ SR
- Pripojenie do internetu
- Nainštalovaný softvér na podpisovanie stiahnuteľný zo stránok DR SR
- Konto v elektronickej podateľni správcu dane a zmluvu o využívaní elektronickej služby

Colná správa SR
www.colnasprava.sk

Prostredníctvom portálu je možné vykonávať nasledovnú elektronickú komunikáciu:

- pri podávaní colných vyhlásení do režimu tranzit, pri ukončení režimu tranzit a pri správe záruky s úradom prijímania záruk v systéme NCTS
- pre podávanie žiadostí o informáciu o stave zabezpečenia dovoznej platby pri dovoze (GDS)
- pri podávaní colných vyhlásení vo vývoze a predbežných colných vyhlásení pri dovoze a vývoze
- pre podávanie a prijímanie správ pri preprave tovaru podliehajúcemu spotrebnej dani v režime pozastavenia dane v rámci systému EMCS (elektronický sprievodný administratívny dokument, správa o prijatí).

Podávajúca osoba potrebuje:
- Kvalifikovaný certifikát na bezpečnom zariadení certifikovanom NBÚ SR
- Pripojenie do internetu
- Nainštalovaný aplikačný softvér na komunikáciu s Colnou správou SR
- Dohodu o elektronickej komunikácii

Súdy v SR

Je možné podávať všetky druhy podaní na súdy v SR buď prostredníctvom e-mail adries jednotlivých súdov www.justice.gov.sk resp. prostredníctvom portálu ezaloby www.ezaloby.justice.sk.

Podávajúca osoba potrebuje:

- Kvalifikovaný certifikát na bezpečnom zariadení certifikovanom NBÚ SR
- Pripojenie do internetu s web prehliadačom resp. poštovým klientom
- Klientsku aplikácia na podpisovanie dokumentov - QSign
- Akreditovanú službu vydávania časovej pečiatky
- V prípade používania portálu ezaloby - registráciu na portáli a program 602XML Filler

Ústredný portál verejnej správy

www.portal.gov.sk

Slúži na elektronickú komunikáciu s Obchodným registrom SR a na možnosť elektronického podania pre 405 subjektov verejnej moci (notári, exekútori, orgány štátnej správy, katastrálne úrady, zdravotné poisťovne ap.).

Podávajúca osoba potrebuje:

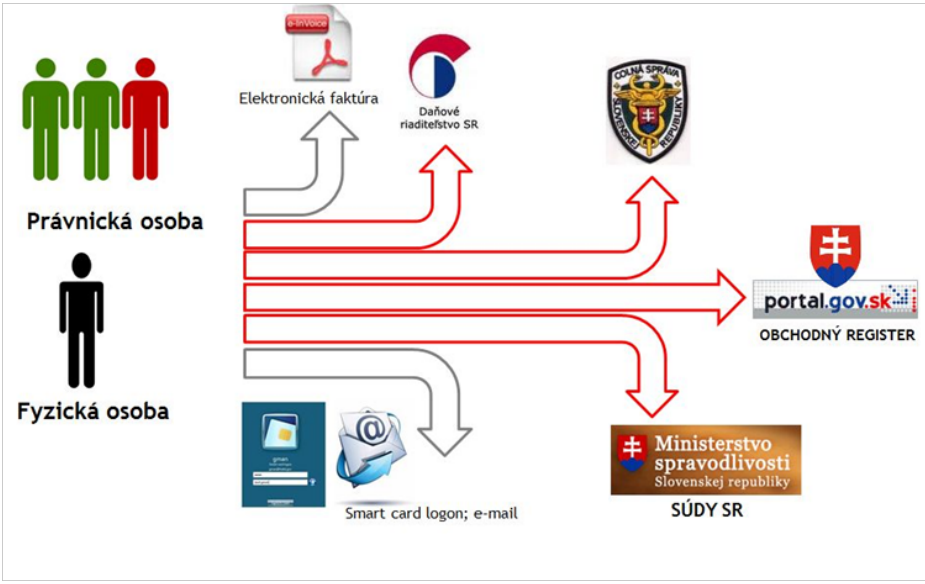
- Kvalifikovaný certifikát na bezpečnom zariadení certifikovanom NBÚ SR
- Pripojenie do internetu s webovým prehliadačom
- Klientsku aplikácia na podpisovanie dokumentov - QSign
- Registráciu na ÚPVS

Zasielanie elektronických faktúr

Zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov umožňuje so súhlasom prijímateľa zasielať faktúry elektronicky.

Zasielajúci potrebuje:

- Certifikát
- Pripojenie do internetu s poštovým klientom
- Aplikáciu umožňujúcu podpisovanie elektronických faktúr



Elektronický podpis resp. kryptografické kľúče majú ešte oveľa širšie použitie ako je obsah tohto dokumentu. Je ich možné využívať pri podpisovaní a šifrovaní elektronickej pošty, bezpečnom prihlasovaní sa na webové stránky poskytovateľov finančných služieb (internetbanking), bezpečné prihlasovanie sa do operačných systémov (smartcard logon), prihlasovanie sa do súkromných sietí (VPN) ap.

Čo dodať na záver?

Jednoducho si musíme uvedomiť, že materiálny svet ukladania informácií sa dynamicky mení na elektronický a je potrebné sa s tým naučiť žiť. Nie je to nič zložité a časom zistíme, že je to jednoduché klikanie, ktoré nevyžaduje až také dokonalé počítačové znalosti ako by sa predpokladalo. Svet informačných technológií sa vyvíja a my sa vyvíjame s ním a elektronický podpis do tohto rýchlo sa vyvíjajúceho sveta jednoducho patrí. Čím skôr si to uvedomíme, tým skôr získame nenahraditeľného pomocníka.

Elektronická identifikácia

Teória identifikácie

Identifikácia je prenesene spôsob zabezpečenia, aby v riadenom prostredí mohol pracovať iba platný používateľ. Vyzerá to ako komplikovaná definícia, avšak iba na prvý pohľad.

Riadeným prostredím sa rozumie také, kde existuje nejaká riadená správa (napr. pracovisko, kde je správcom zamestnávateľ či elektronický informačný systém, kde je správcom jeho vlastník). Platný používateľ je taký, ktorý je v systéme nejakým spôsobom zaevidovaný (napr. na trhu nie je potrebné poznať všetkých zákazníkov, zatiaľ čo informácia o tom, kto sa nachádza na pracovisku, je pre zamestnávateľa dôležitá). Platným používateľom nemusí byť iba fyzická osoba, môže to byť aj právnická osoba alebo, najmä v elektronických systémoch, určité skupiny používateľov (napr. bežní používatelia a administrátori).

Potreba existencie identifikácie a jej ďalších náležitostí závisí od potrieb správcu príslušného riadeného prostredia.

Pokračujúc v definíciách, proces identifikácie, autentizácie a autorizácie je postup sprístupnenia riadeného prostredia používateľovi, pričom každý z týchto pojmov má vlastné náležitosti, aj keď sa väčšinou vykonávajú spolu.

- **Identifikácia** je proces, v ktorom sa používateľ identifikuje ako platný používateľ v danom prostredí.
  - Identifikáciu je možné vykonať napr. uvedením resp. zadaním mena, identifikačného čísla, používateľského profilu, certifikátu, špecifického identifikátora, čiarového kódu, kľúča a pod.
- **Autentifikácia/autentizácia** je proces overenia identity (totožnosti) platného používateľa, t.j. zistenie, či je identita, ktorú používateľ uviedol, naozaj pravá (napr. preukázanie občianskeho preukazu alebo znalosť PIN-u).
  - Rozlišujú sa 3 základné úrovne autentifikácie:
    - „niečo viem“ (používateľ má nejakú informáciu, napr. meno matky),
    - „niečo mám“ (napr. občiansky preukaz, „token“ ako čipovú kartu),

- „niečo som“ (napr. priradenie biometrických údajov, kombinácia s pracovnou pozíciou).

o Uvedené úrovne je možné ľubovoľne kombinovať a vrstviť (napr. viacnásobné overenie informácie a následné preukázanie sa dokladom).

- **Autorizácia** je proces pridelenia oprávnení používateľovi na základe zistenej a overenej identity (napr. vlastník nehnuteľnosti ju môže predať).

o Autorizácia je určovaná správcom na základe potrieb a možností riadeného prostredia nezávisle od činnosti používateľa.

Identifikácia a autentizácia sa v praxi nezvyknú oddeľovať (typicky meno a heslo), aj keď vecne predstavujú odlišné procesy.

Fyzické prostredie vs elektronické prostredie

Fyzické a elektronické prostredia sa z pohľadu identifikácie odlišujú.

Charakteristiky fyzického prostredia:

- väčšinou existuje fyzický kontakt,
- pri identifikácii a autentizácii bez kontaktu (napr. telefónom alebo papierovou poštou) sa zvykne overovať určitá znalosť,
- možnosť narušenia (predstieranie falošnej identity) je relatívne jednorazová.

Charakteristiky elektronického prostredia:

- principiálne je vždy bez fyzického kontaktu (voči systému),
- narušenie môže byť automatizované a teda vykonávané s veľmi vysokou frekvenciou v krátkom čase.

Charakteristiky kombinovaného prostredia:

- Kombinuje vlastnosti oboch prostredí, potlačenie nevýhod a využitie výhod závisí od konkrétneho zavedenia.

Kombinované prostredie je v súčasnom stave informatizácie najčastejšie. Príkladom môže byť situácia, keď prihlásenie do systému vykoná fyzická osoba (sprostredkovateľ, napr. úradník na ÚGKK SR) po fyzickej identifikácii a autorizácii používateľa (žiadateľa o službu).

Bezpečnosť pri identifikácii

Veľmi dôležitou súčasťou identifikácie je bezpečnosť, ktorá má za cieľ minimalizovať až úplne eliminovať nevýhody jednotlivých prostredí a postupov (napr. automatizované pokusy o falošnú identifikáciu je možné potlačiť obmedzením počtu pokusov, uhádnutie spôsoby tvorby identifikátorov zase obmedzením konkrétnej odpovede systému o chybe).

Je však nutné uviesť, že nič nie je 100% bezpečné. Bezpečnosť má byť primeraná t.j. taká, aby sa útočníkovi neoplatilo ju narušiť (bezvýznamné údaje nie je potrebné chrániť tak ako tie kritické). Nemala by však byť ani zbytočne prehnaná.

Elektronická identifikácia (eID)

Venujúc sa ďalej iba elektronickému prostrediu, identifikáciu v ňom je možné koncepčne riešiť podľa niekoľkých základných kritérií:

Jedným z kritérií je rozmer využitia (rozmer prostredia resp. oblasti použitia):

- Používateľ je rozoznávaný v 1 systéme – lokálne využitie (napr. účtovníctvo, webový on-line obchod).
- Používateľ je rozoznávaný vo viacerých homogénnych systémoch – lokálne (napr. rôzne systémy pobočky jednej firmy) alebo regionálne využitie (napr. systémy inštitúcií obce či štátu, všetkých firemných pobočiek).
- Používateľ je vo viacerých nehomogénnych systémoch a prostrediach - regionálne alebo globálne využitie (napr. systémy sesterských firiem, spoločné portály, systémy viacerých štátov).

Ďalším kritériom je spôsob správy a tvorby identifikátorov:

- Centralizovaný - unifikovaný(é) identifikátor(y) (napr. jeden, dva párové).
- Decentralizovaný - každý systém má vlastný identifikátor, môžu existovať tzv. „párovacie tabuľky“, ktoré priraďujú identifikátory v jednom systéme identifikátorom v druhom systéme.
- Kombinovaný – napr. každý systém (sektor) má vlastný identifikátor, ale tento sa vypočítava z centrálneho identifikátora.

Pohľad do zahraničia nám hovorí, že stratégie a modely identifikácie sa zásadne rôznia. Niektoré štáty stratégiu pre národný eID iba vyvíjajú, iné sú už v štádiách revízie zavedeného eID. Niektoré

štáty majú kombinovaný model eID (napr. Rakúsko), iné majú iba jeden eID pre výlučné použitie voči úradom (napr. národné sociálne číslo vo Veľkej Británii), ďalšie zase majú síce jeden eID, ale jeho použitie je otvorené až do úrovne voľnej tvorby aplikácií (napr. Belgicko) a ďalšie zase akceptujú aj identifikátory tretích strán (napr. eID banky pre použitie vo verejnom sektore Švédska). Princíp jediného počiatočného prihlásenia pre všetky úkony (tzv. „single-sign-on“) napr. v Holandsku podporujú iba pre verejnú správu, v Dánsku a Portugalsku zvažujú s výhľadom pre súkromný sektor a v Nemecku je úplne zakázaný.

Na Slovensku je situácia v oblasti identifikácie právnických osôb jednoduchá – súčasné IČO vyhovuje využitiu aj v elektronickej prostredí. Identifikácia fyzických osôb je naopak výrazne zložitejšia, nakoľko rodné číslo z viacerých dôvodov nevyhovuje – obsahuje osobné údaje, existujú duplicity a najmä je úplne všade (tzv. synergický efekt), takže v elektronickom prostredí by jeden „klik“ mohol znamenať získanie všetkých informácií o konkrétnej osobe, čo by kriminálne živly vedeli veľmi jednoducho zneužiť.

V rámci informatizácie spoločnosti sa pripravuje nový model, ktorý vychádza ako z projektu Operačného programu informatizácia spoločnosti, tak z legislatívneho nastavenia prostredníctvom nového zákona o elektronizácii administratívnych procesov. Model je vo fáze finálnych diskusií, isté však je, že rodné číslo nebude identifikátorom v prostredí tzv. elektronickej verejnej správy Slovenska.

Ako je vidieť, v rámci Európskej únie existuje relatívne úplný chaos prijatých riešení. Oficiálnu elektronickú úradnú komunikáciu je však potrebné vyriešiť aj cezhranične. Európska únia sa preto tejto problematiku intenzívne venuje už niekoľko rokov.

Ako dôležité je potrebné uviesť najmä strategický dokument „eID Interoperabilita pre PEGS: Návrh pre mechanizmus multiúrovňovej autentizácie“ z decembra 2007 (www.ec.europa.eu/idabc/en/document/6484.html) a projekt STORK z roku 2009, ktorý vytvoril platformu pre interoperabilitu európskych eID, kde pri cezhraničných použitiach národných identifikátorov nezávisí na národných riešeniach - dôležité je rozhranie a správna identifikácia potrebných údajov na vstupno-výstupnom systéme. Od roku 2012 sa chystá pokračovanie projektu pod názvom STORK II, viac o oboch projektoch je možné nájsť na adrese www.eid-stork.eu.

eID v súkromnom sektore

Elektronickú identifikáciu v súkromnom sektore je potrebné vidieť v dvoch rovinách - v internom prostredí (vnútro firemné voči zamestnancom, správcom systémov ap.) a externom prostredí (obchodné voči zákazníkom, partnerom ap.). Potreby oboch prostredí sú väčšinou odlišné.

Viazať sa na zatiaľ neexistujúce riešenie štátu nie je vhodné - zosúladenie má svoje výhody, ale pozastaviť kvôli nemu všetku činnosť je kontraproduktívne.

EID V INTERNOM PROSTREDÍ

Firma alebo podnikateľ by mali zvážiť potrebu úrovní bezpečnosti, bezpečnostnej politiky a príslušných opatrení. Najmä malé a stredné podniky väčšinou spravujú rozsiahle a relatívne nekomplikované informačné systémy, preto si dokážu určiť aj relatívne jednoduché pravidlá (meno a heslo interne stačí, role v systéme stačí deliť na administrátorov a používateľov ap.). Pri ich tvorbe je možné vychádzať z medzinárodných noriem (napr. ISO 27001), tieto sú však veľmi často komplikované a finančne náročné. Rovnako je možné použiť napr. bezpečnostné štandardy z výnosu MF SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy, ktoré určujú jednoduchšie rámce alebo si nechať poradiť od bezpečnostného odborníka (je však vhodné overiť si jeho referencie), či sa spoľahnúť na dodané riešenie.

To však neznamená, že by mali byť laxné - nejasná správa eID môže byť spomaľujúca pre celý výkon organizácie (vyčerpávajúca zdroje a čas) a najmä nebezpečná - únik citlivých informácií z vnútorného prostredia môže byť ničivý, rovnako ako zneužitie informačno-komunikačných technológií firmy na vykonanie trestného činu (hackerského útoku, falošnej identifikácie ap.).

Vlastní zamestnanci sú väčšinou považovaní za dôveryhodné prostredie, paradoxne však väčšinu bezpečnostných incidentov spôsobujú práve oni (podľa niektorých štatistík až okolo 70 %). Je preto dobré riadiť sa známym heslom „dôveruj, ale preveruj".

EID V EXTERNOM PROSTREDÍ

Externé prostredie treba chápať ako a priori nepriateľské, t.j. každý jeho klient je potenciálny útočník. Zatiaľ čo jednoduché fórum alebo on-line zákaznícka poradňa sa musí pri identifikácii chrániť nanajvýš pred spamom, pri on-line obchodných transakciách už je potrebné mať istotu, že zákazník naozaj zaplatil resp. zaplatí alebo, že tovar či služba mu boli doručené resp. poskytnuté.

V prípade nákupných portálov býva väčšinou zodpovednosť na zákazníkovi, ale pozor na dobré meno. Jeho strata môže byť omnoho ničivejšia ako jednorazová finančná strata (viď. napr. „nebezpečnosť" Facebook-u vs bezpečnosti Ebay-u či Amazon-u. V našom prostredí je možné vidieť rôzne riešenia napr. Martinus, Alza, Hej, Mall ap.). Rovnako nepríjemné môžu byť prípadné súdne spory z dôvodu poškodenia zákazníka, zneužitia jeho klientskeho profilu či kreditnej karty atď.

Pri technologických nastaveniach elektronickej identifikácie je možné vychádzať z rôznych noriem, zaužívané sú napr. štandardy SAML 2.0, používanie párových kľúčov, smart kariet a podobne.

Úrovne autentizácie je možné nastaviť od najjednoduchšieho mena a hesla cez grid karty, jednorazové heslá, sms potvrdenia až po biometriku a zaručené certifikáty.

Autorizácia vychádza výlučne z potrieb organizácie, väčšinou je jedna spoločná skupina klientov postačujúca, rovnako ako aj jedna skupina systémových administrátorov.

Pri administrátoroch je však potrebné uvažovať napr. o tom, či sú tiež z externého prostredia (napr. dodávatelia) a potom zvážiť, či by mali mať možnosť vidieť alebo meniť vlastné údaje systému (napr. údaje o klientoch, transakciách atď.). Väčšinou je to úplne nevhodné. Politika ochrany prístupu už však nie je predmetom tohto dokumentu.

Pri tvorbe riešenia je dobré zvážiť aj obchodnú politiku integrácie s vládnymi či bankovými riešeniami (napr. mestská karta, rôzne priame platobné služby bánk).

Záver

Čo dodať na záver? Nastavenie alebo nenastavenie elektronickej identifikácie závisí od potrieb konkrétnej organizácie, rovnako aj úroveň jej bezpečnosti a rôzne súvisiace náležitosti. Dôležité je zvážiť najmä na čo má vlastne dlhodobo či krátkodobo slúžiť a podľa toho nastaviť všetko potrebné.

ELEKTRONICKÝ **PODPIS** A ELEKTRONICKÁ **IDENTIFIKÁCIA**

Národná agentúra pre rozvoj
malého a stredného podnikania
Enterprise Europe Network
02/ 50 24 45 00
nadsme@een.sk
www.nadsme.sk

www.enterprise-europe-network.sk

Tento leták bol vydaný Národnou agentúrou pre rozvoj malého a stredného podnikania (NARMSP) v rámci projektu Participácia slovenských MSP na tvorbe európskej legislatívy, spolufinancovaného Európskou komisiou. Slúži na všeobecnú orientáciu slovenských malých a stredných podnikateľov v téme elektronický podpis a elektronická identifikácia. Obsah tohto letáku nepredstavuje názor ani stanovisko Európskej komisie alebo NARMSP.