Vyhotovovanie elektronických podpisov na diaľku

Ľuboš Batěk, Jaroslav Imrich
Disig a.s.
Záhradnícka 151, 821 08 Bratislava
e-mail: lubos.batek@disig.sk, jaroslav.imrich@disig.sk

Abstrakt

Rozmach mobilných platforiem predstavuje pre svet kvalifikovaného elektronického podpisu výzvu, pretože väčšina z nich nedisponuje tradičnými hardvérovými ani softvérovými rozhraniami pre prácu s kryptografickým hardvérom aký predstavujú čipové karty. Nariadenie eIDAS však do praxe zavádza pojem "vyhotovovanie elektronických podpisov na diaľku", za ktorým sa môže skrývať pre koncového používateľa technicky nenáročné a zároveň ekonomicky výhodné riešenie použiteľné na všetkých mobilných ale aj desktopových platformách. V príspevku sú definované hlavné technické, bezpečnostné ale aj ekonomické rozdiely medzi tradičnými decentralizovanými riešeniami a riešeniami pre centralizovanú správu kľúčového materiálu, ktoré môžu byť použité pre vyhotovovanie elektronických podpisov na diaľku.

1. Elektronický podpis

Používanie elektronického podpisu upravuje na európskej úrovni "Nariadenie Európskeho parlamentu a Rady č. 910/2014 z 23. júla 2014" (ďalej len nariadenie eIDAS v príslušnom gramatickom tvare), ktoré definuje tri typy elektronického podpisu a síce „elektronický podpis“, „zdokonalený elektronický podpis“ a „kvalifikovaný elektronický podpis“ [1].

Prvé dva typy, elektronický podpis a zdokonalený elektronický podpis, sú v podstate technologicky neutrálne, a teda zahŕňajú napríklad aj biometrický podpis alebo bežne používaný elektronický podpis založený na certifikáte verejného kľúča, vyhotovovaný bez použitia bezpečného zariadenia. Týmto dvom typom podpisov nariadenie eIDAS nepriznáva právny účinok rovnocenný s vlastnoručným podpisom.

Naopak tretí typ, kvalifikovaný elektronický podpis, má v zmysle nariadenia eIDAS právny účinok rovnocenný s vlastnoručným podpisom a predstavuje len elektronický podpis založený na kvalifikovanom certifikáte verejného kľúča vyhotovovaný pomocou bezpečného zariadenia.

Technológia elektronického podpisu na báze asymetrickej kryptografie s využitím certifikátu verejného kľúča tak vďaka nariadeniu eIDAS získava akýsi špeciálny význam, pretože je ako jediná použiteľná na vyhotovovanie všetkých troch typov podpisov. Ďalší text bude venovaný výlučne tejto technológii.

1.1 Elektronický podpis na báze asymetrickej kryptografie

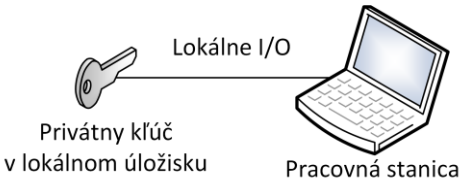
Elektronický podpis na báze asymetrickej kryptografie vo všeobecnosti predpokladá existenciu kľúčového páru zloženého zo súkromnej časti (tzv. privátny kľúč) a verejnej časti (tzv. verejný kľúč).

Verejný kľúč je používaný na overenie podpisu a v praxi je zvyčajne neobmedzene distribuovaný tretím stranám.

Privátny kľúč je používaný na vytvorenie podpisu a musí byť prístupný výlučne iba svojmu vlastníkovi. Pokiaľ by bol dostupný aj inej entite, nebolo by možné rozlíšiť podpisy tejto entity od podpisov reálneho vlastníka kľúča. Privátny kľúč je preto nutné chrániť a je potrebné zamedziť vytváraniu jeho kópií.

2. Lokálne podpisovanie

Pri lokálnom podpisovaní sa používajú softvérové alebo hardvérové úložiská privátneho kľúča prístupné priamo systému vyhotovujúcemu podpis.



2.1 Softvérové úložisko kľúčov

V najjednoduchších scenároch môže byť privátny kľúč uložený v softvérovom úložisku. Typickým predstaviteľom tohto typu úložiska je súbor vo formáte PKCS#12 alebo softvérové úložisko kľúčov operačného systému.

Softvérové úložiská sa na jednej strane veľmi ľahko používajú, no na druhej strane útočníkovi umožňujú vytvoriť kópiu privátneho kľúča spôsobom, ktorý vo väčšine prípadov nie je detekovateľný – skopírovaním súboru alebo sady súborov.

Softvérové úložiská síce môžu byť chránené symetrickou šifrou, no po vytvorení kópie úložiska je naň možné takmer neobmedzene aplikovať útoky hrubou silou, prípadne na systéme obete nasadiť špecializovanú aplikáciu na zaznamenávanie používateľskej aktivity, ktorá môže heslo pre prístup k úložisku odchytiť v momente jeho zadávania používateľom.

Napriek uvedeným bezpečnostným nevýhodám však majú softvérové úložiská značnú výhodu v podobe jednoduchej použiteľnosti na mobilných platformách, kde mobilná aplikácia jednoducho načíta privátny kľúč zo súboru a podpis zostaví softvérovou implementáciou podpisového algoritmu.

2.2 Hardvérové úložisko kľúčov

Kvôli uvedeným bezpečnostným obmedzeniam softvérových úložísk sa privátne kľúče zvyknú presúvať na špecializované bezpečné zariadenia, ktoré predstavujú nezávislý počítač s vlastným operačným systémom a vlastnými bezpečnostnými nastaveniami. Typickým predstaviteľom takéhoto bezpečného zariadenia je napríklad kryptografická čipová karta.

Používateľ sa voči bezpečnému zariadeniu autentizuje napríklad zadaním PIN kódu a podpisová aplikácia ho následne požiada o vytvorenie podpisu pomocou privátneho kľúča, ktorý je perzistovaný priamo v pamäti zariadenia.

Väčšina zariadení neumožňuje vytvoriť kópiu kľúča nedetekovateľným spôsobom a obsahuje aj mechanizmy zabraňujúce útokom hrubou silou na autentizačný proces. Najznámejší mechanizmus tohto typu predstavuje zablokovanie karty po viacerých zadaniach nesprávneho PIN kódu.

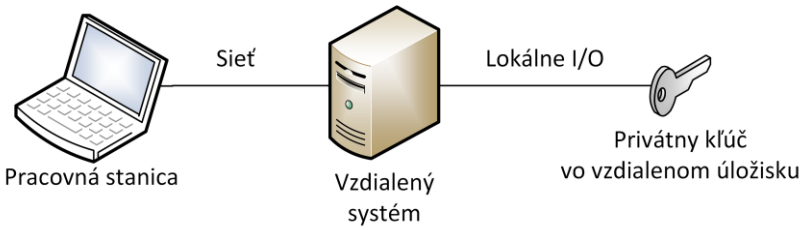
Útokom so špecializovanou aplikáciou na zaznamenávanie používateľskej aktivity sa možno brániť napríklad použitím čítačky so zabudovanou klávesnicou na zadávanie PIN kódu, ktorá odovzdá PIN kód karte bez toho, aby mal k nemu prístup

hostiteľský systém. Toto riešenie sa však v praxi kvôli výrazne vyššej cene používa skôr zriedkavo.

Jednoznačné bezpečnostné výhody hardvérových úložísk sú však bohužiaľ sprevádzané obmedzenou použiteľnosťou na mobilných platformách, na ktorých vo väčšine prípadov chýbajú hardvérové (napr. USB port) a / alebo aj softvérovým rozhrania (napr. PC/SC subsystém operačného systému) potrebné na prácu s týmito úložiskami.

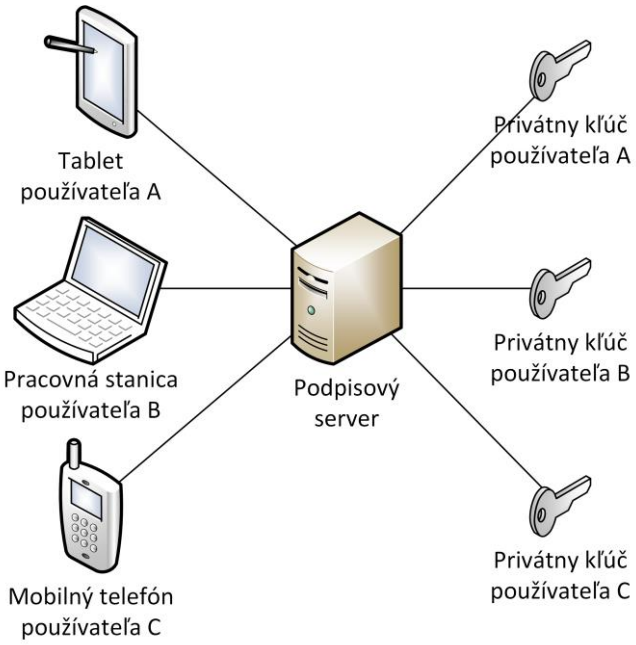
2. Podpisovanie na diaľku

Základná idea podpisovania na diaľku je jednoduchá - spočíva v presunutí kľúčov na vzdialený dôveryhodný server a jeho sprístupnení cez sieť pomocou API, ktoré je jednoducho použiteľné na väčšine známych platforiem.



Tento koncept má potenciál poskytovať obdobnú mieru bezpečnosti ako bežné hardvérové úložiská využívané pri lokálnom podpisovaní, no zároveň dokáže používateľa oslobodiť od nutnosti takéto zariadenie vlastniť a mať ho pripojené k systému, na ktorom podpisuje.

Jednoduchým rozšírením modelu je navyše možné vytvoriť viacpoužívateľský systém, ktorý umožňuje koncovým používateľom využívať privátne kľúče uložené v centrálne spravovanom bezpečnom zariadení.



S vyhotovovaním kvalifikovaného elektronického podpisu na diaľku počíta aj nariadenie eIDAS, kde sa v ods. 51 uvádza:

„Podpisovateľ by mal mať možnosť zveriť kvalifikované zariadenia na vyhotovenie elektronického podpisu do starostlivosti tretej strany za predpokladu, že sa zavedú vhodné mechanizmy a postupy, ktorými sa zabezpečí, že podpisovateľ bude mať výlučnú kontrolu nad používaním svojich údajov na vyhotovenie elektronického podpisu a že pri používaní zariadenia budú splnené požiadavky na kvalifikovaný elektronický podpis.“ [1]

Nariadenie eIDAS zároveň predpokladá, že prevádzkovateľ systému na podpisovanie na diaľku musí spĺňať rovnaké požiadavky ako poskytovatelia dôveryhodných služieb.

3. Štandardy upravujúce podpisovanie na diaľku

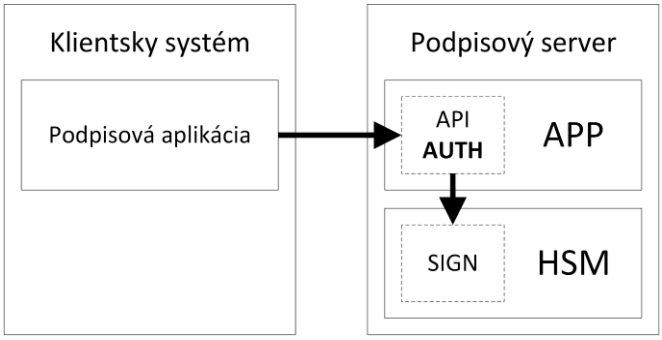
Pri návrhu systémov pre podpisovanie na diaľku sa zohľadňujú bezpečnostné opatrenia definované štandardom CEN/TS 419241:2014 [2] (ďalej len štandard v príslušnom gramatickom tvare) a dopĺňajú sa o ďalšie požiadavky v zmysle normy ISO/IEC 15408, ktorá predstavuje medzinárodné uznávaný základ pre posudzovanie bezpečnosti informačných systémov.

V zmysle článku 26 nariadenia eIDAS musí byť zdokonalený a kvalifikovaný elektronický podpis vyhotovovaný pomocou privátneho kľúča, ktorý môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou.

Štandard definuje dve úrovne výlučnej kontroly, ktorú môže systém pre podpisovanie na diaľku poskytovať používateľovi.

3.1 Výlučná kontrola úrovne 1

Nasledujúci diagram znázorňuje typické rozloženie komponentov v systéme, ktorý v zmysle štandardu poskytuje podpisovateľovi výlučnú kontrolu úrovne 1.



Autentizácia používateľa (AUTH) je v tomto prípade vykonávaná softvérovými komponentami na strane servera (APP), ktoré sú samostatne autentizované voči bezpečnému zariadeniu (HSM), na ktorom prebieha vyhotovovanie podpisu (SIGN).

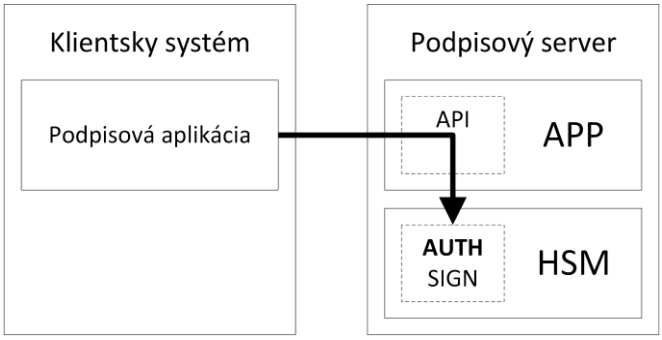
V tomto modeli sa teda vzdialený používateľ autentizuje voči serverovému softvéru a serverový softvér sa samostatne autentizuje voči bezpečnému zariadeniu. Bezpečné zariadenie nemá informáciu o tom, ktorý používateľ ktorým kľúčom podpisuje a nemôže vykonávať autorizáciu operácie v kontexte vzdialený používateľ verzus použitý privátny kľúč.

Pri tejto úrovni výlučnej kontroly je úlohou softvérových komponentov na strane servera zabezpečiť, že na vyhotovovanie podpisu konkrétnym používateľom bude použitý správny privátny kľúč. Narušenie činnosti týchto komponentov môže mať za následok neoprávnené použitie privátneho kľúča.

Výlučnú kontrolu úrovne 1 poskytuje väčšina dostupných serverových produktov pre vzdialené podpisovanie. Samotný štandard však nepredpokladá, že by takýto systém bol schopný naplniť požiadavky kladené na SSCD zariadenie použiteľné pre kvalifikovaný elektronický podpis.

3.2 Výlučná kontrola úrovne 2

Nasledujúci diagram znázorňuje typické rozloženie komponentov v systéme, ktorý v zmysle štandardu poskytuje podpisovateľovi výlučnú kontrolu úrovne 2.



Autentizácia používateľa (AUTH) je v tomto prípade vykonávaná priamo bezpečným zariadením (HSM), na ktorom prebieha vyhotovovanie podpisu (SIGN). Autentizácia používateľa môže byť samozrejme vykonávaná aj softvérovými komponentami na strane servera (APP), a štandard počíta s tým, že pri použití viacfaktorovej autentizácie bude jeden faktor overovaný softvérovými komponentami servera a druhý faktor overovaný bezpečným zariadením.

V tomto modeli sa teda využíva end-to-end autentizácia medzi používateľom a bezpečným zariadením na strane servera, ktoré vďaka tomu dokáže vykonávať autorizáciu operácie v kontexte vzdialený používateľ verzus použitý privátny kľúč.

Štandard predpokladá, že systém poskytujúci výlučnú kontrolu úrovne 2 by mal byť schopný naplniť požiadavky kladené na SSCD zariadenie použiteľné pre kvalifikovaný elektronický podpis. Implementácia takéhoto systému je však oveľa náročnejšia, pretože vyžaduje, aby v bezpečnom zariadení na strane servera boli vykonávané algoritmy, ktoré tieto zariadenia štandardne nepodporujú.

4. Výhody a nevýhody podpisovania na diaľku

4.1 Technické výhody

V súčasnosti snáď najčastejšie uvádzanou výhodou systémov pre vyhotovovanie elektronických podpisov na diaľku je fakt, že sú ľahko použiteľné na mobilných platformách.

Nemenej významnou výhodou je však aj možnosť integrácie so systémami certifikačných autorít. Výsledkom takejto integrácie môže byť vysoká miera automatizácie správy certifikátov. Technicky menej zdatní používatelia systému pre podpisovanie na diaľku v podstate nemusia o existencii certifikátu vedieť a už vôbec sa nemusia zaoberať jeho exspiráciou. Ak to typ certifikátu a politiky certifikačnej autority umožňujú, systém môže automaticky vygenerovať nový kľúčový pár a zabezpečiť vydanie nového certifikátu. Bežný používateľ tak môže výhody PKI infraštruktúry využívať a nemusí sa do jej prevádzky nijako zapájať.

Systémy pre vyhotovovanie elektronických podpisov na diaľku môžu byť vhodným riešením aj pre organizácie, ktoré potrebujú podpisovať dokumenty kvalifikovanou elektronickou pečaťou, no ich biznis procesy vyžadujú, aby privátny kľúč prislúchajúci ku kvalifikovanému certifikátu pre elektronickú pečať mohlo používať viacero zamestnancov súčasne. Pre správne navrhnuté centralizované úložisko kľúčového materiálu by bezpečné zdieľanie kľúčov viacerými používateľmi nemalo predstavovať zásadný prevádzkový ani bezpečnostný problém.

Centralizované úložiská kľúčov však poskytujú množstvo výhod nielen pri podpisovaní ale aj pri ďalších kryptografických operáciách. Ako celkom bežný príklad môže poslúžiť šifrovanie e-mailových správ. Používateľ má na svojej čipovej karte uložený privátny kľúč slúžiaci na dešifrovanie správ. Tento kľúč sa spolu s certifikátom zhruba po roku zvyknú nahrádzať novými, no na dešifrovanie starších správ používateľ potrebuje mať k dispozícii aj staršie kľúče. Po pár rokoch môže byť používateľ konfrontovaný s obmedzenou kapacitou čipovej karty, na ktorú sa mu nové kľúče už nezmestia. Problém navyše môže nastať aj pri strate alebo poškodení karty. Ak neexistuje záloha šifrovacích kľúčov, používateľ sa k obsahu svojich správ s veľkou pravdepodobnosťou už nedostane. Centralizované úložiská riešia oba uvedené problémy, pretože ponúkajú prakticky neobmedzenú úložnú kapacitu a všetky v nich uložené kľúče môžu byť bezpečne a centrálne zálohované.

4.2 Bezpečnostné výhody

Systémy pre vzdialené podpisovanie vo väčšine prípadov môžu byť nezávislé od technológie používanej na autentizáciu koncových používateľov. Vďaka tomu ich je možné integrovať do firemných prostredí s využitím už zavedených autentizačných mechanizmov alebo v prípade potreby môže byť menej bezpečný mechanizmus používaný takýmto systémom nahradený bezpečnejším. Centrálna správa autentizačných mechanizmov a používateľov navyše umožňuje definovať a efektívne vynucovať rôzne druhy bezpečnostných politík (silu hesla, počet faktorov atď.).

Na rozdiel od väčšiny bežne dostupných čipových kariet sú centralizované úložiská schopné vytvárať dôveryhodné auditné záznamy o všetkých operáciách vykonávaných s kľúčmi. Výhody tejto schopnosti sa naplno prejavujú pri zdieľaných kľúčoch, ktoré používajú viaceré osoby, napríklad na vyhotovovanie elektronickej pečate organizácie alebo na podpisovanie softvéru vydávaného organizáciou (angl. code signing). Pri lokálnom podpisovaní sme neraz svedkami toho, že si kvôli uľahčeniu práce viaceré osoby medzi sebou požičiavajú jednu čipovú kartu a poznajú jej PIN kódy. Pri takomto postupe je prakticky nemožné dokázať, ktorá z nich vytvorila ktorý podpis. Pri vzdialenom podpisovaní zdieľaným kľúčom môže centralizované úložisko zaznamenať nielen podpisovaný hash, ale aj identitu používateľa, ktorý ho podpísal. Zároveň umožňuje kedykoľvek zrušiť alebo udeliť prístup ďalším osobám.

4.3 Ekonomické výhody

Z ekonomického pohľadu je najvýraznejšou výhodou riešení pre podpisovanie na diaľku jednoznačne minimalizácia nákladov na nákup bezpečných zariadení pre koncových používateľov a tiež eliminácia nákladov spojených so správou týchto zariadení a s ich prvotnou distribúciou od vydavateľa k používateľom.

4.4 Nevýhody

Na rozdiel od lokálneho podpisovania, podpisovanie na diaľku nemôže prebiehať v off-line režime. Podpisová aplikácia bežiaca na zariadení koncového používateľa musí byť schopná nadviazať sieťové spojenie so vzdialeným serverom, na ktorom je uložený privátny kľúč. Toto obmedzenie však predstavuje zásadný problém iba v minimálnom počte prípadov.

Nezanedbateľnú nevýhodu systémov pre podpisovanie na diaľku však môže predstavovať fakt, že konzervatívnejší používatelia ich považujú za nebezpečné a odmietajú akceptovať skutočnosť, že pojem „výlučná kontrola“ v zmysle nariadenia eIDAS nemusí nutne predstavovať kontrolu fyzickú. Z ich úst zaznieva otázka, prečo by mali veriť prevádzkovateľovi služby pre podpisovanie na diaľku, že naozaj dokáže ochrániť ním spravované privátne kľúče. Málokedy si ale položia aj analogickú otázku, prečo by mali veriť výrobcovi čipovej karty, že karta naozaj dokáže ochrániť v nej uložené privátne kľúče. V konečnom dôsledku sú obidva prístupy založené na rovnakom princípe - dôvere. V prípade čipovej karty si používateľ vyberá výrobcu, ktorému dôveruje, že jeho výrobok je bezpečný a v prípade podpisovania na diaľku si vyberá poskytovateľa služby, ktorému dôveruje, že ním poskytovaná služba je bezpečná.

Resumé

Snaha používať na mobilných platformách tradičné bezpečné zariadenia dlhodobo neprináša pozitívne výsledky. Používateľ je väčšinou zaťažovaný množstvom čítačiek a redukcií s najrôznejšími konektormi, alebo musí používať ďalšie externé zariadenie komunikujúce pomocou technológie bluetooth, ktoré je oveľa väčšie a potrebuje dobíjať batérie.

Systémy pre vyhotovovanie elektronických podpisov na diaľku majú potenciál poskytovať obdobnú mieru bezpečnosti ako tradičné bezpečné zariadenia a nevyžadujú k zariadeniu koncového používateľa pripájať žiadny nový hardvér. Možno konštatovať, že doposiaľ boli v „legislatívnom vákuu“, no nariadenie eIDAS jednoznačne očakáva nárast ich rozšírenia.

Ak systém pre vyhotovovanie elektronických podpisov na diaľku dokáže splniť náročné bezpečnostné požiadavky štandardu CEN/TS 419241:2014 a je schopný koncovému používateľovi poskytnúť výlučnú kontrolu úrovne 2, môže byť používaný nielen na vyhotovovanie zdokonaleného elektronického podpisu ale aj na vyhotovovanie kvalifikovaného elektronického podpisu.

Literatúra

[1] NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES. Dostupné na: <http://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32014R0910>

[2] CEN/TS 419241:2014 - Security Requirements for Trustworthy Systems Supporting Server Signing