Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Elektronický podpis v informačných systémoch Univerzity Komenského

Bakalárska práca

2018
Lukáš Kiss

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Elektronický podpis v informačných systémoch Univerzity Komenského

Bakalárska práca

Študijný program:	Informatika
Študijný odbor:	2508 Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	doc. RNDr. Daniel Olejár, PhD.
Konzultant:	Mgr. Peter Kopáč

Bratislava, 2018
Lukáš Kiss

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Lukáš Kiss
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Elektronický podpis v informačných systémoch Univerzity Komenského
Electronic signature in information systems of Comenius University

Anotácia: Analyzovať možnosti využívania elektronického podpisu v existujúcich informačných systémoch Univerzity Komenského, navrhnúť a implementovať/ integrovať riešenia na vytváranie a overovanie elektronických podpisov pomocou občianskych preukazov do systémov UK. V súvislosti s odhalenými slabinami OP analyzovať bezpečnosť navrhovaného riešenia a dôsledky zmien kľúčov, algoritmov v občianskych preukazoch pre navrhované riešenie.

Kľúčové slová: elektronický podpis, e-gov, informačné systémy UK

Vedúci: doc. RNDr. Daniel Olejár, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Dátum zadania: 21.11.2017

Dátum schválenia: 10.01.2018 doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie: Týmto by som chcel poďakovať všetkým, čo mi pomohli pri riešení bakalárskej práce, hlavne svojmu vedúcemu **doc. RNDr. Danielovi Olejárovi, PhD.**, ktorý ma uviedol do problematiky a viedol ma počas celej bakalárskej práce. Za ochotu a ústretovosť ďakujem **Mgr. Peterovi Kopáčovi**, ktorý mi pomohol pri návrhu a programovaní demo riešenia. Nakoniec by som chcel poďakovať **Mgr. Matejovi Zagibovi**, ktorý mi pohol pri ladení a hľadaní chýb v demo riešení.

Abstrakt

Táto bakalárska práca sa zaoberá využitím občianskeho preukazu s čipom na autentifikáciu a vytváranie elektronického podpisu a popisuje návrh skladajúci sa z webového rozšírenia a lokálnej aplikácie. V prvej časti popisuje ich komunikáciu cez post požiadavky a následne opisuje demo verziu tohto návrhu, ktorá dokáže vytvoriť elektronický podpis, získať certifikát a overiť elektronický podpis pomocou certifikátu. Kvôli interakcii mnoho modulov, v predposlednej kapitole táto práca popisuje automatickú inštaláciu demo riešenia. Pri jej možnom zlyhaní, vysvetľuje aj manuálnu inštaláciu ako pod OS Windows, tak aj pod OS Linux. V poslednej časti sa práca venuje skúmaniu možných vylepšení demo riešenia a analyzuje aj jeho bezpečnosť.

Kľúčové slová: elektronický podpis, občiansky preukaz s čipom, webové rozšírenie

Abstract

This bachelor thesis deals with the use of a citizen card with an electronic chip and the creation of an electronic signature and describes a proposal consisting of web extension and local application. In the first part, it describes their communication via POST requests and then describes a demo version of this design that can create an electronic signature, obtain a certificate and verify the electronic signature with a certificate. Due to the interaction of many modules, in the penultimate chapter this work describes the automatic installation of a demo solution. In its possible failure, it explains the manual installation both under Windows and under Linux. In the last part, the work is devoted to examining the possible improvements of the demo solution and analyzes its security.

Keywords: electronic signature, citizen ID with eletronic chip, web extension

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Elektronizácia administratívnych úkonov má priniesť väčšiu efektivitu, rýchlosť spracovania a vyššiu bezpečnosť vykonávania jednotlivých úkonov. Túto problematiku má každý štát v Európskej únii upravenú podľa seba, preto Európsky parlament vydal nariadenie eIDAS (electronic IDentification, Authentication and trust Services), ktoré má zjednotiť túto legislatívu vo všeobecnej miere. Toto nariadenie je množinou nariadení pre elektronickú identifikáciu a dôveryhodných služieb pre elektronické transakcie na európskom vnútornom trhu, z ktorého vyplývajú povinnosti aj pre našu krajinu, ako napríklad vytvoriť národný identifikačný systém.

V spojitosti na toto nariadenie od Európskeho parlamentu, Slovenská národná rada vydala zákon o e-Govermente. Tento zákon vedie k modernizácii verejnej správy. Jedným zo znakov modernizácie sú občianske preukazy s elektronickým čipom. Tento čip obsahuje identifikačné údaje a údaje na vytvorenie elektronického podpisu, na základe ktorých sa občan dokáže autentifikovať do verejnej správy alebo elektronicky podpísať dokument. Do verejnej správy patria aj univerzity, preto sa v našej bakalárskej práci budeme zaoberať využitím občianskeho preukazu s čipom v univerzitných systémoch.

Navrhneme systém, pomocou ktorého sa bude možné autentifikovať do univerzitného systému alebo ho využiť pre dvojfaktorovú autentifikáciu, čo prinesie vyššiu bezpečnosť a ľahšiu komunikáciu s univerzitnými systémami. Navyše, náš návrh by mal byť schopný vytvárať elektronický podpis, ktorý využijeme či už pri podpisovaní dokumentov alebo emailov.

Analýzou požiadaviek dospejeme k zisteniu, že najlepším návrhom by mohlo byť webové rozšírenie, ktoré by dokázalo interagovať nie len s užívateľom ale aj s webovou stránkou alebo dokonca so serverom.

Na autentifikovanie a vytvorenie elektronického podpisu sa využíva kryptografické funkcie a vyžadujú sa bezpečnostné požiadavky od týchto funkcii. Prvá kapitola bude zaoberať základmi informačnej bezpečnosti. Popíšeme základné bezpečnostné požiadavky a nazrieme do kryptológie a kryptosystémov.

V následnej kapitole popíšeme, aký je rozdiel medzi elektronickým a digitálnym podpisom a pozrieme sa, aké požiadavky kladie zákon na elektronický podpis a ako sa implementuje digitálny podpis pomocou asymetrického kryptosystému.

Tretia kapitola bude zahŕňať popis občianskeho preukazu, čo sa pod tým rozumie

a aké údaje obsahuje. Niektoré občianske preukazy obsahujú elektronický čip, ktorý je nutný pre elektronickú komunikáciu s verejnou správou. Aj tento čip popíšeme v tejto kapitole.

V štvrtej kapitole navrhneme riešenie a popíšeme, na aké problémy môžeme naraziť pri navrhovaní riešenia. Porovnáme aj jednotlivé riešenia a povieme si, prečo niektoré nebudú fungovať alebo sú na implementáciu nevhodné. Pozrieme sa aj na knižnice, ktoré nám umožnia abstrahovať od jednotlivých malých problémov a sústrediť sa iba na vývoj.

Piata kapitola bude obsahovať postup manuálnej inštalácie a odinštalácie lokálnej aplikácie a webového rozšírenia. Opíšeme, ako treba s aplikáciou pracovať, čo umožňuje a ako overiť jej správnu funkčnosť.

V poslednej kapitole sa pozrieme na možné vylepšenia našej demo aplikácie a jej nevýhody. Popíšeme, čo všetko by aplikácia mohla ešte podporovať. Na konci kapitoly by sme sa pokúsili analyzovať bezpečnosť nášho riešenia a bezpečnostné chyby, ktoré by sa mohli dať odstrániť alebo len čiastočne opraviť.

Kapitola 1

Informačná bezpečnosť

V tejto kapitole si definujeme základné bezpečnostné požiadavky a uvedieme základy kryptológie, ktoré budeme potrebovať na pochopenie nášho riešenia.

Terminológia informačnej bezpečnosti ešte nie je ustalená, a preto uvedieme základné pojmy, s ktorými budeme pracovať v celej bakalárskej práci. Pre čitateľov, ktorý majú väčší záujem o túto problematiku, odporúčame knihy [7] alebo [6].

1.1 Bezpečnostné požiadavky

Pri analýze bezpečnostného systému budeme zohľadňovať základné bezpečnostné požiadavky, ktoré sú:

1. **Dôvernosť** - základný bezpečnostný atribút alebo základná požiadavka na ochranu informácie. Zaistenie dôvernosti informácie znamená, že informácia nie je prezradená/odhalená neoprávneným entitám alebo procesom. Na zaistenie dôvernosti sa používajú tak metódy riadenia prístupu k údajom, ako aj šifrovanie.

2. **Integrita** - v úzkom zmysle sa integrita chápe ako ochrana proti neoprávnenej modifikácii alebo zničeniu údajov.

3. **Autentickosť** - vlastnosť vyjadrujúca, že identita entity je tá, ktorá bola deklarovaná.

4. **Nepopretie pôvodu** - bezpečnostná funkcia, pri použití ktorej má príjemca údajov záruku správnosti proklamovanej identity odosielateľa týchto údajov, ktorý vďaka tomu nemôže poprieť, že údaje vytvoril (poslal).

5. **Autentifikácia** - bezpečnostná funkcia, ktorá identifikuje identitu a následne ju aj overí.

6. **Autorizácia** - oprávnenie využívať definované služby chráneného systému, resp. pristupovať definovaným spôsobom k chráneným informáciám.

1.2 Základy kryptológie

Viaceré bezpečnostné funkcie, ktorými sa zapodievame v tejto bakalárskej práci, sú postavené na kryptografických funkciách, preto sa v tejto časti pozrieme na základy kryptológie. Definujeme kryptosystém a typy kryptosystémov, PKI, certifikát a certifikačná autorita.

Kryptológia sa delí na dve časti:

- na **kryptografiu**, ktorá sa zameriava na návrh a skúmanie kryptografických systémov,
- na **kryptoanalýzu**, ktorá sa zameriava na hľadanie slabín v kryptografických systémov a ich využitie.

Kryptografia aj kryptoanalýza sú nutné na navrhnutie dobrého kryptosystému.

1.2.1 Kryptosystémy

Už od minulosti chceli ľudia skrývať informácie pred nepriateľmi alebo len pred svojimi konkurentmi. Tieto dôvody utajovania pretrvávajú do súčasnosti a stimulujú vznik mnohých kryptosystémov. Pod pojmom **kryptosystémom** rozumieme dvojicu kryptografických transformácii (E, D), kde E je šifrovacia transformácia (funkcia, ktorá prevedie vstup do zašifrovanej podoby) a D je dešifrovacia transformácia (funkcia, ktorá dešifruje vstup).[5].

Kryptosystémy je možné rozdeliť podľa viacerých kritérií. V práci ich budeme deliť na symetrické a asymetrické. Pri ich vysvetľovaní využijeme entity Alica a Boba a Evy, ktorá chce do komunikácie medzi Alicou a Bobom zasiahnuť.

Symetrický kryptosystém

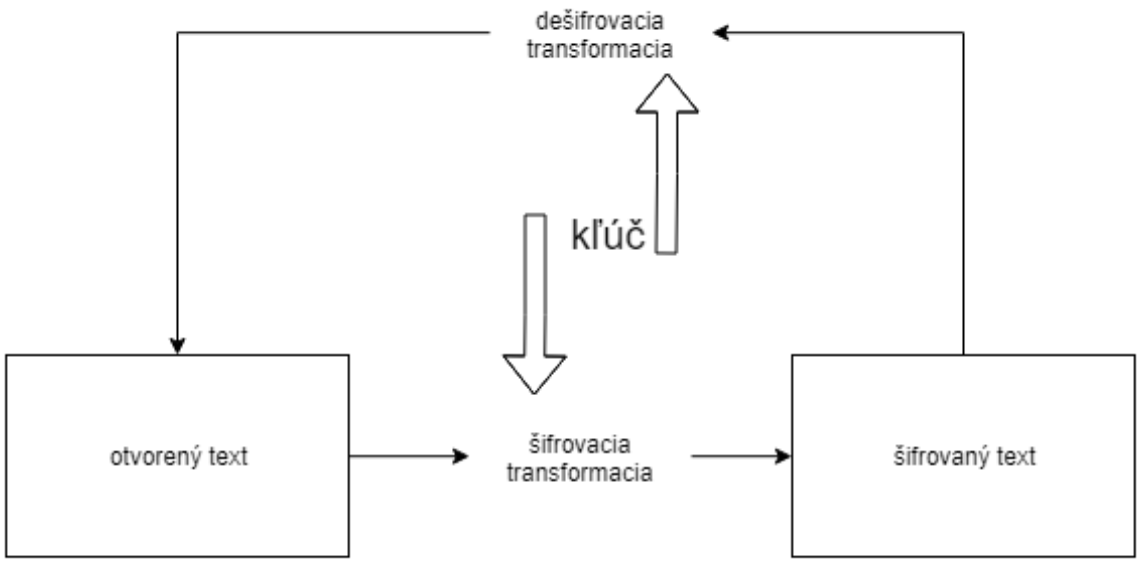
Symetrický kryptosystém je charakterizovaný tým, že šifrovacia a dešifrovacia transformácia zdieľa ten istý kryptografický kľuč, ktorý sa nazýva aj tajný kľuč, pretože ho používajúce entity musia utajiť.

Na obrázku 1.1 je vidieť, že dešifrovacia transformácia je inverzná funkcia k šifrovacej transformácii práve vtedy, keď sa použije rovnaký kľúč v obidvoch transformáciách.

Základnou bezpečnostnou požiadavkou je sila kľúča, ktorá hlavne závisí od jeho dĺžky. Ak dĺžka kľúča je príliš malá, útočník môže prezrieť celý priestor možných kľúčov a týmto spôsobom nájsť správny kľúč na dešifrovanie. Z tohto dôvodu sa v dnešnej dobe používajú dĺžky kľúčov aspoň veľkosti 128 bitov. Pri použití takejto dĺžky[1] je pre utočníka neefektívne[2] použiť útok hrubou silou.

[1] Ak bol kľúč vygenerovaný náhodným spôsobom

[2] Pomer vynaloženého úsilia na získanie informácie a ceny informácie je veľmi malý.



Obr. 1.1: Šifrovanie a dešifrovanie pomocou symetrického kryptosystému

Pozrieme sa, ako prebieha komunikácia medzi Alicou a Bobom, keď Eva chce zistiť informácie, ktoré si posielajú. Alica a Bob chcú chrániť obsah svojej komunikácie pomocou symetrického kryptosystému. Najprv sa musia nejakým spôsobom dohodnúť na kľúči[3], ktorý budú využívať pri šifrovaní a dešifrovaní. Urobia tak pomocou iného kanálu, ktorý nemôže Eva odpočúvať. Dôvernosť komunikácie spočíva na utajení kľúča. Ak Eva správne uhádne alebo zistí kľúč, ktorý používa Alica a Bob na komunikáciu, vie nielen dešifrovať nasledujúcu a predošlú komunikáciu, ale aj vytvárať falošné správy.

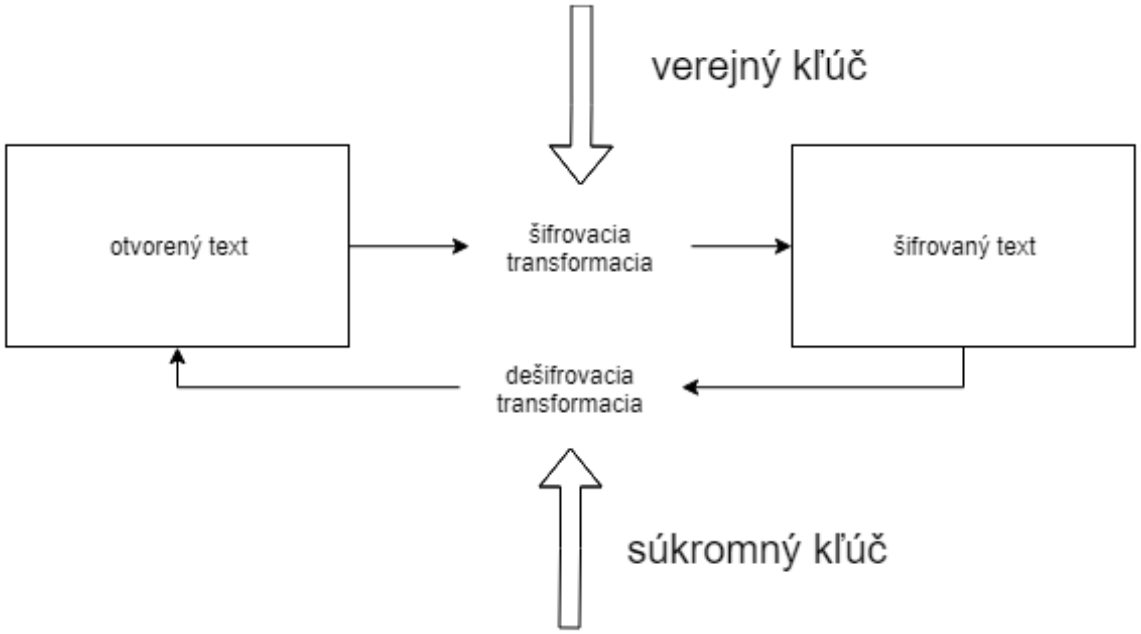
Hlavnou výhodou symetrického kryptosystému je rýchlosť šifrovania dát a nasledovného dešifrovania. Vo viacerých zariadených sú jednotlivé šifry hardwarovo implementované kvôli ich jednoduchosti. Známe sú AES, DES, GOST.

Nevýhodou symetrického kryptosystému je zdieľanie kľúča, ktorý si musia entity nejako bezpečne odovzdať. Distribúcia kľúčov v prípade veľkom počtu používateľov je zložitá a ťažko sa efektívne realizuje. Tento problém rieši práve asymetrická kryptografia.

Asymetrický kryptosystém

Narozdiel od symetrického kryptosystému, ktorý využíva jeden kryptografický (tajný) kľúč, asymetrický kryptosystém používa dva rôzne kryptografické kľúče, z ktorých jeden slúži na šifrovanie a druhý na dešifrovanie dát. Asymetrický kryptosystém je postavený na riešení ťažkých matematických problémov[4], ktorých parametrami sú kryptografické kľúče, ktoré sa z jeden druhého nedajú odvodiť. To umožňuje jeden z kľúčov zverejniť (verejný kľúč) a tento kľúč pozná každý na sieti, na rozdiel od druhého, tzv.

[3]Napríklad ho Bob odovzdá Alici uzatvorenej obálke.
[4]diskrétny logaritmus, faktorizácia prvočísel



Obr. 1.2: Šifrovanie pomocou verejného kľúča a následné dešifrovanie pomocou súkromného kľúča

súkromného kľúča, ktorý si entita uchováva v tajnosti.

Hlavnou výhodou asymetrického kryptosystému je, že Alica a Bob nepotrebujú zabezpečený kanál na výmenu verejných kľúčov. Aby Eva nemohla Bobovi podvrhnúť svoj verejný kľúč a vydávať ho za Alicin, tak na distribúciu verejných kľúčov sa využije riešenie typu PKI (viď 1.3) alebo PGP[5].

Aj keď principiálne máme vyriešený problém distribúcie verejných kľúčov (pomocou PKI alebo PGP), pri implementácii treba vyriešiť aj iné (možnosť útoku so znalosťou otvoreného textu).

Známe asymetrické šifry sú RSA-PKCS1v1.5 alebo ElGamal.

1.2.2 Hashovacia funkcia

Zohráva dôležitú úlohu pri zachovaní integrity a autentickosti dokumentu. **Hashovacia funkcia** je funkcia, ktorá na základe vstupu (bitového vektora) vypočíta tzv. hashovaciu hodnotu (hashword). Argumenty, ktoré spracováva hashovacia funkcia nemávajú spravidla rovnakú dĺžku. Výsledné hashovacie hodnoty sú slová rovnakej dĺžky, spravidla podstatne kratšej ako sú vstupné hodnoty. Vďaka tomu nie je hashovacia funkcia injektívna, t.j. existuje viacero vstupných hodnôt, ktorým je priradená tá istá hashovacia hodnota. Príkladom hashovacej funkcie je zobrazenie, ktoré (textovému) súboru priradí 1 byte, získaný ako suma mod 2 všetkých bytov vstupného súboru. Hashovanie sa využíva pri vytváraní usporiadaných dátových štruktúr a na ochranu integrity

[5] https://sk.wikipedia.org/wiki/Pretty_Good_Privacy

údajov.

V kryptografických konštrukciách sa využívajú tzv. kryptograficky silné hashovacie funkcie, ktoré musia spĺňať nasledujúce požiadavky[4]:

- Sú deterministické, tá istá správa vedie k rovnakému hashu.
- Je možné rýchlo vypočítať hash pre každú danú správu.
- Nie je môžné vygenerovať správu z ich hash hodnoty inak ako skúšaním všetkých možností.
- Malá zmena správy by mala zmeniť každý bit výstupu hashovacích funkcií s pravdepodobnosťou 1/2.
- Je nemožné nájsť dve rôzne správy s rovnakou hodnotou hash.

1.3 PKI (Infraštruktúra verejného kľúča)

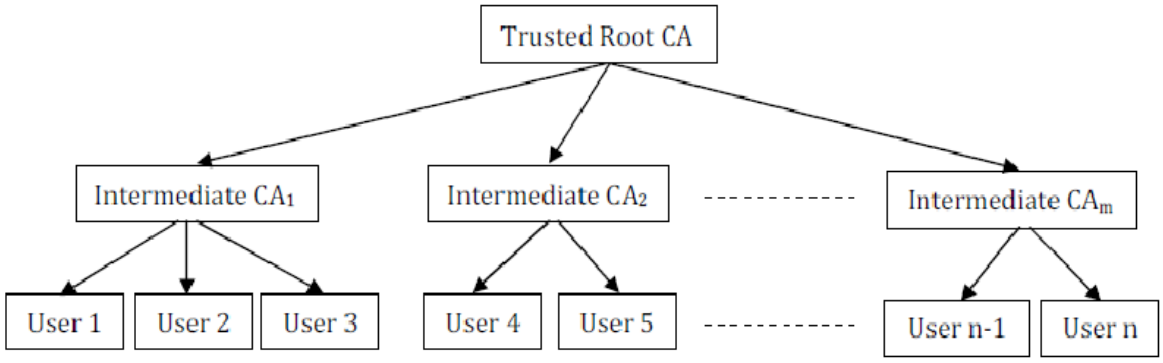
PKI je infraštruktúra verejného kľúča pozostávajúca z certifikačnýách autorít a iných poskytovateľov certifikačných služieb, ktorého úlohou je napomáhať používaniu digitálnych podpisov založených na certifikátoch verejného kľúča (kvôli stručnosti budeme „certifikát verejného kľúča“ označovať pojmom „certifikát“).

Na spojenie identity človeka a verejného kľúča slúži **certifikát**, ktorý je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje (vo väčšine prípadov certifikačná autorita), že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný [2, §6 odsek 1]. Respektíve je to elektronický dokument, ktorý definuje vlastníctvo verejného kľúča právnickej alebo fyzickej osobe. Pre identifikáciu osoby pomocou certifikátu sa nachádzajú v certifikáte identifikačné údaje vydavateľa ako aj držiteľa certifikátu. Certifikát vydáva používateľovi certifikačná autorita.

Certifikačná autorita je poskytovateľ certifikačných služieb, ktorá spravuje certifikáty a vykonáva certifikačnú činnosť [2, §12 odsek 1]. Inak povedané, je to subjekt, ktorý vydáva, spravuje certifikáty a poskytuje certifikačné služby a svojou autoritou potvrdzuje pravosť certifikátov. Na zaistenie autentickosti dát na certifikáte sa využíva digitálny podpis. Na zabezpečenie autentickosti dát na certifikáte slúži digitálny/elektronický podpis (viď kapitola 2) certifikačnej autority.

V našom prípade z asymetrického kryptosystému (viď. asymetrický kryptosystém 1.2.1) by Alica poslala Bobovi svoj certifikát podpísaný certifikačnou autoritou a certifikát certifikačnej autority, ktorým bol Alicin certifikát podpísaný. Ak Eva sa pokúsi nahradiť poslané certifikáty svojimi[6], tak Bob tento podvod rýchlo odhalí, pretože Bob

[6]Eva si vytvorí oba certifikáty a k nim patričné kľúče. Následne jedným súkromným kľúčom podpíše druhý certifikát.



Obr. 1.3: Znázornenie hierarchickej štruktúry PKI, kde na vrchu stromu sa nachádza koreňová certifikačná autorita
(zdroj: https://www.researchgate.net/figure/M-PKI-hierarchical-model_fig4_263526947)

môže mať certifikát certifikačnej autority od iného zdroja, môže ísť na webovú stránku certifikačnej autority, ktorej dôveruje.

Autorít môže existovať viacero a Bob nemusí o všetkých vedieť. Ako má teda Bob dôverovať aj tým certifikačným autoritám, ktoré nepozná? Tento problém rieši **koreňová certifikačná autorita**, ktorá vydáva certifikáty iba certifikačným autoritám. Nasledovne tieto certifikačné autority vydávajú certifikáty ostatným. Takto Bobovi stačí dôverovať iba koreňovým certifikačným autoritám a následne pomocou predávanie dôvery[7] Bob môže dôverovať aj iným certifikačným autoritám, ktorým daná koreňová certifikačná autorita vydala certifikát. Bob takto môže dôverovať aj preňho neznámym certifikačným autoritám.

Pomocou koreňových certifikačných autorít, certifikačných autorít a entity[8] vytvoríme hierarchický model (viď obr. 1.3), kde na vrchu sa nachádza koreňová certifikačná autorita.

Alica má teraz dostupnú metódu ako poslať Bobovi svoj verejný kľúč. PKI Bobovi overiť, že verejný kľúč, ktorý prijal, naozaj patrí Alici. Alica pošle svoj certifikát a celú reťaz certifikátov[9] Bobovi. Bob nasledovne overí všetky certifikáty až ku koreňovej certifikačnej autorite. Až potom Bob môže veriť tomu, že verejný kľúč (nachádzajúci sa v certifikáte, ktorý patrí Alici), ktorý dostal, naozaj patrí Alici. Rovnakým spôsobom bude prebiehať poslanie a overenie Bobového verejného kľúča.

[7]Koreňová certifikačná autorita vydá certifikačnej autorite certifikát. Ak Bob dôveroval koreňovej certifikačnej autorite, tak potom dôveruje aj certifikačnej autorite, ktorej koreňová certifikačná autorita certifikát vydala.

[8]Myslíme osobu alebo inštitúciu, ktorému alebo ktorej bol vydaný certifikát.

[9]Reťaz certifikátov (certificate chain) sú certifikáty od entity až po koreňovú autoritu pospájanú pomocou digitálneho podpisu. Na overenie certifikátu využijeme verejný kľuč z certifikátu o úroveň vyššie.

Zrušenie certifikátov

Certifikačná autorita vydáva certifikáty s určitou dobou platnosti. Platnosť certifikátov môže okamžite zrušiť (pridať do zoznamu zrušených certifikátov). Certifikačná autorita môže zrušiť certifikát z nasledovných dôvodov:

- Stratenie patričného súkromného kľúča danému certifikátu. Entita môže stratiť súkromný kľuč, a preto kvôli bezpečnosti by už nemal daný certifikát platiť (pozn. mohol by ho nájsť niekto neautorizovaný na prácu s tým súkromným kľúčom).
- Ukradnutie kľúča. V tomto prípade môže aj neautorizovaná osoba dešifrovať alebo vytvárať elektronické podpisy, preto sa daný certifikát ihneď pridá do zoznamu zrušených certifikátov.
- Zmena údajov. Entita sa môže rozhodnúť zmeniť svoje identifikačné údaje, čo spôsobí, že certifikačná autorita vydá nový certifikát a zruší platnosť predchádzajúceho certifikátu.
- Z verejného kľúča sa dá hrubou silou nájsť jemu prislúchajúci súkromný kľuč. Tento problém má viacero asymetrických šifier, ale čas, ktorý je potrebný na úspešný útok hrubou silou je obrovský (viac ako 50 000 rokov). Preto existuje obmedzená platnosť certifikátu, ktorá je rádovo menšia (pár rokov).

Podnet na zrušenie certifikátu môže dať úrad, držiteľ certifikátu alebo certifikačná autorita.

Pri overovaní certifikátu musí Alica aj Bob overiť, či prijatému certifikátu neskončila platnosť alebo sa nenachádza v zozname zrušených certifikátov. Tento test platnosti musia spraviť pre každý certifikát z príslušnej reťaze certifikátov vrátane koreňovej certifikačnej autority.

1.4 Zhrnutie

V tejto kapitole sme uviedli základy informačnej bezpečnosti a kryptológie, na ktorých budeme stavať v celej našej bakalárskej práce. Hlavne sa budeme opierať o asymetrické šifrovanie a kryptografické hashovacie funkcie, pomocou ktorých zavedieme digitálny podpis.

Kapitola 2

Podpis v elektronickej forme

Človek už od oddávna dával súhlas svojím slovom, neskôr po vynájdení písma sa súhlas s textom začal vyjadrovať pomocou jedinečného identifikačné znaku nazývaného podpis. Tento prostriedok súhlasu sa používa dodnes. Po rozvinutí elektronického sveta sa ľudstvo snažilo preniesť tento prostriedok súhlasu aj do elektronickej formy a nazýva sa elektronický podpis.

Často sa stáva, že pojmy elektronický podpis a digitálny popis sú nesprávne zamieňané. Elektronický podpis je legislatívny koncept, na rozdiel od digitálneho podpisu, čo je bezpečnostná technológia na vytvorenie elektronického podpisu. Elektronický podpis má byť nezávislý od technológie, ktorá bola použitá na vytvorenie tohto podpisu.

2.1 Elektronický podpis

Ako už vieme, podpis v elektronickej forme sa nazýva elektronický podpis, čo je legislatívny koncept. Aby podpis mal podobné vlastnosti ako vlastnoručný podpis, sú naňho kladené isté bezpečnostné požiadavky zákonom [2, §3 odsek 1.] , ktorý znie:

1. 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.
2. Podpisovateľ vyhotoví elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a elektronického dokumentu vyhotoví nový údaj, ktorý spĺňa podmienky podľa odseku 1.

Stále však nenahrádza vlastnoručný podpis overený notárom, pretože nespĺňa niektoré požiadavky, ako napr. non repudiation of origin (nepopierateľnosť pôvodu), autor môže

tvrdiť, že on ten podpis nevytvoril. Preto vznikol nový typ elektronického podpisu **KEP**.

KEP je skratka pre kvalifikovaný elektronický podpis, ktorý zmenil názov zo **ZEP** (zaručeného elektronického podpisu). Rozdiel medzi **EP** (elektronický podpis) a **KEP** je, že na vytvorenie **KEP** sú kladené vyššie bezpečnostné požiadavky, pomocou ktorých vie **KEP** zabezpečiť aj zvyšné bezpečnostné požiadavky ako autenticita alebo nepopierateľnosť. Vďaka týmto vlastnostiam dokáže nahradiť vlastnoručný podpis overený notárom v elektronickom svete.

2.2 Digitálny podpis

V úvode sme spomenuli, že digitálny podpis je technológia na vytvorenie elektronického podpisu. Táto technológia využíva jednotlivé kryptografické funkcie na dosiahnutie jednotlivých požiadaviek, ktoré sa opisujú už v spomínanom zákone, (viď Elektronický podpis). Na splnenie požiadaviek zákona [2, §3 odsek 1. písm. (a) a písm. (b)] sa využíva konštrukcia založená na asymetrickom šifrovaní a kryptografickej hashovacej funkcii (viď základy kryptológie 1.2). Na splnenie poslednej požiadavky zákona [2, §3 odsek 1. písm. (c)] použijeme certifikát verejného kľúča, ktorý držiteľovi vydala certifikačná autorita.

Teraz sa pozrieme na to, ako pomocou kryptografickej hashovacej funkcii, asymetrického šifrovania a PKI vytvoríme a overíme elektronický podpis. Overenie a vytvorenie sa robí automatizovane pomocou hardvérových zariadení alebo softwarových aplikácií.

2.2.1 Vytvorenie digitálneho podpisu

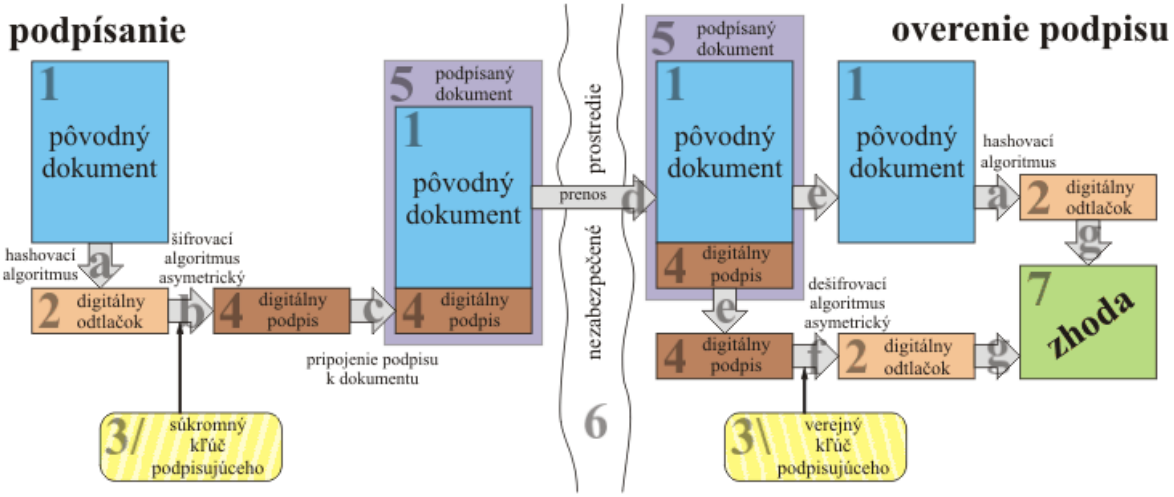
Teraz popíšeme algoritmus, ktorý daná aplikácia používa na vytvorenia digitálneho podpisu z pohľadu Boba.

1. Bob zoberie dokument Doc, ktorý chce podpísať. Následne vytvorí hash H_{Doc} toho dokumentu použitím kryptografickej hashovacej funkcii H.

2. Bob zoberie svoj súkromný kľúč $K_{Bob,privat}$[1] (k tomuto súkromnému kľúču existuje aj verejný Bobov kľúč $K_{Bob,public}$) a pomocou šifrovacej funkcie E vytvorí z hashu digitálny podpis $P_B(Doc) = E(H_{Doc}, K_{Bob,privat})$.

3. Nakoniec Bob priloží podpis $P_B(Doc)$ k dokumentu Doc.

[1] K tomuto súkromnému kľúču musí existovať párový verejný $K_{Bob,public}$, ktorý sa nachádza na certifikáte. Tento certifikát je podpísaný certifikačnou autoritou a deklaruje, že ten verejný kľúč $K_{Bob,public}$ patrí Bobovi.



Obr. 2.1: Na obrázku môžeme vidieť podpísanie elektronického dokumentu a následné overenia daného podpisu
(zdroj: http://epodpis.tuke.sk/digit_podpis.html)

2.2.2 Overenie digitálneho podpisu

Ak nejaká entita potrebuje overiť podpis daného dokumentu. Použije overovací proces. Tento proces si popíšeme z pohľadu Alice.

1. Alica extrahuje verejný kľúč $K_{Bob,public}$ z Bobovho certifikátu.
2. Pomocou verejného kľúča $K_{Bob,public}$ a pomocou dešifrovacej funkcie D Alica dešifruje Bobov podpis P a získa hash H_b.
3. V ďalšom kroku Alica z dokumentu Doc, ktorý Bob podpísal, vypočíta hash H_a.
4. Nakoniec Alica porovná hasha H_a a H_b. Ak sa hashe rovnajú, tak podpis P je správny , inak podpis P nepatrí patričnému dokumentu Doc alebo daný podpis nevytvoril Bob.

2.3 Zhrnutie

V tejto kapitole sme popísali a vysvetlili, čo je to elektronicky a digitálny podpis, aký je rozdiel medzi elektronickým a kvalifikovaným podpisom. Uviedli sme, ako sa vytvára digitálny/ elektronický podpis.

Kapitola 3

Občiansky preukaz

V tejto časti práce popíšeme elektronický preukaz s čipom, uvedieme aké objekty na ňom nachádzajú a ako sa dá použiť v elektronickom svete.

Občiansky preukaz je verejná listina, ktorá slúži na preukázanie totožnosti a štátneho občianstva. Túto verejnú listinu musí mať každý občan, ktorý dovŕšil pätnásty rok veku a má trvalý pobyt na území Slovenskej republiky [3, §2]. To znamená, že každý človek by mohol mať občiansky preukaz s čipom[1], čo by umožňovalo využiť ho na autentifikáciu do univerzitného systému alebo iných systémov, v ktorých sa bude naše riešenie využívať.

Ako už vieme, každý občan nad 15 rokov musí mať občiansky preukaz. Tento občiansky preukaz obsahuje základné údaje o tejto osobe, ako sú meno, priezvisko, rodné priezvisko, pohlavie, štátne občianstvo, dátum a miesto narodenia, rodné číslo a adresa trvalého pobytu občana a elektronický čip [3, §3 odsek 1.].

My sa hlavne zameriame na elektronický čip, ktorý nám umožní preniesť tieto údaje do elektronického sveta.

3.1 Elektronický čip

Pozrieme sa, aké údaje obsahuje elektronický čip na občianskom preukaze. Zákon Slovenskej Republiky umožňuje mať na elektronickom čipe tieto údaje, ktoré možno zapísať do občianskeho preukazu podľa § 3 ods. 1 až 3 a možno zapísať ďalšie údaje v rozsahu a za podmienok ustanovených osobitným predpisom [3, §4]. V našom prípade sa hlavne budeme zaoberať predpisom, zákonom č. 215/2002 o elektronickom podpise, ktorý hovorí o ďalších údajoch, ktoré sa tam môžu zapísať. Tieto údaje môžu byť certifikáty, verejné alebo súkromné kľúče.

Po dlhodobom experimentovaní s elektronickým čipom, sme zistili, že elektronický

[1]Tu môže nastať problém, keď človek môže mať občiansky preukaz s čipom (cudzinci môžu použiť namiesto občianskeho preukazu s čipom eDoPP, o ktorý môže požiadať každý cudzinec s povolením na pobyt na Slovensku), ale nemusí mať vygenerované certifikáty a súkromné kľúče.

Obr. 3.1: Občiansky preukaz s čipom
(zdroj: http://www.b-1.sk/eid-obciansky-preukaz-s-cipom/)

čip obsahuje kryptografické tokeny[2]. Pretože občiansky preukaz obsahuje kryptografické tokeny, tak na prístup k informáciám vyžaduje bezpečnostné požiadavky. Jenda z bezpečnostných požiadavok je zadanie BOK kódu alebo ZEP kódu, ktoré slúžia ako autentifikačný prostriedok. Po zadaní príslušného kódu sme mohli pomocou čítačky a programu pristupovať k jednotlivým údajom použitím Cryptoki API (viď PKCS#11). Občiansky preukaz s čipom obsahuje tieto tokeny:

- Token, ktorý uchováva súkromný kľuč na vytvorenie KEP (viď elektronický podpis 2.1), na ktorého použitie potrebujeme ešte zadať ZEP kód a kvalifikovaný certifikát (odkaz na zákon o kvalifikovanom certifikáte) obsahujúci informácie o držiteľovi občianskeho preukazu a verejný kľuč na overenie KEP podpisu. Aby KEP bol platný, musí byť vyhotovený na bezpečnostnom zariadení podľa zákona [2, §4].

- Na druhom tokene sa nachádzajú dva certifikáty a k nim patričné súkromné kľúče, ktoré sú rozlíšiteľné (tie dva súkromné kľúče) pomocou ID. Z tých dvoch certifikátov, jeden slúži na overovanie elektronického podpisu a jemu patričný kľuč na vytváranie toho podpisu. Druhý certifikát slúži na šifrovanie a jeho patričný kľuč na dešifrovane. Odhadujeme, že tento certifikát sa používa aj so súkromným kľúčom prevažne pri autentifikácii do verejnej správy. Nepodarilo sa nám to, žiaľ, zistiť pre nedostatoku času a pomalej odozvy od štátnych orgánov.

Zaujímavosťou je, že na prístup k certifikátom uložených na týchto tokenoch musíme tiež zadať BOK kód.

Na komunikáciu s kryptografickými tokenmi sa využíva štandard PKCS#11.

PKCS#11 je štandard, ktorý špecifikuje API rozhranie, nazývané **Cryptoki** pre zariadenia, ktoré uchovávajú kryptografické informácie a vykonávajú na nich krypto-

[2]Sú fyzické zariadenia, ktoré sa používajú na uchovávajú kryptografické údaje.

grafické operácie. **Cryptoki** nasleduje[3] jednoduchý objektovo postavený návrh, kde adresuje nezávislosť technológii a zdieľanie zdrojov (viacero aplikácii pristupuje k viacerým zariadeniam) a prezentuje bežný logický pohľad na zariadenia nazývané **kryptografický token** (cryptographic token) [1].

3.2 Zhrnutie

V tejto kapitole sme si popísali občiansky preukaz a elektronický čip. Elektronický čip sa skladá z kryptografických tokenov. Aby sme mohli pristupovať k jednotlivým údajom, sme pred prístupom museli zadať prístupvoý BOK kód.

V budúcnosti sa očakáva, že každý občan nad 15 rokov bude vlastniť občiansky preukaz s elektronickým čipom, čo nám umožní ho využívať na autentifikáciu do elektronických systémov alebo podpisovať elektronické dokumenty.

[3]Pod týmto myslíme, že je narvhnutý týmto spôsobom