Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Elektronické doklady o vzdelaní na Univerzite Komenského

Bakalárska práca

2017
Zuzana Hromcová

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Elektronické doklady o vzdelaní na Univerzite Komenského

Bakalárska práca

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

Bratislava, 2017
Zuzana Hromcová

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Zuzana Hromcová
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: Elektronické doklady o vzdelaní na Univerzite Komenského
Electronic documents on education at Comenius University

Cieľ: 1. preskúmať požiadavky, ktoré na UK vyplývajú zo Zákona o e-Governmente (s dôrazom na identifikáciu a autentifikáciu entít v Integrovanom informačnom a komunikačnom systéme IIKS UK, úradnú komunikáciu medzi UK a študentmi, UK a ostatnými orgánmi verejnej moci);
2. analyzovať procesy v oblasti študijnej agendy UK, ktoré spadajú do výkonu verejnej moci a zistiť, ako by ich bolo možné elektronizovať tak, aby UK splnila povinnosti vyplývajúce zo zákona,
3. pre vybranú oblasť (napr. vydávanie dokladov o vzdelaní, overovanie ich platnosti, vydávanie kópií, duálnych dokumentov v listinnej a elektronickej forme) navrhnúť, implementovať a dokumentovať modelové riešenie.

Anotácia:

Kľúčové slová: vzdelanie,e-Government, elektronické dokumenty, Univerzita Komenského

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

Dátum zadania: 07.11.2016

Dátum schválenia: 07.11.2016 doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie:

Táto bakalárska práca sa zaoberá problematikou, ktorá v sebe okrem informatiky skrýva aj prvky z oblasti práva, manažmentu a nemalý kus praktických problémov z reálneho života. Vzhľadom na veľký rozsah problematiky sa jej cieľ postupne vyvíjal a menil s pribúdajúcimi informáciami a skúsenosťami, preto bolo v niektorých momentoch náročné pevne uchopiť jej smer a viackrát bolo nutné predefinovať naše pôvodné zámery. Preto ďakujem svojmu školiteľovi, **doc. RNDr. Danielovi Olejárovi, PhD.**, za to, že ma voviedol do skúmanej problematiky a sprevádzal ma spleťou (často na prvý pohľad nejasných) čiastkových úloh, ktoré viedli až ku splneniu stanovených cieľov.

Dokončenie práce by však nebolo možné bez spolupráce mnohých ďalších zamestnancov Univerzity Komenského, či už v podobe zasvätenia do vnútorného chodu Univerzity v administratívnej oblasti, alebo podelenia sa o praktické skúsenosti z oblasti informatiky a informačnej bezpečnosti.

Za ochotu a ústretovosť preto ďakujem **Mgr. Ľubici Janáčkovej**, **Ing. Petrovi Juráškovi, CSc.**, **Bc. Petre Kopáčovej** a pani referentkám zo študijného oddelenia, ktorí mi pomohli preniknúť do tajov fungovania informačných systémov a organizačných procesov Univerzity, a v neposlednom rade **RNDr. Jaroslavovi Janáčkovi, PhD.**, **Mgr. Gustávovi Pálosovi** a **Mgr. Matejovi Zagibovi**, ktorí mi poskytli konzultácie k technickým aspektom mojej práce, zodpovedali množstvo praktických otázok a pomohli mi formovať moju predstavu o mojom finálnom návrhu riešenia pre skúmanú problematiku.

Abstrakt

Táto práca sa zaoberá informatizáciou procesov a činností prebiehajúcich na Univerzite Komenského v súvislosti so Zákonom o e-Governmente, ktorý upravuje činnosť Univerzity ako orgánu verejnej moci v elektronickom priestore. V prvej časti sa venuje analýze požiadaviek, ktoré pre Univerzitu Komenského vyplývajú priamo zo Zákona o e-Governmente, v druhej časti skúma možnosti implementácie tohto zákona v praxi. Autori sa podrobnejšie zameriavajú na oblasť vydávania dokladov o vzdelaní, špecificky diplomov. Práca obsahuje návrh systému na informatizáciu tejto oblasti, analýzu problematických miest a ďalších úloh, ktoré vyplynuli z implementácie modelového riešenia v simulovanom prostredí.

Kľúčové slová: vzdelanie, e-Government, elektronické dokumenty, Univerzita Komenského

Abstract

This thesis deals with informatization of agenda of Comenius University in Bratislava related to the e-Government Act which regulates operation of government and public institutions in cyberspace. The aim of this thesis is to identify the major obligations of the University implied by the Act and study possible implementations of the Act in practice. In the first part, basic terms of information security are explained and e-Government Act is analyzed. The thesis then concentrates on one particular process of University agenda - maintenance of documents on education. For this process, a concept for a solution in cyberspace is designed and implemented. In conclusion, the thesis discusses the major drawbacks and possible modifications to the proposed solution.

Keywords: education, e-Government, electronic documents, Comenius University

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Vývoj moderných informačných technológií otvára možnosti pre prenos tradičných činností do elektronického sveta. Prebiehajúca informatizácia spoločnosti zasiahla aj verejnú správu a nastolila požiadavku, aby úrady, školy a iné verejné inštitúcie riešili podnety občanov elektronicky, pretože informatizácia prináša väčšiu rýchlosť, efektivitu a v neposlednom rade aj bezpečnosť rôznych úkonov a operácií.

Pre elektronický svet však ešte nie sú právne predpisy zadefinované tak dobre ako v tom hmotnom svete. Inak sa pozerá napríklad na krádež auta oproti krádeži osobných údajov - rozdielna je úroveň prijatej legislatívy, ale aj kontroly a vymáhateľnosti práva. Preto v poslednom období Európska únia aj Slovenská republika prijímajú rôzne zákony a nariadenia, ktorými chcú upravovať správanie občanov aj verejných inštitúcií v elektronickom svete.

V súvislosti s konaním verejných inštitúcií v elektronickom svete nedávno Národná rada Slovenskej republiky prijala dôležitý Zákon o e-Governmente, ktorý upravuje výkon verejnej moci elektronicky. Tento zákon spolu s ďalšími nariadeniami EÚ a zákonmi SR predstavuje základný rámec pre komunikáciu občanov s inštitúciami elektronicky.

Zákon je však napísaný všeobecne, pre všetky orgány verejnej moci, a hoci sa týka mnohých oblastí, poskytuje málo podrobností. Nakoľko Univerzita Komenského je orgánom verejnej moci v oblasti vzdelávania, je nevyhnutné, aby si bola vedomá svojich právomocí a povinností, ktoré jej vyplývajú z tohto zákona, a aby implementovala potrebné opatrenia, aby všetky povinnosti splnila v určenom čase.

Už z prvotnej analýzy zákona vyplynulo, že jeho aplikovanie v praxi si bude vyžadovať pomerne veľký zásah do fungovania Univerzity, či už pôjde o technické alebo organizačné opatrenia. To si bude vyžadovať nielen podporu informatikov, ale aj administratívnych a vedúcich pracovníkov, preto sa Univerzita Komenského rozhodla zahájiť projekt prípravy zavádzania zákona o e-Governmente na Univerzite pod vedením doc. RNDr. Daniela Olejára, PhD., ktorého súčasťou je viacero čiastkových projektov, vrátane tejto bakalárskej práce.

V tejto práci sa venujeme analýze Zákona o e-Governmente z pohľadu Univerzity Komenského, pričom cieľom je identifikovať a popísať kľúčové požiadavky kladené na Univerzitu, rovnako ako opatrenia, ktoré bude musieť prijať. Špecificky sa zameriavame na oblasť vydávania dokladov o vzdelaní, aby sme demonštrovali rozsah zmien, ktoré

bude treba zaviesť.

Túto oblasť v práci analyzujeme a popisujeme, čo by si vyžadovalo prenesenie správy dokladov o vzdelaní do elektronického sveta. Implementujeme modelové riešenie a popisujeme problémy, ktoré sú spojené s informatizáciou vydávania diplomov.

Nakoľko do zavádzania opatrení vyplývajúcich zo Zákona o e-Gov sa budú musieť zapojiť rovnako technicky zdatní zamestnanci UK, ako aj laici, v kapitole 1 vysvetľujeme základné pojmy z informačnej bezpečnosti, na ktoré sa budeme neskôr v práci odvolávať. V tejto kapitole taktiež zjednocujeme terminológiu použitú v rôznych zákonoch týkajúcich sa informatizácie a informačnej bezpečnosti, nakoľko táto nie je ustálená a objavujú sa v nej rôzne odchýlky v interpretácii pojmov, ktoré by mohli viesť k nedorozumeniam.

V kapitole 2 sa venujeme samotnej analýze Zákona o e-Governmente. Popíšeme jeho základnú myšlienku a povinnosti, ktoré UK zo zákona priamo vyplývajú, ale aj povinnosti, ktoré si implementácia zákona vyžiada nepriamo, predovšetkým procesné a technické zmeny na Univerzite.

Pre demonštráciu, čo všetko si takáto zmena môže vyžiadať, sa v kapitole 3 zameriavame na analýzu procesov výkonu verejnej moci, ktoré bude potrebné na Univerzite Komenského elektronizovať. Obzvlášť sa venujeme vybranej oblasti výkonu verejnej moci - vydávaniu a správe dokladov o vzdelaní, špecificky diplomov.

V kapitole 4 túto oblasť analyzujeme a identifikujeme, aké roly v nej vystupujú, aké požiadavky môžu byť na Univerzitu kladené a ako je ich splnenie vyriešené v listinnom svete. Pre túto oblasť následne popisujeme návrh transformácie tohto procesu do elektronického sveta, so zachovaním rovnakých požiadaviek a bezpečnostných prvkov.

V kapitole 5 navrhneme jedno možné riešenie pre správu diplomov v elektronickom svete, a na demonštráciu hlavnej funkcionality popíšeme hlavné časti našej ukážkovej implementácie tohto riešenia.

V kapitole 6 sa zameriavame na výhody a nevýhody nami navrhnutého konceptu, problémy, s ktorými sme sa stretli pri implementovaní ukážkového riešenia a rady, odporúčania a otvorené otázky, na ktoré bude potrebné myslieť pri implementovaní a zavádzaní riešenia v reálnych podmienkach.

Kapitola 1

Základy informačnej bezpečnosti

V tejto kapitole sa budeme venovať budovaniu teoretického základu, ktorý bude nevyhnutný pre ďalšie časti práce. Text je určený nielen informaticky vzdelanému čitateľovi, ale aj laikovi, čomu je prispôsobená aj jeho náročnosť a stupeň detailu. Náročnejší čitateľ nájde viac podrobností o popisovanej problematike v knihách od Bishopa [7], Schneiera [17] a Stinsona [18].

Terminológia súvisiaca s informačnou bezpečnosťou nie je nijako koordinovaná ani ustálená, preto sa v rôznych štandardoch, zákonoch a iných zdrojoch môžu objaviť nekonzistentnosti, najmä pokiaľ ide o preklad termínov z anglického jazyka. Aby sme predišli nesprávnej interpretácii jednotlivých termínov, v nasledujúcich častiach definujeme a vysvetlíme základné pojmy informačnej bezpečnosti a najčastejšie používané pojmy v tejto práci.

1.1 Základné pojmy

Informačná bezpečnosť je súhrn procedúr a opatrení, ktorých cieľom je ochrana informácií a informačných systémov pred neautorizovaným prístupom, zneužitím, odhalením, poškodením alebo zničením [14, str. 94].

Medzi objekty, s ktorými pracujeme v informačnej bezpečnosti, patria napríklad informácie, technické zariadenia, programové vybavenie, ľudia, pravidlá, finančné prostriedky alebo vzťahy. Tieto objekty môžu mať rozličný charakter, ale všetky predstavujú tzv. *entity*. Entita je akýkoľvek objekt, ktorý sa dá odlíšiť od iných objektov toho istého typu.

Entita sa vyznačuje súborom *atribútov* (vlastností, charakteristík), ktorých hodnoty ju odlišujú od iných entít toho istého typu. Množina atribútov postačujúcich na odlíšenie entity od iných entít toho istého typu sa nazýva *identita*. Jedna entita môže mať aj viac identít, pričom identity môžu mať obmedzenú platnosť - *oblasť pôsobenia*.

Entitou môže byť napríklad banka, zamestnanec banky, bankový trezor alebo da-

tabáza klientov banky. V tejto práci sú entitami zvyčajne osoby a dokumenty. Medzi atribúty banky patrí jej obchodné meno, sídlo a identifikačné číslo, ktoré spolu jednoznačne odlišujú banku od iných entít, a tak tvoria jej identitu. Atribútmi dokumentu môže byť jeho autor, čas zhotovenia alebo jeho rozsah.

V praxi často potrebujeme jednoznačne určiť entitu, s ktorou pracujeme, napríklad preto, aby sme vedeli, či nejakej osobe alebo procesu umožníme vykonať nejakú činnosť alebo či im umožníme prístup k nejakým zdrojom. Určenie entity sa spravidla skladá z dvoch procesov - identifikácie a autentifikácie.

Identifikácia je proces, kedy entita uvedie svoju identitu. Overenie tejto identity nazývame *autentifikácia*. *Autorizácia* je proces overenia oprávnenia na vykonanie nejakej operácie. Ak entita disponuje týmto oprávnením, je na operáciu *autorizovaná*, v opačnom prípade je *neautorizovaná*.

Pre prihlásenie do databázy klientov banky sa musí zamestnanec banky najprv identifikovať - napríklad zadať svoje prihlasovacie meno, a následne autentifikovať - zadať heslo. Pokiaľ pre uvedené prihlasovacie meno a heslo existuje príslušný záznam v databáze oprávnených používateľov, zamestnanec je autorizovaný na prístup k databáze klientov.

Aktívum organizácie je každá entita, ktorú organizácia vlastní, má o nej znalosť alebo ju považuje za hodnotnú, t.j. čokoľvek, čo má pre organizáciu nejakú hodnotu. Akúkoľvek potenciálnu možnosť narušenia aktív organizácie nazveme *hrozbou*. Môže ísť o prírodný jav (blesk, zemetrasenie, záplavy), technickú poruchu, organizačný nedostatok, ľudskú chybu alebo úmyselný útok.

Hrozba má svojho *nositeľa*, je zameraná na nejaké aktívum a jej naplnenie je podmienené existenciou *zraniteľnosti*, teda okolnosti, ktorá nositeľovi umožňuje poškodiť aktívum. Zraniteľnosťou môže byť chyba, organizačný nedostatok, ale aj spôsob používania aktíva - napríklad pripojenie na Internet umožňuje naplnenie hrozby nakazenia počítača nežiaducim škodlivým softvérom stiahnutým z Internetu.

V predošlom príklade by bankový trezor a databáza klientov tvorili aktíva banky, zatiaľ čo možnosť vykradnutia trezora by bola hrozbou. Nositeľom hrozby by bol zlodej. Nemalou hrozbou by však bol aj únik informácií z databázy klientov. Citlivé informácie by mohli byť zneužité konkurenciou, čo by mohlo viesť ku kompromitácii banky, ale aj útočníkmi, ktorí by mohli informácie zneužiť na preposlanie peňazí na svoj účet, a tak by banka prišla o peniaze aj dôveru zákazníkov. Aktívami v elektronickom svete sú zvyčajne elektronické dokumenty, elektronické správy, databázy a iné informácie.

Zraniteľnosťami v tomto prípade by mohlo byť napríklad nezamknutie trezora banky alebo vyzradenie hesla do databázy klientov. V prvom prípade zraniteľnosť umožňuje naplnenie hrozby vykradnutia trezoru, v druhom prípade hrozby neautorizovaného prístupu do systému banky.

Každý pokus o naplnenie hrozby (vrátane neúspešného) nazývame *bezpečnostný incident*. Ujmu na aktíve či organizácii nazveme *dopadom hrozby*. Hlavným cieľom organizácie je chrániť jej aktíva pred hrozbami, preto prijíma *bezpečnostné opatrenia*. Všetky hrozby však pokryť nemôže, preto organizácia skúma *riziká*, v ktorých zohľadňuje nielen dopad hrozby, ale aj pravdepodobnosť toho, že sa hrozba naplní. Za *hodnotu rizika* považujeme strednú hodnotu dopadu hrozby. Organizácia prijíma také bezpečnostné opatrenia, aby riziko hrozieb znížila, odstránila, preniesla na inú entitu alebo minimalizovala jeho dosah.

Nakoľko hrozieb a zraniteľností je veľmi veľa a my potrebujeme bezpečnosť systému riešiť prakticky, cieľom informačnej bezpečnosti v praxi je naplniť nasledujúce základné *bezpečnostné požiadavky*:

- *integrita* - zabezpečenie ochrany pred neúmyselnou či úmyselnou zmenou alebo zničením informácie,
- *autentickosť* - zabezpečenie toho, že informácia nebola po vytvorení nepozorovane modifikovaná a že deklarovaný pôvodca informácie zodpovedá jej skutočnému pôvodcovi,
- *dostupnosť* - zabezpečenie spoľahlivého prístupu autorizovanej entity k informáciám,
- *dôvernosť* - obmedzenie prístupu k informáciám neautoarizovaným entitám,
- *nepopretie pôvodu* - záruka, že príjemca informácie má k dispozícii dôkaz o identite odosielateľa, a teda odosielateľ nemôže neskôr poprieť odoslanie informácie.

Bezpečnostné opatrenia, ktoré zabezpečujú tieto bezpečnostné požiadavky, zriedkakedy úplne eliminujú riziko, prípadne sú neprimerane drahé vzhľadom na jeho hodnotu. Preto sa v informačnej bezpečnosti zaoberáme nielen zavedením opatrenia, ale aj skúmaním, aké je toto opatrenie účinné. To vyjadruje úroveň záruk.

Úrovňou záruky nazveme mieru naplnenia bezpečnostnej požiadavky pre dané aktívum. Stanovujeme ju podľa ceny aktíva a hodnoty rizika. Podľa dôležitosti jednotlivých požiadaviek môžeme definovať škálu stupňov záruky od najnižších až po najvyššie. Každé aktívum môže mať iné požiadavky na stupne záruky pre rôzne bezpečnostné požiadavky, pričom málokedy je možné dosiahnuť maximálne naplnenie všetkých požiadaviek naraz.

Maximálnu dôvernosť elektronického dokumentu by sme mohli dosiahnuť napríklad jeho vymazaním - tým by sme ale dosiahli minimálnu úroveň jeho dostupnosti. Naopak, maximálnu dostupnosť by sme dosiahli zverejnením dokumentu na Internete, čím by sme ale obmedzili jeho dôvernosť.

Naplnenie bezpečnostných požiadaviek pre každé aktívum si vyžaduje najprv dôslednú analýzu, aký stupeň záruky požadujeme pre ktorú bezpečnostnú požiadavku a následne aplikovanie bezpečnostných opatrení, medzi ktoré patria organizačné, fyzické a logické opatrenia.

Pod fyzickým zabezpečením si môžeme predstaviť zamknutie dverí miestnosti, v ktorej je umiestnený počítač. Organizačným opatrením môžu byť rôzne predpisy, kontrolné mechanizmy a sankcie, napríklad požiadavka pre zamestnancov, aby si heslá ku svojim kontám menili každý mesiac. Mnohé z bezpečnostných opatrení, najmä na zaistenie integrity, autentickosti a dôvernosti informácie sa zakladajú na kryptografických riešeniach„ ktorým sa budeme venovať v nasledujúcej časti.

1.2 Základy kryptológie

Kryptológia je 4000 rokov [13] stará vedná disciplína, ktorá sa pôvodne zaoberala konštrukciou šifier (*kryptografiou*) a ich lúštením (*kryptoanalýzou*). V posledných 50 rokoch sa však jej aplikácie podstatne rozšírili, a preto výskum v kryptológii dostal systematický matematicko-informatický základ.

V tejto práci sa nebudeme zaoberať históriou kryptológie ani detailným výkladom jej základov. Historický prehľad nájde čitateľ v knihe od Kahna [13], ako úvod do kryptológie poslúžia knihy od Schneiera [17] a Stinsona [18]. V ďalších častiach len stručne prejdeme cez základné pojmy kryptológie, ktoré budeme v práci potrebovať.

Základným problémom, ktorý kryptografia rieši, je zachovanie dôvernosti informácie, ktorá je prenášaná

- v priestore - z jedného miesta na druhé nezabezpečeným kanálom, alebo
- v čase - uloženie informácie do nezaisteného úložiska a jej opätovné prečítanie v neskoršom čase.

Keďže rozdiely medzi prenosom informácie v čase a priestore nie sú z kryptografického hľadiska podstatné, v ďalšom budeme hovoriť len o prenose informácie v priestore. Navyše budeme predpokladať, že Alica odosiela správy nezabezpečeným kanálom Bobovi[1]. Ku komunikačnému kanálu má prístup Eva, ktorá môže správy čítať, ale nemôže zasahovať do komunikácie. Úlohou je zabezpečenie dôvernosti komunikácie medzi Alicou a Bobom. Na riešenie tohto problému používame šifrovanie, ktorému sa venujeme v časti 1.2.

Ďalšími úlohami kryptografie môže byť zabezpečenie autentickosti a integrity správ. Nech Alica a Bob sú dve komunikujúce entity a Mallory je tretia entita, ktorá môže komunikačný kanál nielen odpočúvať, ale môže jednotlivé správy meniť, nahrádzať a

[1] Alica a Bob sú štandardnými účastníkmi kryptografických protokolov v súvisiacej literatúre

preposielať staré správy. Úlohou kryptografie v tejto situácii je zabezpečiť, aby Mallory nemohol vystupovať ako Alica ani Bob a nemohol nepozorovane meniť obsah ich správ. Tieto úlohy plní hašovanie a digitálny podpis, ktorým sa budeme venovať v sekciách 1.2.2, resp. 1.2.3.

Kryptografia však nevie naplniť všetky požiadavky informačnej bezpečnosti, nedokáže napríklad zabezpečiť dostupnosť.

Kryptoanalýza sa zaoberá skúmaním metód, ako prelomiť jednotlivé šifry, napríklad ako prečítať utajovanú správu alebo vystupovať pod falošnou identitou. Jednou z metód kryptoanalýzy je *útok hrubou silou (brute force attack)* - vyskúšanie všetkých možností dešifrovania. Môžeme si ho predstaviť ako vyskúšanie všetkých kombinácií trezoru, čo je síce časovo náročné, ale nakoniec vedie k prelomeniu šifry (resp. otvoreniu trezora).

Úlohou kryptografie je poskytnúť na ochranu správ také prostriedky (šifry), ktoré sú dostatočne bezpečné a použiteľné z praktického hľadiska - t.j. na prekonanie ktorých nie je známy žiadny efektívny postup a útok hrubou silou je výpočtovo nerealizovateľný v rozumnom čase s použitím všetkých súčasných a budúcich dostupných výpočtových prostriedkov.

1.2.1 Symetrické a asymetrické šifrovanie

V tejto časti uvedieme základné pojmy kryptografie a vysvetlíme rozdiel medzi symetrickým a asymetrickým šifrovaním.

Šifra (kryptosystém) je dvojica zobrazení (E, D)[2] - šifrovania a dešifrovania. Pre jednoduchosť predpokladajme, že Alica a Bob pri komunikácii používajú bežnú abecedu a rovnako výsledkom šifrovania je text nad touto abecedou. Označme ju Σ.

Šifrovacia transformácia je zobrazenie

$$E : \Sigma^* \to \Sigma^*.$$

Text, na ktorý sme zatiaľ nepoužili žiadnu kryptografickú transformáciu (teda text pôvodnej správy) nazveme *otvorený text (plaintext)*. Výsledok šifrovania otvoreného textu nazveme *šifrový text (ciphertext)*.

Dešifrovacia transformácia je zobrazenie

$$D : \Sigma^* \to \Sigma^*,$$

ktoré sa vyznačuje tým, že pre ľubovoľnú správu m platí

$$D(E(m)) = m.$$

Nevýhodou takéhoto šifrovania je, že pokiaľ Eva zistí, aké transformácie Alica s Bobom používajú, môže čítať všetky ich správy (stačí použiť rovnaké transformácie).

[2]Iniciály z anglických názvov zobrazení - encryption (šifrovanie) a decryption (dešifrovanie)

Preto sa v praxi používajú šifry, kde okrem spôsobu transformácie je dôležitý aj tajný parameter, nazývaný *kryptografický kľúč*.

V takom prípade šifra je zadaná trojicou (E, D, K), kde K je množina kryptografických kľúčov, E je šifrovacia transformácia

$$E(m, k_1) = c$$

a D je dešifrovacia transformácia

$$D(c, k_2) = m,$$

pričom m je otvorený text, c šifrový text a $k_1, k_2 \in K$ sú kryptografické kľúče.

Z pohľadu použitia kľúča poznáme dva druhy šifier: *symetrické* a *asymetrické*. Pri symetrických šifrách používame ten istý kľúč na šifrovanie aj dešifrovanie (teda $k_1 = k_2$) alebo sa jeden z kľúčov dá z druhého ľahko odvodiť. Ak Alica s Bobom používajú symetrickú šifru, musia kľúč v záujme zachovania dôvernosti komunikácie utajiť, preto ho nazývame *tajným kľúčom*.

Príkladom jednoduchej symetrickej šifry je Cézarova šifra. Nech otvorený text je `KRYPTOGRAFIA` a kľúč k má hodnotu 5. Tento text zašifrujeme na šifrovaný tak, že každé jeho písmeno posunieme o k miest v abecede smerom nadol. Ak dôjdeme na koniec abecedy, budeme pokračovať od začiatku, takže napríklad A zašifrujeme na F, B na G, U na Z a V na A[3]. Šifrovaným textom tak bude reťazec `PWDUYTLWFKNF`. Naopak, reťazec `PWDUYTLWFKNF` dešifujeme tak, že každé písmeno posunieme o k miest v abecede smerom nahor.

Použitie symetrického šifrovania má viacero nevýhod [17, str. 29]:

- Alica a Bob musia poznať rovnaký tajný kľúč, na ktorom sa musia vopred dohodnúť použitím iného kanálu (napríklad osobne).
- Pokiaľ Eva odhalí alebo uhádne tajný kľúč, vie dešifrovať nielen správy aktuálne prebiehajúcej komunikácie, ale aj všetky správy v minulosti a budúcnosti (pokiaľ nedôjde k zmene kľúča).
- Pokiaľ Eva odhalí alebo uhádne tajný kľúč, môže posielať falošné správy jednému z komunikantov a vydávať sa pritom za toho druhého.
- Pokiaľ používame rôzne kľúče pre každú dvojicu komunikantov, počet potrebných kľúčov rastie kvadraticky vzhľadom na počet používateľov siete (pre n používateľov potrebujeme $n \cdot (n-1)/2$ kľúčov).

[3]Teda ak písmenám anglickej abecedy A-Z priradíme postupne hodnoty $0, 1, ..., 25$, tak Cézarova šifra každému znaku x s hodnotou n priradí znak y taký, že jeho hodnotou je $(n + k)$ *mod* 26

Tieto nevýhody rieši druhý typ šifrovania - asymetrické šifrovanie. Pri asymetrických šifrách sa používajú dva rôzne kľúče $k_1 \neq k_2$, pričom jeden kľúč sa z druhého nedá odvodiť[4]. Každý komunikant tak má priradenú dvojicu kľúčov, ktoré nazveme *súkromný* a *verejný kľúč*. Verejný kľúč je známy všetkým používateľom siete, ale súkromný kľúč pozná len daný komunikant.

Ak chce Alica poslať správu Bobovi s použitím asymetrického šifrovania, zašifruje otvorený text správy Bobovým verejným kľúčom (ktorý je Alici známy) a pošle správu Bobovi. Bob správu následne dešifruje svojím súkromným kľúčom. Výhodou asymetrického šifrovania je, že Alica a Bob sa pred zahájením komunikácie vôbec nemusia poznať a nemusia dohadovať tajný kľúč, stačí, ak budú navzájom poznať svoje verejné kľúče. S tým súvisí jeden z najdôležitejších praktických problémov kryptografie - *bezpečná distribúcia verejných kľúčov*. Tejto problematike sa budeme venovať v časti 1.3.

Na rozdiel od použitia symetrického šifrovania, pri použití asymetrického kryptosystému počet použitých kľúčov rastie lineárne s počtom používateľov siete, n používateľov si vyžiada použitie $2 \cdot n$ kľúčov.

Príkladom asymetrickej šifry je RSA, ktorej bezpečnosť je založená na ťažkosti problému rozkladu veľkých prvočísel. Podrobnosti sa čitateľ dozvie v knihe od Stinsona [18, 5].

1.2.2 Hašovanie

V predošlej časti sme popísali niekoľko kryptografických riešení, ktorými možno zabezpečiť dôvernosť komunikácie. V tejto práci je však viac než dôvernosť nutné zabezpečiť ďalšie vlastnosti - najmä autentickosť a ochranu integrity elektronických dokumentov.

Autentickosť elektronických dokumentov možno zabezpečiť digitálnym podpisom, ktorý popisujeme v časti 1.2.3. Ešte predtým predstavíme riešenie na overovanie ich integrity, ktorým je použitie hašovacích funkcií.

Hašovacia funkcia je funkcia, ktorá vstup ľubovoľnej dĺžky konvertuje na výstup fixnej (zvyčajne menšej) dĺžky, nazvaný *digitálny odtlačok (hash)*. *Jednosmerná hašovacia funkcia* je taká funkcia, kedy je ľahké vypočítať jej hodnotu pre daný vstup, ale je ťažké nájsť vstup, ktorého digitálnym odtlačkom je zadaná hodnota. Malá zmena vo vstupe spôsobí značnú zmenu vo výstupe hašovacej funkcie.

Príkladom hašovacej funkcie je funkcia, ktorá správu prevedie do binárnej podoby a spočíta počet jednotkových bitov. Ak je tento počet párny, výstupom je 0, inak je výstupom 1. Táto funkcia však nie je jednosmerná, pretože je triviálne ľahké nájsť správy pre zadaný digitálny odtlačok. V praxi sa používajú oveľa sofistikovanejšie hašovacie funkcie - niekoľko príkladov čitateľ nájde v knihe od Schneiera [17, 18].

[4]Resp. nie je na to známy efektívny algoritmus

Použitím hašovania pri zabezpečení komunikácie môžeme naplniť požiadavku zachovania integrity dát. Ak sa digitálne odtlačky dvoch vstupov (napríklad prijatej a odoslanej správy) zhodujú, môžeme predpokladať, že sa zhodujú aj vstupy. Pravdepodobnosť, s akou môžeme prijať tento predpoklad, závisí od jednosmernosti hašovacej funkcie, obzvlášť od pravdepodobnosti *kolízií* - teda pravdepodobnosti, s akou sa dve rôzne vstupné hodnoty transformujú použitím hašovacej funkcie na tú istú hodnotu. Ak sa ale odtlačky líšia, vieme s určitosťou povedať, že sa líšia aj vstupné hodnoty.

1.2.3 Digitálny podpis

Pri vydávaní elektronických dokumentov je dôležitá otázka autentickosti - možnosti potvrdenia pôvodnosti príslušného dokumentu. V prípade listinných dokumentov túto vlastnosť zabezpečuje vlastnoručný podpis. Jeho analógiou v elektronickom svete je *digitálny podpis*.

Vlastnoručný podpis poskytuje naplnenie nasledujúcich bezpečnostných požiadaviek [17, str. 35]:

1. *autentickosť* - podpis je zárukou, že podpisovateľ dokument podpísal vedome a zámerne,
2. *nesfalšovateľnosť* - podpis je zárukou, že dokument podpísal podpisovateľ, čím potvrdil súhlas s jeho obsahom, a nie nikto iný,
3. *neprenositeľnosť* - podpis je súčasťou dokumentu, nemožno ho preniesť a znovu použiť pre iný dokument,
4. *nemeniteľnosť* - podpísaný dokument nemôže byť nijako upravený,
5. *nepopretie pôvodu* - podpisovateľ nemôže poprieť, že dokument podpísal.

V skutočnosti žiaden z uvedených výrokov nie je celkom pravdivý, pretože podpisy môžu byť sfalšované a podpísané dokumenty zmenené. Ide však o akceptované skutočnosti vzhľadom na technickú náročnosť takéhoto podvádzania.

Pokiaľ však ide o realizáciu podpisu v elektronickej podobe - napríklad v naskenovanom dokumente, falšovanie podpisu je technicky triviálne. Podpis nie je pevne spojený s dokumentom, a možno ho teda vystrihnúť a prilepiť na iný dokument, alebo dokument upraviť bez zanechania akéhokoľvek dôkazu o tejto úprave.

Pri realizácii podpisu elektronicky je teda na zabezpečenie bezpečnostných požiadaviek potrebný silnejší mechanizmus, preto vznikol digitálny podpis, založený na kryptografii.

Jeho najjednoduchšou realizáciou by mohlo byť použitie asymetrickej kryptografie. Ak chce Alica poslať Bobovi podpísaný dokument, zašifruje ho svojim súkromným kľúčom a pošle ho Bobovi, ktorý ho následne môže dešifrovať jej verejným kľúčom.

Toto riešenie je funkčné, nie však efektívne. Šifrovanie celého dokumentu môže trvať dlho, najmä ak ide o rozsiahly dokument. Navyše, podpísaný dokument je rovnako veľký ako pôvodný, takže ak chceme uchovať alebo poslať oba dokumenty súčasne, potrebujeme dvakrát viac pamäťového miesta. Okrem toho, ak by bola použitá bloková šifra (teda dokument by bol šifrovaný po častiach), bolo by možné nepozorovane nahradiť časť dokumentu iným blokom šifrového textu, šifrovaného tým istým kľúčom. Integrita teda v tomto prípade nie je dostatočne chránená.

Preto sa v praxi využíva kombinácia hašovania a asymetrickej kryptografie. Ak chce Alica poslať Bobovi podpísanú správu alebo dokument, postupuje nasledovne:

- Alica vypočíta digitálny odtlačok dokumentu.
- Alica zašifruje vypočítaný odtlačok svojím súkromným kľúčom.
- Pôvodný dokument spolu s podpísaným odtlačkom pošle Alica Bobovi.

Pre overenie platnosti podpisu dokumentu Bob najprv vypočíta digitálny odtlačok dokumentu, potom dešifruje zašifrovaný odtlačok od Alice jej verejným kľúčom a tieto dve hodnoty porovná. Ak sú hodnoty totožné, podpis považuje za pravý, inak ide s určitosťou o falzifikát.

Takéto riešenie je rovnako funkčné ako predchádzajúce, poskytuje však vyššiu efektivitu. Vytvorenie digitálneho podpisu trvá kratšie a samotný podpis nezaberá veľa miesta. Integritu zabezpečuje jednosmernosť hašovacích funkcií.

Digitálny podpis napĺňa bezpečnostné požiadavky na vlastnoručný podpis v rozsahu rovnakom alebo vyššom ako vlastnoručný podpis. Vďaka použitiu hašovacej funkcie je podpis pevne spätý s dokumentom a zaručuje tak jeho nemeniteľnosť a neprenositeľnosť na iný dokument. Pri pokuse o použitie digitálneho podpisu na iný alebo zmenený dokument by overenie podpisu zlyhalo pre nezhodu digitálnych odtlačkov[5].

Použitie asymetrickej kryptografie garantuje autentickosť a nesfalšovateľnosť podpisu. Keďže Alica ako jediná pozná svoj súkromný kľúč, bez jej vedomia nemôže byť dokument v jej mene podpísaný.

Popísaná schéma digitálneho podpisovania ešte nevylučuje možnosť popretia pôvodu. Alica môže podpísať digitálny dokument (napríklad šek pre Boba výmenou za jeho auto), následne vyzradiť svoj súkromný kľúč (napríklad jeho zverejnením na Internete) a tvrdiť, že podpis na šeku nepochádza od nej, nakoľko nebola jedinou osobou,

[5]Za predpokladu, že dokumenty majú rôzne digitálne odtlačky, čo je vzhľadom na vlastnosti použitej hašovacej funkcie vysoko pravdepodobné

ktorá mala prístup k svojmu súkromnému kľúču. Riešenie takejto situácie má dve časti. Prvou je doplnenie dokumentu o informáciu o čase, v ktorom bol dokument podpísaný.

Druhou časťou riešenia je znemožniť vlastníkovi súkromného kľúča tento kľúč poznať (a teda aj kompromitovať). To dosiahneme tak, že na vytváranie digitálneho podpisu použijeme špecializovaný hardvér, ktorý bude schopný vytvárať digitálny podpis, ale nie exportovať súkromný kľúč, ktorý je na ňom uložený. Na tento účel sa používa takzvaná *čipová karta (smart card)*, na ktorej sú uložené kryptografické kľúče a certifikáty, v spojení s *čítačkou kariet*, ktorá zabezpečuje podpisovanie dokumentov s použitím kľúča uloženého na karte.

Európska legislatíva [4] rozlišuje niekoľko druhov elektronických podpisov podľa úrovne záruk, ktoré poskytujú. Pod pojmom *elektronický podpis* rozumie akýkoľvek podpis v elektronickej podobe, teda aj sken vlastnoručného podpisu, meno napísané v textovom editore, prípadne podpis vyhotovený napísaním na tablete. Za *zdokonalený elektronický podpis* sa považuje digitálny podpis, teda podpis vytvorený za pomoci kryptografických prostriedkov. Najvyššiou úrovňou z hľadiska bezpečnosti je *kvalifikovaný elektronický podpis*, pod ktorým sa rozumie digitálny podpis vytvorený za pomoci špecializovaného hardvéru, ktorý znemožňuje export súkromného kľúča.

Nakoľko posledný z menovaných spĺňa všetky bezpečnostné požiadavky, ktoré spĺňa aj vlastnoručný podpis, má kvalifikovaný elektronický právny účinok rovnocenný s vlastnoručným podpisom. V slovenskej legislatíve sa tento podpis vyskytuje aj pod pojmom *zaručený elektronický podpis* [5]. Ak budeme v kontexte tejto práce spomínať elektronický alebo digitálny podpis, budeme mať vždy na mysli jeho najvyššiu úroveň, teda zaručený elektronický podpis (resp. kvalifikovaný elektronický podpis či digitálny podpis vytvorený za pomoci špecializovaného hardvéru).

1.3 PKI (Public Key Infrastructure)

V predošlých častiach sme popísali niekoľko možností využitia asymetrickej kryptografie - najmä šifrovanú komunikáciu a digitálny podpis. Pri opisovaní modelových situácií sme doposiaľ vždy predpokladali, že verejné kľúče jednotlivých entít sú známe všetkým účastníkom komunikácie.

Otázkou zostáva, ako zabezpečiť ich bezpečnú distribúciu tak, aby sa komunikanti mohli spoľahnúť na ich autenticitu. Len v takom prípade spolu môžu bezpečne komunikovať aj dve entity, ktoré sa navzájom nepoznajú - ak chce Alica poslať správu Bobovi, potrebuje jeho verejný kľúč a istotu, že kľúč patrí naozaj jemu a nie napríklad Eve.

1.3.1 Základný koncept PKI

Riešením problému bezpečnej distribúcie verejných kľúčov je *PKI (Public Key Infrastructure)*, systém na kontrolu a správu certifikátov [18, str. 457]. *Certifikačná autorita* je základnou stavebnou jednotkou PKI. Certifikačná autorita vydáva entitám (*držiteľom certifikátu*) *certifikáty verejného kľúča*.

Certifikát verejného kľúča je z bezpečnostného hľadiska bezpečnostný mechanizmus, ktorý plní nasledujúce funkcie:

- obsahuje verejný kľúč držiteľa certifikátu v takej forme, ktorá chráni jeho autentickosť a umožňuje jeho spoľahlivú distribúciu,
- spája verejný kľúč s identitou držiteľa súkromného kľúča, ktorý prislúcha tomuto verejnému kľúču.

Certifikát verejného kľúča môže plniť aj iné funkcie, môže byť napríklad zdrojom informácií potrebných na overenie digitálneho podpisu.

Certifikátom je z hľadiska spracovania elektronický dokument so štruktúrovanou formou, pričom obsah a štruktúra jednotlivých polí, ktoré sú jeho súčasťou, závisia od zvoleného štandardu. Každý certifikát však musí obsahovať informácie o certifikačnej autorite, ktorá certifikát vydala, držiteľovi certifikátu a období platnosti certifikátu. Certifikát musí obsahovať verejný kľúč jej držiteľa a musí byť podpísaný digitálnym podpisom certifikačnej autority.

Aby bolo možné jednoznačne určiť, odkedy certifikát nadobúda platnosť, podpis certifikačnej autority môže zahŕňať *časovú pečiatku* - informáciu o čase, v ktorom bol certifikát vydaný.

Certifikát verejného kľúča entity je teda podpísaný verejným kľúčom certifikačnej autority. Tu sa ale dostávame opäť k tomu istému problému - ako overiť, či príslušný verejný kľúč naozaj patrí certifikačnej autorite? Je známych niekoľko riešení tohto problému, zo všetkých spomenieme riešenie, kedy certifikačné autority tvoria hierarchickú štruktúru s jednou koreňovou certifikačnou autoritou. Každá certifikačná autorita má svoj verejný kľúč potvrdený podpisom jej nadradenej certifikačnej autority, ktorá jej vydala certifikát. Výnimkou je koreňová certifikačná autorita, ktorej verejný kľúč je zverejnený na nejakom verejne dostupnom mieste, napríklad v novinách alebo v zbierke zákonov.

V našej modelovej situácii Bob teda najprv požiada certifikačnú autoritu o vydanie certifikátu pre jeho verejný kľúč. Certifikačná autorita overí jeho identitu a vydá mu certifikát, ktorý bude podpísaný jej súkromným kľúčom.

Ak chce Alica poslať správu Bobovi, najprv zistí jeho verejný kľúč a overí platnosť podpisu certifikačnej autority na certifikáte tohto verejného kľúča. Pokiaľ Alica certi-

fikačnej autorite dôveruje, dôveruje aj autentickosti tohto verejného kľúča a môže ho bezpečne použiť v komunikácii s Bobom.

V predošlej časti sme zaviedli pojmy elektronický podpis, zdokonalený elektronický podpis a kvalifikovaný elektronický podpis. Rovnako sa v legislatíve rozlišuje viacero pojmov pre certifikáty. V kontexte tejto práce budeme používať najmä pojmy *certifikát* a *mandátny certifikát*. Pod pojmom certifikát budeme rozumieť certifikát verejného kľúča vydaný certifikačnou autoritou, pod pojmom mandátny certifikát budeme rozumieť certifikát pre elektronický podpis vydaný štatutárovi (právnickej osoby alebo orgánu verejnej moci) alebo splnomocnencovi (fyzickej osobe oprávnenej konať v mene inej fyzickej, právnickej osoby alebo orgánu verejnej moci). Mandátny certifikát je udelený napríklad riaditeľovi školy, firmy alebo rektorovi univerzity.

1.3.2 Zrušenie certifikátu

Každý certifikát vydaný certifikačnou autoritou je platný len po určité obdobie - *dobu platnosti certifikátu*. Ešte pred uplynutím tejto doby môže držiteľ certifikátu požiadať certifikačnú autoritu o vydanie nového certifikátu. Toto opatrenie prispieva k vyššej bezpečnosti systému PKI, nakoľko čas potrebný na zistenie súkromného kľúča k verejnému útokom hrubou silou je oveľa väčší ako obdobie platnosti certifikátu tohto kľúča.

V niektorých prípadoch však môže držiteľ požiadať certifikačnú autoritu o predčasné zrušenie certifikátu, najmä v prípadoch, kedy došlo k strate alebo prezradeniu jeho súkromného kľúča, prípadne k zmene údajov v certifikáte. Certifikačná autorita musí platnosť tohto certifikátu zrušiť okamžite a zverejniť tento fakt v *Zozname zrušených certifikátov*.

Zoznam zrušených certifikátov je vydávaný pravidelne, napríklad každých 12 alebo 24 hodín. Certifikačné autority zvyčajne poskytujú aj možnosť online overenia, či je certifikát platný alebo bol zrušený, a to porovnaním identifikačného čísla certifikátu s údajmi v ich databázach.

Zoznam zrušených certifikátov sa používa pri overovaní platnosti certifikátu. Ak Alica chce overiť platnosť Bobovho certifikátu, najprv overí pravosť digitálneho podpisu certifikačnej autority, ktorá certifikát vydala, a následne si preverí, či sa Bobov certifikát nenachádza v zozname zrušených certifikátov. Ak nie, až vtedy ho považuje za platný.

1.4 Zhrnutie

V tejto kapitole sme sa oboznámili so základnými pojmami informačnej bezpečnosti a kryptológie a zaviedli sme pojmy, ktoré budeme používať v kontexte tejto práce. V ďalších častiach práce budeme využívať digitálny podpis na ochranu integrity vydáva-

ných dokumentov (diplomov). Pri overovaní ich platnosti budeme využívať popísané princípy PKI.

Kapitola 2

Analýza Zákona o e-Governmente

V tejto kapitole sa budeme zaoberať analýzou Zákona o e-Governmente, nosného zákona, ktorý upravuje výkon orgánov verejnej moci elektronicky. Z pohľadu Univerzity Komenského (UK) budeme skúmať, aké povinnosti jej zákon ukladá a čo si ich naplnenie bude vyžadovať. V prvej časti kapitoly popíšeme hlavné časti zákona, v ďalších častiach pomenujeme povinnosti, ktoré Univerzite Komenského z tohto zákona vyplývajú.

2.1 Zákon o e-Governmente

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (Zákon o e-Governmente) bol prijatý Národnou radou Slovenskej republiky 4.9.2013 a platnosť nadobudol 1.11.2013 okrem niektorých ustanovení, ktoré nadobudli účinnosť 1.11.2016. Zákon bol odvtedy niekoľkokrát novelizovaný a jeho účinnosť posunutá, preto niektoré jeho časti nadobudnú účinnosť v priebehu rokov 2017 a 2018.

Zákon upravuje výkon verejnej moci v elektronickej podobe, ktorá by sa mala stať alternatívou k papierovému (listinnému) spôsobu výkonu verejnej moci. Ustanovuje elektronickú komunikáciu ako nosnú formu komunikácie, či už medzi občanmi a orgánmi verejnej moci, alebo medzi orgánmi verejnej moci navzájom. Jeho cieľom je zjednodušenie, zrýchlenie, sprehľadnenie a zjednotenie komunikačných procesov, a v neposlednom rade aj zvýšenie bezpečnosti komunikácie. [9]

Zákon stanovuje povinnosti a právomoci orgánom verejnej moci, medzi ktoré sa zaraďuje aj Univerzita Komenského, a preto aj Univerzita musí prijať vhodné opatrenia na to, aby tento zákon naplnila. Nakoľko sa ale Zákon o e-Governmente týka výkonu veľkého množstva orgánov verejnej moci, je formulovaný pomerne všeobecne. Preto sa v časti 2.2 budeme venovať podrobnejšej analýze tých jeho častí, ktoré sa vzťahujú aj na Univerzitu Komenského ako na orgán verejnej moci.

2.1.1 Hlavné časti zákona

Zákon o e-Governmente upravuje výkon verejnej moci elektronicky v medziach už existujúcich právomocí príslušného orgánu verejnej moci. Orgánom verejnej moci teda neurčuje nové právomoci, len rozširuje spôsob ich vykonávania o elektronický.

Zákon zavádza nové pojmy - *elektronická schránka* a *elektronické doručovanie*. Elektronická schránka je úložisko elektronických správ, je teda analógiou poštovej schránky. Rôzne žiadosti úradom (alebo napríklad prihlášku na vysokú školu) tak bude možné okrem zaslania v papierovej podobe bežnou poštou odoslať aj elektronicky do elektronickej schránky príslušného úradu, vysokej školy alebo iného orgánu verejnej moci.

V prvej fáze bude elektronická schránka zriadená všetkým orgánom verejnej moci a právnickým osobám, aby bola umožnená elektronická komunikácia s nimi. Je cieľom, aby postupne mali elektronické schránky zriadené všetci plnoletí občania Slovenskej republiky, aby sa elektronická forma komunikácie stala dominantnou.

Komunikovať s orgánmi verejnej moci bude možné vyplnením *elektronického formulára* a odoslaním *elektronického podania*, ktoré týmto vyplnením vznikne. O prijatí elektronického podania, ako aj o priebehu príslušného procesu, bude občan informovaný *notifikáciou* do svojej elektronickej schránky.

Orgány verejnej moci budú s verejnosťou komunikovať buď zasielaním *elektronických úradných správ* (ktoré vzniknú rovnako vyplnením elektronického formulára), alebo notifikácií do elektronických schránok občanov, alebo zverejňovaním dôležitých informácií na elektronických úradných tabuliach, ktoré budú analógiou úradných tabúľ.

Na zaistenie bezpečnosti elektronickej komunikácie je nutné zaviesť spoľahlivé prostriedky na identifikáciu, autentifikáciu a autorizáciu. Na identifikáciu a autentifikáciu, teda prístup k elektronickej schránke, sa v prípade fyzických osôb bude používať predovšetkým občiansky preukaz s čipom. V prípade právnických osôb alebo orgánov verejnej moci sa použije občiansky preukaz s čipom osoby oprávnenej konať v ich mene[1].

Na autorizáciu sa použije *zaručený elektronický podpis*, ktorý je v prípade orgánu verejnej moci doplnený o *mandátny certifikát* alebo nahradený *zaručenou elektronickou pečaťou* s pripojenou *časovou pečiatkou*.

Nakoľko verejná moc bude vykonávaná listinne aj elektronicky, vznikne potreba prevádzania dokumentov z jednej formy do druhej. Je pritom žiaduce, aby bol zachovaný nielen obsah dokumentu, ale aj úroveň bezpečnostných prvkov (napríklad notársky overený podpis). Preto sa zavádza pojem *zaručená konverzia*. Zákon upravuje spôsob jej vykonávania a udeľuje oprávnenia vykonávať zaručenú konverziu (napríklad orgánom verejnej moci, notárovi či advokátovi).

[1] Právnické osoby a orgány verejnej moci majú okrem toho možnosť využiť automatizovaný prístup k elektronickej schránke [3, §22a, 22aa]

Komunikácia občanov s orgánmi verejnej moci bude možná buď s použitím ich vlastných zariadení s nainštalovaným príslušným softvérom, alebo prostredníctvom integrovaných obslužných miest. O ich zriadenie a prevádzku sa budú starať najmä obce, ktoré tak budú poskytovať asistenciu pri komunikácii s orgánmi verejnej moci elektronicky.

Zákon upravuje aj spôsob úhrady poplatkov orgánom verejnej moci (napríklad súdnych alebo správnych poplatkov). Tento bude možný prostredníctvom *akreditovaného platcu* alebo na integrovanom obslužnom mieste.

K zvýšeniu efektivity výkonu verejnej moci prispeje aj prepojenie informačných systémov jednotlivých orgánov verejnej moci s centrálnymi informačnými systémami - *ústredným portálom*, ktorý bude sprostredkovávať elektronickú úradnú komunikáciu s orgánmi verejnej moci. Navyše sa zavádza pojem *referenčné registre* - teda databázy, ktoré budú obsahovať istý základný typ údajov, napríklad zoznam právnických osôb alebo uchádzačov o zamestnanie.

Občania a podnikatelia tak pri komunikácii s orgánmi verejnej moci (napríklad pri vypĺňaní elektronických formulárov) nebudú musieť znovu predkladať údaje, ktorými už štát disponuje - či už pôjde o údaj z niektorého z informačných systémov orgánov verejnej moci, ústredného portálu alebo referenčných registrov. Ministerstvo financií Slovenskej republiky túto skutočnosť označuje pojmom „jedenkrát a dosť“.

2.2 Povinnosti Univerzity Komenského

V nasledujúcich častiach uvedieme hlavné povinnosti a právomoci Univerzity Komenského ako orgánu verejnej moci, ktoré jej vyplývajú zo Zákona o e-Governmente a súvisiacich zákonov a nariadení.

Kompletnú analýzu Zákona o e-Governmente z pohľadu UK ako orgánu verejnej moci nájde čitateľ v dodatku A.

2.2.1 Elektronické schránky

Univerzita Komenského má podľa [3, §11] ako orgán verejnej moci bezplatne zriadenú elektronickú schránku. Túto schránku má povinnosť aktivovať najneskôr do 1. júla 2017. Majiteľom schránky UK je jej štatutár, teda rektor [1, §10].

Majiteľ elektronickej schránky má právo na prístup k nej, ako aj na udeľovanie oprávnení na prístup iným osobám, a určenie rozsahu týchto oprávnení.

Elektronické schránky môžu byť zriadené aj organizačným zložkám a súčastiam Univerzity, napríklad jednotlivým fakultám, internátu, rektorátu. O zriadenie takejto elektronickej schránky môže prostredníctvom ústredného portálu požiadať rektor UK.

Oprávnenie na prístup k takto zriadenej elektronickej schránke má vedúci organizačnej zložky alebo súčasti UK (napríklad dekan fakulty), majiteľom schránky je rektor UK. Univerzita bude mať k dispozícii zoznam všetkých takto vytvorených schránok.

Univerzita Komenského má povinnosť udržiavať zoznam všetkých organizačných zložiek a jej súčastí, rovnako ako osôb oprávnených na prístup k ich elektronickým schránkam.

Po zániku organizačnej zložky alebo súčasti je takáto schránka deaktivovaná, pričom sa zachová jej obsah a prístup k nej.

Ako orgán verejnej moci má UK nárok na vyššiu úložnú kapacitu elektronickej schránky ako fyzické či právnické osoby. Navyše, ak UK túto kapacitu prekročí, môže požiadať o jej bezplatné navýšenie. [3, §16]

Univerzita Komenského má oprávnenie prevádzkovať v rámci svojho informačného systému vlastnú elektronickú schránku [3, §16], do ktorej môže preposielať notifikácie a správy, ktoré nie sú určené do vlastných rúk [3, §30].

2.2.2 Elektronická podateľňa

Podľa [3, §30] je Univerzita Komenského ako orgán verejnej moci povinná kontrolovať elektronickú schránku každodenne, s výnimkou štátnych sviatkov a dní pracovného pokoja. Na tieto účely musí mať zriadenú elektronickú podateľňu, ktorá bude potvrdzovať prijatie elektronických správ.

Elektronické správy, ktoré majú byť doručené do vlastných rúk, potvrdí vytvorením elektronickej doručenky. Doručenie ostatných správ bude potvrdzované automaticky pomocou notifikačného modulu.

UK môže notifikačný modul využiť aj na zasielanie výziev a dôležitých oznámení verejnosti, napríklad oznámenie o zverejnení výsledkov prijímacích skúšok.

2.2.3 Elektronické formuláre

Univerzita Komenského má povinnosť spracovávať elektronické podania, ktoré vzniknú vyplnením elektronických formulárov zverejnených v module elektronických formulárov ústredného portálu [3, §24]. Takéto podanie je ekvivalentné podaniu v listinnej forme.

UK musí zabezpečiť aj spracovanie takého elektronického podania, ktoré nevzniklo vyplnením elektronického formulára, ale má rovnakú štruktúru a vizuálnu podobu.

Elektronické úradné dokumenty (napríklad rôzne rozhodnutia) môže UK vytvárať vyplnením príslušného elektronického formulára alebo bez jeho použitia, ak zabezpečí rovnakú štruktúru a vizuálnu podobu.

Vytváranie, aktualizáciu a rušenie elektronických formulárov, ktoré bude UK spracovávať, zabezpečuje Ministerstvo školstva, vedy, výskumu a športu Slovenskej repub-

liky (ministerstvo školstva). Ministerstvo môže vytvorením formulára poveriť aj orgán verejnej moci, teda aj Univerzitu Komenského.

2.2.4 Elektronická úradná tabuľa

UK musí na elektronickej úradnej tabuli zverejňovať všetky elektronické dokumenty, ktorých listinnú analógiu má povinnosť zverejňovať na úradnej tabuli, a to v ten istý deň, ako dokumenty zverejní na úradnej tabuli [3, §34].

Prístup k elektronickej úradnej tabuli udelí Univerzite správca modulu elektronického doručovania, teda Úrad vlády Slovenskej republiky.

2.2.5 Zaručená konverzia

Podľa [3, §35] má UK ako orgán verejnej moci právo vykonávať zaručenú konverziu elektronických dokumentov na listinné a opačne, a to podľa postupu popísaného v [3, §36]. Nebude tak musieť ďalej za takéto služby platiť notárom. Má však povinnosť udržiavať záznamy o všetkých vykonaných zaručených konverziách.

2.2.6 Identifikácia, autentifikácia a autorizácia

Na preukázanie identity pri využívaní elektronických služieb poskytovaných orgánmi verejnej moci (napríklad úradmi, súdmi, ministerstvami, ale aj vysokými školami) sa podľa Zákona o e-Governmente bude používať občiansky preukaz s čipom (eID). Ide o nový typ občianskeho preukazu, ktorý okrem preukazovania totožnosti pri osobnom styku s orgánmi verejnej moci bude slúžiť aj na identifikáciu a autentifikáciu v elektronickom priestore. Okrem osobných údajov o občanovi obsahuje elektronický čip. Na jeho použitie je potrebná čítačka kariet a príslušný obslužný softvér.

Elektronický čip obsahuje kryptografické kľúče a certifikát pre zaručený elektronický podpis. Ku eID sú priradené tri číselné kombinácie - bezpečnostný osobný kód (BOK), ZEP PIN a ZEP PUK, ktoré si občan zvolí pri preberaní dokladu. Ide o tajné číselné kódy, ktoré sa používajú na vytváranie zaručeného elektronického podpisu; podrobnosti uvedieme nižšie.

Občiansky preukaz s čipom je možné využiť na autentifikáciu, vytvorenie elektronického podpisu, vytvorenie zaručeného elektronického podpisu a šifrovanie. Na identifikáciu a autentifikáciu slúži použitie eID a zadanie BOK. Na vytvorenie zaručeného elektronického podpisu je nutné použitie ZEP PIN. Po troch nesprávnych pokusoch zadania ZEP PIN sa zablokuje možnosť použitia súkromného kľúča na vytvorenie ZEP, pričom odblokovanie je možné len po zadaní ZEP PUK.

Na preukázanie identity pri prístupe do elektronickej schránky teda musí rektor UK a ním poverené osoby využívať občiansky preukaz s čipom. Univerzita Komenského

môže k elektronickej schránke pristupovať aj automatizovane, podmienky upravuje [3, §22a, §22aa, §22b].

UK bude vykonávať autorizáciu (teda podpisovanie elektronických úradných podaní) zaručeným elektronickým podpisom a mandátnym certifikátom alebo zaručenou elektronickou pečaťou s časovou pečiatkou [3, §23]. Na tento účel si rektor Univerzity musí vybaviť občiansky preukaz s čipom a mandátnym certifikátom.

Univerzita Komenského je povinná prispôsobiť svoje informačné systémy tak, aby na identifikáciu a autentifikáciu osôb, ktorých sa týka konanie UK ako orgánu verejnej moci, využívala identifikátor a autentifikátor osoby podľa [3, §3, §22].

Identifikátorom osoby je rodné číslo v spojení s menom a priezviskom alebo iný identifikátor, ak ide o zahraničnú osobu. Autentifikátorom sa rozumie občiansky preukaz s čipom.

UK môže vo svojich informačných systémoch využívať aj iný identifikátor a autentifikátor osôb (napríklad univerzitný login), musí však zabezpečiť ich obojsmernú transformáciu na identifikátor a autentifikátor osoby podľa Zákona o e-Governmente.

2.2.7 Prepojenie informačných systémov

Podľa [3, §6, §17] musí UK poskytovať iným orgánom verejnej moci prístup k údajom svojho informačného systému, ktoré môžu potrebovať pre výkon verejnej moci, a to aj automatizovane. UK je povinná poskytovať informácie o svojej činnosti správcovi ústredného portálu a musí umožniť prepojenie ústredného portálu so svojím informačným systémom, ktorý súvisí s výkonom verejnej moci. Prepojenie informačných systémov bude koordinovať Ministerstvo financií Slovenskej republiky.

Univerzita Komenského je povinná poskytnúť hodnoty údajov z registrov, ktoré vedie (t.j. databáz, ktoré spravuje), na účely výkonu verejnej moci elektronicky. Pri výkone verejnej moci zároveň UK nesmie od dotknutých osôb žiadať údaje, ktoré sú známe jej alebo iným orgánom verejnej moci z predošlej činnosti, prípadne sú obsahom referenčných registrov. Preto má UK právo žiadať iné orgány verejnej moci o hodnoty údajov z nimi vedených registrov.

Podľa [1, §54, §80b, §102a] Univerzita Komenského poskytuje údaje do Registra študijných programov a Registra zamestnancov vysokých škôl. Do Registra vysokých škôl UK poskytuje informácie o jej súčastiach, členoch správnej rady či osobách poverených vykonávaním funkcie rektora, prorektoroch a iných vedúcich zamestnancoch vysokej školy. Tieto registre spravuje ministerstvo školstva.

Podľa [1, §73, §73a] Univerzita Komenského vedie Register študentov, z ktorého poskytuje údaje do Centrálneho registra študentov. Centrálny register študentov spravuje a poskytovanie údajov koordinuje ministerstvo školstva.

2.3 Ďalšie povinnosti Univerzity Komenského

V predošlej časti sme popísali povinnosti, ktoré Univerzite Komenského priamo ukladá Zákon o e-Governmente, napríklad zriadenie a používanie elektronickej schránky na komunikáciu so študentami. Okrem toho sme však identifikovali ďalšie povinnosti, ktoré musí Univerzita splniť, aby naplnila všetky požiadavky zákona. Podľa Zákona o e-Governmente [3, §4] je totiž nutné zabezpečiť, aby informačné systémy Univerzity Komenského „boli vybudované takým spôsobom, ktorý umožní výkon verejnej moci elektronickými prostriedkami v celom rozsahu a v každom štádiu“. Na splnenie tejto požiadavky budú potrebné ďalšie zmeny.

Aj keď sa zákon o e-Governmente sústredí najmä na popisovanie elektronickej komunikácie medzi orgánmi verejnej moci a občanmi, zároveň kladie požiadavku na to, aby aj spracovanie prijatých elektronických podaní prebiehalo elektronicky a automatizovane. Hlavný cieľ zákona - dosiahnuť zjednodušenie, sprehľadnenie a zefektívnenie výkonu verejnej moci - totiž nie je zabezpečený len používaním elektronickej komunikácie, ale práve jej kombináciou s elektronizáciou samotného výkonu verejnej moci.

V opačnom prípade by sa výkon verejnej moci elektronicky obmedzil na doručovanie elektronických podaní orgánom verejnej moci, ktoré by sa následne vytlačili, spracovali tradičným spôsobom a ich výsledok by sa opäť previedol do elektronickej podoby. Toto by bolo len mylne možné považovať za informatizáciu výkonu verejnej moci, v skutočnosti by išlo o rovnako pomalý proces s eliminovaním fyzického kontaktu s verejnosťou.

Nakoľko sa zákon dotýka veľkého množstva inštitúcií, ktorých činnosti sú rozmanité, definovanie elektronizácie činnosti každej z nich by výrazne presahovalo rozsah Zákona o e-Governmente. Zákon preto ďalej spôsob spracovania prijatých elektronických formulárov nijako nešpecifikuje a neupravuje, a je teda nutné, aby sa o naplnenie tejto časti informatizácie svojho výkonu verejnej moci postarala každá inštitúcia (vrátane Univerzity Komenského) špecificky, či už vo vlastnej réžii, alebo (aby sa predišlo vzniku chaosu a množstva nekompatibilných riešení) pod vedením orgánov zodpovedných za informatizáciu verejnej správy, respektíve jednotlivých ministerstiev (v prípade Univerzity ministerstva školstva).

Na splnenie požiadaviek Zákona o e-Governmente teda nebude stačiť používať pripravené centrálne spravované moduly, ale tiež vykonať nemalé technické úpravy v informačných systémoch Univerzity, rovnako ako organizačné zmeny v spôsobe samotného výkonu verejnej moci. Tejto problematike sa budeme venovať v ďalších častiach práce.

2.4 Zhrnutie

V tejto kapitole sme čitateľovi priblížili hlavné idey Zákona o e-Governmente a popísali sme jeho časti, ktoré sú relevantné pre Univerzitu Komenského ako pre orgán verejnej moci.

Z našej analýzy vyplynulo, že Zákon o e-Governmente sa venuje primárne elektronizácii komunikácie, či už medzi občanom a orgánom verejnej moci, právnickou osobou a orgánom verejnej moci, alebo orgánmi verejnej moci navzájom. Univerzite Komenského tak zo zákona priamo vyplýva niekoľko povinností, ktoré s komunikáciou súvisia - zriadenie elektronickej schránky, udržiavanie elektronickej podateľne a poskytovanie údajov z jej informačných systémov do referenčných registrov, resp. koordináciu jej databáz s databázami ostatných orgánov verejnej moci a centrálne spravovanými databázami.

Na druhej strane, hoci primárnym cieľom zákona bolo zabezpečenie zefektívnenia procesov, zákon sa nevenuje práve elektronizácii spracovania dokumentov. Upravuje len podmienky spracovania vstupu a výstupu (komunikácie), avšak nie samotného procesu. Výsledkom informatizácie činnosti orgánov verejnej moci by však nemala byť len transformácia ich komunikácie do elektronickej formy, ale predovšetkým automatizácia procesu spracovania v každom kroku. Preto sme ako ďalšiu požiadavku vyplývajúcu zo Zákona o e-Governmente identifikovali prispôsobenie informačných systémov Univerzity, aby bola splnená požiadavka automatizácie. Tejto problematike sa budeme venovať v nasledujúcej a ďalších kapitolách.

Samozrejme, Zákon o e-Governmente bude potrebné sledovať aj naďalej a reagovať na všetky jeho prípadné novely, ktoré budú môcť obsahovať ďalšie požiadavky na Univerzitu Komenského.

Kapitola 3

Informatizácia výkonu verejnej moci

V kapitole 2 sme popísali azda najväčšiu úlohu, ktorá pre Univerzitu Komenského vyplýva zo Zákona o e-Governmente. Keďže zákon upravuje spôsob elektronickej komunikácie Univerzity Komenského s občanmi, ale už nepopisuje samotný proces výkonu verejnej moci, bude potrebné upraviť spôsob výkonu verejnej moci a previesť ho do elektronického sveta.

Prvým krokom informatizácie nutne musí byť analýza existujúceho stavu - zistenie, aké procesy prebiehajú na Univerzite Komenského, ako prebiehajú v listinnom svete a akým spôsobom ich bude možné previesť do elektronického sveta (či už priamočiaro, alebo bude potrebné prispôsobiť aj samotný proces). Takáto analýza je obsahom prvej časti tejto kapitoly.

V jej druhej časti sa zameriame na jeden vybraný proces - vydávanie a správu dokladov o vzdelaní, ktorý zanalyzujeme a popíšeme podrobnejšie. Táto analýza bude slúžiť ako východisko pre ostatné časti, kedy sa pokúsime o informatizáciu tohto procesu. Rovnako bude potrebné postupovať pre ostatné relevantné procesy.

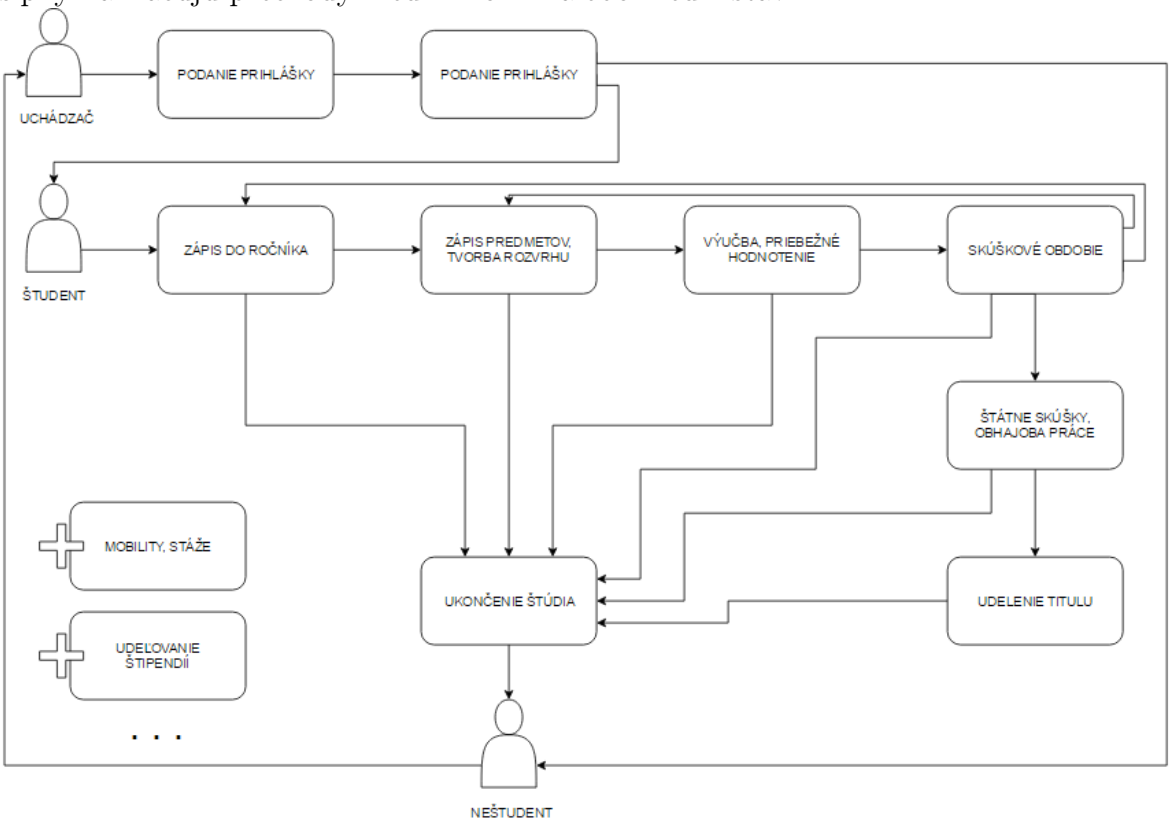
3.1 Identifikácia kľúčových procesov

Univerzita Komenského je orgánom verejnej moci v oblasti vzdelávania, preto aj dokumenty, ktoré bude v súvislosti s výkonom verejnej moci spracovávať, budú súvisieť s procesmi študijnej agendy. Univerzita ako orgán verejnej moci komunikuje predovšetkým s občanmi (viac ako s právnickými osobami a inými orgánmi verejnej moci), v najväčšej miere však so študentami.

Pre identifikáciu týchto dokumentov preto budeme prirodzene sledovať vzdelávací proces vzhľadom na životný cyklus študenta - od podania prihlášky až po udelenie diplomu. Pre každý stav v životnom cykle študenta identifikujeme dokumenty, ktoré môže študent adresovať univerzite a rozhodnutia, ktoré môže Univerzita vydať.

Osoba (študent) sa z pohľadu univerzity môže nachádzať vo viacerých stavoch:

Obr. 3.1: Obrázok znázorňuje tri možné stavy osoby (študenta) a možné prechody medzi týmito stavmi v jednotlivých krokoch, ktoré predstavujú procesy študijnej agendy univerzity. Stavy sú vyznačené obrázkami postavičiek, obdĺžniky predstavujú kroky a šípky naznačujú prechody medzi krokmi alebo medzi stavmi.



1. *uchádzač* - osoba, ktorá má záujem o štúdium na univerzite,
2. *študent* - osoba študujúca na univerzite,
3. *neštudent* - osoba, ktorá nie je uchádzačom ani študentom (môže ísť aj o osobu, ktorá štúdium na univerzite absolvovala, prerušila alebo ukončila).

Prechody medzi jednotlivými stavmi sú znázornené na obrázku 3.1, pričom každý prechod je rozdelený do niekoľkých krokov. Prípadom prechodu zo stavu *uchádzač* do stavu *študent* môže byť nasledujúca postupnosť krokov:

1. uchádzač podá prihlášku na štúdium,
2. uchádzač splní kritériá pre daný odbor, preto je pozvaný na prijímacie konanie,
3. uchádzač absolvuje prijímacie konanie a dosiahne počet bodov potrebný na prijatie,
4. uchádzač sa stáva študentom.

Naopak, nasledujúce kroky by mohli viesť k prechodu zo stavu *študent* do stavu *uchádzač*:

1. študent absolvuje zápis do ročníka,
2. študent si vytvorí študijný plán pre semester,
3. študent absolvuje predmety zo študijného plánu,
4. študent absolvuje skúšky, avšak nesplní podmienky na prechod do ďalšieho semestra (nezíska dostatočný počet kreditov),
5. študent ukončí štúdium a prejde do stavu *neštudent*,
6. neštudent sa rozhodne pre pokus o opakovanie štúdia a prejde do stavu *uchádzač*.

Pre jednotlivé kroky v rámci životného cyklu študenta môžeme identifikovať procesy, ktoré na Univerzite prebiehajú a dokumenty, ktoré sú v rámci nich vydávané. Niekoľko príkladov takýchto procesov a s nimi súvisiacich dokumentov ilustruje tabuľka 3.1. Keďže agenda Univerzity Komenského je rozsiahla, sústredíme sa len na základné procesy a dokumenty, nejde teda o ich kompletný zoznam.

Uvedené dokumenty budú mať svoju analógiu v module elektronických formulárov podľa Zákona o e-Governmente. Formát a štruktúru týchto elektronických formulárov stanoví ministerstvo školstva, úlohou Univerzity bude ich používať na vydávanie elektronických úradných dokumentov.

Aby však bola automatizácia procesu úplná, bude nutné elektronizovať aj ostatné jeho časti, nie len jeho výstupy, ktorými sú úradné rozhodnutia - a to aj keď nie všetky časti procesu priamo súvisia s výkonom verejnej moci.

Napríklad proces prijímacieho konania zahŕňa evidenciu a vyhodnocovanie prihlášok, zasielanie pozvánok na prijímacie skúšky, vyhodnocovanie skúšok a zasielanie rozhodnutí o prijatí či neprijatí. Hoci napríklad rozhodnutie o prijatí patrí do kategórie úradných rozhodnutí, zatiaľ čo pozvánka na prijímacie skúšky má len informatívny charakter, informačný systém Univerzity by mal podporovať správu všetkých týchto častí, a to automatizovaným spôsobom, aby bola dosiahnutá maximálna efektívnosť.

V nasledujúcej časti s takýmto zámerom popíšeme jeden proces študijnej agendy do detailov, aby sme vedeli identifikovať a následne elektronizovať jeho jednotlivé časti. Obdobne by sme mohli postupovať aj pri ostatných procesoch nielen v študijnej, ale aj vo vedecko-výskumnej oblasti, v ktorej je Univerzita Komenského taktiež orgánom verejnej moci.

3.2 Správa dokladov o vzdelaní

V tejto časti sa budeme podrobnejšie venovať procesu vydávania a správy dokladov o vzdelaní v listinnom svete. Medzi tieto doklady zaraďujeme diplom, vysvedčenie o štátnej skúške a záznam o vydaní diplomu v matričnej knihe, pre jednoduchosť sa ďalej budeme venovať výlučne diplomom. Pre zvyšné dva doklady by sme mohli postupovať analogicky.

Zákon o e-Governmente stanovuje, akým spôsobom by Univerzita mala posielať diplomy - vyplnením a podpísaním elektronického formulára. To však zďaleka nepokrýva celú agendu vydávania diplomov, v rámci ktorej môžeme definovať viacero rolí a viacero krokov.

3.2.1 Životný cyklus diplomu

Na vydávaní a spravovaní diplomov sa podieľa viacero rolí:

- študijný referent (referent) - administratívny pracovník študijného oddelenia fakulty alebo univerzity,
- dekan - štatutár fakulty,
- rektor - štatutár univerzity,
- študent - osoba, ktorej je diplom vydávaný,
- autorita - overovateľ pravosti diplomu alebo jeho kópie (napríklad notár),
- tretia strana - osoba, ktorá si chce overiť platnosť diplomu (napríklad potenciálny budúci zamestnávateľ).

Samotný životný cyklus diplomu môžeme rozdeliť do niekoľkých častí. Pre každú časť popíšeme, aké roly sa na nej podieľajú, čo je vstupmi a výstupmi tejto časti procesu a za akých okolností prebieha.

1. **Vytvorenie diplomu**
   Vykonávateľom tejto činnosti je referent. Vstupmi sú údaje o študentovi a spôsob ich prezentovania (šablóna). Vysokoškolský diplom obsahuje niekoľko základných, povinných údajov, ktoré sú určené Zákonom o vysokých školách [1], a ďalšie údaje, ktoré definuje univerzita. Univerzita navyše určuje aj presné rozloženie údajov na diplome, teda jeho vizuálnu podobu. Referent transformuje dáta potrebné na tvorbu diplomu (napríklad informácie o študentovi alebo študijnom odbore) do vizuálnej podoby na základe jednej zo zvolených šablón. Výstupom tohto procesu je diplom v elektronickej podobe.

2. **Pridanie bezpečnostných prvkov**
   Túto činnosť vykonáva referent, dekan a rektor. Po vytvorení a kontrole diplomu je tento vytlačený na špeciálny papier s vodoznakom v tvare loga Univerzity. Následne je na diplom pridaných niekoľko bezpečnostných prvkov - reliéfna pečať v tvare štátneho znaku, pečať Univerzity a vlastnoručný podpis dekana a rektora Univerzity. Vstupom je teda elektronická verzia diplomu a výstupom finálna listinná podoba diplomu s bezpečnostnými prvkami.

3. **Archivácia diplomu**
   Po vytvorení diplomu je o ňom vytvorený záznam v matričnej knihe, ktorá je následne uložená v archíve. Túto činnosť vykonáva referent.

4. **Distribúcia diplomu**
   Diplom odovzdáva zástupca Univerzity (rektor, dekan) študentovi počas slávnostnej promócie. Ďalej je diplom vo vlastníctve študenta.

5. **Tvorba kópie alebo odpisu diplomu**
   Študent môže požiadať Univerzitu o tvorbu kópie alebo odpisu jemu vydaného diplomu, napríklad pre účely poskytnutia tretej strane. Kópiu alebo odpis vyhotoví referent, platnosť kópie potvrdí autorita.

6. **Overovanie diplomu**
   Tretia strana (napríklad zamestnávateľ alebo iná univerzita) môže požiadať o overenie platnosti doloženého diplomu. Pravosť kópie alebo odpisu diplomu si tretia strana overuje u autority (notára), platnosť originálu diplomu na Univerzite (u referenta).

3.3 Zhrnutie

V tejto kapitole sme identifikovali kľúčové procesy agendy Univerzity Komenského, ktoré bude potrebné na naplnenie Zákona o e-Governmente elektronizovať. Pre ich úspešnú informatizáciu bude potrebné vhodne prispôsobiť informačné systémy, zaškoliť ich používateľov a aktualizovať organizačné postupy pri jednotlivých procesoch.

Vybraný proces - proces spravovania dokladov o vzdelaní - sme zanalyzovali podrobne: popísali sme jeho časti z hľadiska funkcionalít a popísali spôsob ich spracovávania v listinnom svete. Z tejto analýzy budeme vychádzať v ďalších kapitolách, v ktorých navrhneme spôsob prenesenia tohto procesu do elektronického sveta, implementujeme a popíšeme modelové riešenie.

Tabuľka 3.1: Tabuľka znázorňuje procesy, ktoré na Univerzite Komenského prebiehajú počas životného cyklu študenta a typy dokumentov, ktoré vytvára študent alebo Univerzita v jednotlivých jeho krokoch.

Podanie prihlášky	
Študent	Prihláška na štúdium
Univerzita	Pozvánka na prijímacie konanie
Prijímacie konanie	
Študent	Odvolanie voči rozhodnutiu o neprijatí
Univerzita	Informácia o výsledku prijímacieho konania, Rozhodnutie o prijatí/neprijatí
Zápis do ročníka	
Študent	Potvrdenie účasti na zápise (návratka), Žiadosť o vydanie/predĺženie preukazu študenta, Potvrdenie účasti na školení o BOZP, Súhlas so spracovaním osobných údajov
Univerzita	Pozvánka na zápis, Platobný príkaz na platbu školného
Zápis predmetov, tvorba rozvrhu	
Študent	Žiadosť o uznanie predmetu, Žiadosť o odpustenie prerekvizity
Univerzita	Zmluva o štúdiu (súhlas so štúdiom predmetu inej fakulty), Potvrdenie o štúdiu, Protokol o študijnom pláne študenta
Udeľovanie štipendií	
Študent	Žiadosť o mimoriadne štipendium, Žiadosť o sociálne štipendium
Univerzita	Rozhodnutie o udelení štipendia
Mobility a zahraničné stáže	
Študent	Žiadosť o účasť na mobilite, Žiadosť o predĺženie mobility, Žiadosť o zrušenie mobility
Univerzita	Odporúčací list (mobilita), Rozhodnutie o udelenie grantu na mobilitu
Výučba, priebežné hodnotenie, skúškové obdobie	
Študent	Žiadosť o prerušenie štúdia, Žiadosť o zmenu študijného programu, Žiadosť o zmenu formy štúdia
Univerzita	Výkaz o hodnotení predmetov, Hodnotenie skúšky
Štátne skúšky, obhajoba práce	
Študent	Prihlásenie na štátne skúšky
Univerzita	Zadanie záverečnej práce, Posudok a hodnotenie záverečnej práce vedúceho a oponentov, Zápisnica zo štátnej skúšky
Udelenie titulu	
Študent	Žiadosť o kópiu diplomu
Univerzita	Vysvedčenie o štátnej skúške, Diplom, Záznam v matričnej knihe
Ukončenie štúdia	
Univerzita	Potvrdenie o vysporiadaní záväzkov študenta voči knižnici, Potvrdenie o prerušení štúdia, Potvrdenie o skončení štúdia

Kapitola 4

Koncept

V tejto kapitole nadviažeme na analýzu procesu vydávania diplomov v listinnom svete z časti 3.2 a navrhneme a popíšeme koncept systému pre elektronizáciu tohto procesu špecificky na Univerzite Komenského, berúc do úvahy jej ďalšie informačné systémy.

4.1 Životný cyklus elektronického diplomu

Cieľom informatizácie procesu z listinného sveta je zníženie počtu nutných krokov a rolí zapojených do procesu pri zachovaní rovnakej funkcionality. V nasledujúcej časti teda popíšeme model, v ktorom činnosti popísané v časti 3.2.1 prevedieme do elektronickej podoby.

Aj v elektronizovanej verzii procesu zachováme rovnaké roly - referent, dekan, rektor, študent, autorita a tretia strana. Zmení sa však typický predstaviteľ autority - tou už nebude notár, ale certifikačná autorita.

Diplomy budeme totiž narozdiel od analógovej verzie procesu vydávať, overovať a archivovať výlučne elektronicky, pričom elektronické budú aj ochranné prvky, ktoré budú diplomy niesť. Kľúčovou zmenou bude využitie kryptografie na vytváranie ochranných prvkov a overovanie platnosti diplomu.

Jednotlivé časti životného cyklu diplomu sa zmenia nasledujúcim spôsobom:

1. **Vytvorenie diplomu**
   Referent transformuje dáta z informačného systému s použitím niektorej zo šablón do elektronického dokumentu. Tento dokument podpíše svojím elektronickým podpisom, ktorým potvrdzuje, že údaje na diplome sú správne.

2. **Pridanie bezpečnostných prvkov**
   Diplom podpísaný referentom v ďalšom kroku podpíše svojím elektronickým podpisom dekan (ako zástupca fakulty) a následne rektor (ako zástupca univerzity). Reliéfna pečať a špeciálny papier sú vynechané vzhľadom na ich fyzický charakter. Oproti diplomu v listinnej podobe vynechávame aj pečiatku univerzity,

nakoľko certifikát verejného kľúča rektora univerzity obsahuje aj mandátny certifikát, ktorý potvrdzuje, že príslušná osoba je naozaj štatutárom univerzity.

3. **Archivácia diplomu**
   Podpísaný diplom je archivovaný v elektronickej podobe v na to určenej databáze (elektronickom archíve). Záznam v matričnej knihe nahradí elektronický záznam v archíve.

4. **Distribúcia diplomu**
   Elektronický diplom je študentovi zaslaný elektronicky do jeho elektronickej schránky. Okrem toho študent dostane prístup k úložisku diplomov, z ktorého má po úspešnej identifikácii a autentifikácii kedykoľvek možnosť získať svoje diplomy v elektronickej podobe.

5. **Tvorba kópie alebo odpisu diplomu**
   Nakoľko študent má elektronickú verziu svojho diplomu k dispozícii, nie je nutné vytvárať ďalšie kópie ani odpisy. Diplom je elektronicky podpísaný, čo eliminuje nutnosť potvrdzovania pravosti kópie u notára - jeho rolu tu preberá certifikačná autorita, ktorá vydala certifikát štatutárom univerzity, ktorí diplom podpísali.

6. **Overovanie diplomu**
   Keďže diplom je elektronicky podpísaný, jeho pravosť sa dá overiť bez pričinenia referenta vďaka použitej kryptografii. Pre overenie platnosti diplomu stačí overiť platnosť elektronického podpisu na diplome (princíp PKI sme popísali v časti 1.3). Okrem toho môžeme poskytnúť ďalšiu funkcionalitu - overenie diplomu online na webstránke univerzity. Ak tretia strana zadá správne identifikačné údaje diplomu, dostane podpísaný elektronický diplom. Výhodou tohto prístupu je, že namiesto posielania celého diplomu môže absolvent napríklad k žiadosti o zamestnanie priložiť len ID diplomu a odkaz na webstránku univerzity, pričom zamestnávateľ si ho môže v prípade záujmu overiť sám. To môže byť užitočné najmä vtedy, ak má zamestnávateľ veľa uchádzačov a uchádzači posielajú viacero diplomov. Vtedy sa zamestnávateľ môže rozhodovať napríklad podľa životopisov uchádzačov, a až v prípade záujmu si stiahne a overí vysokoškolské diplomy užšieho kruhu.

4.2 Návrh systému

V predošlej časti sme popísali systém elektronickej správy diplomov z hľadiska funkcionality. V tejto časti sa na systém pozrieme zvnútra - popíšeme, z akých častí by sa mal skladať a ako by tieto časti mali navzájom komunikovať.

4.2.1 Hlavné časti systému

Pre kompletnú elektronizáciu procesu spracovania diplomov je potrebné zabezpečiť spoluprácu viacerých informačných sytémov. Ide o existujúce systémy Univerzity Komenského, moduly podľa Zákona o e-Governmente a nové moduly pre správu elektronických diplomov.

Prvou kategóriou sú **moduly na identifikáciu a autentifikáciu**. Pod týmto pojmom myslíme Jednotný autentifikačný systém Univerzity Komenského (JAS), ktorý v súčasnosti zabezpečuje identifikáciu a autentifikáciu študentov, zamestnancov a absolventov Univerzity pomocou takzvaného univerzitného loginu. V zmysle Zákona o e-Governmente však bude na autentifikáciu nutné používať aj iný autentifikátor - občiansky preukaz s čipom (eID)[1].

Ďalšie moduly budú slúžiť na **archiváciu** elektronických diplomov. Pôjde predovšetkým o elektronický archív Univerzity Komenského, ale aj modul dlhodobého uchovávania podľa Zákona o e-Governmente. Tak ako v predošlom prípade, ani elektronický archív Univerzity Komenského zatiaľ nebol zriadený, pre jej správne fungovanie v elektronickom svete to však bude nevyhnutné.

Zdrojom údajov pre tvorbu diplomov budú **databázy Univerzity**, najmä Akademický informačný systém Univerzity Komenského (AiS), ktorý obsahuje údaje o študijných programoch, študentoch a ich výsledkoch, ale aj Centrálna databáza osôb (CDO), ktorá obsahuje informácie o zamestnancoch a ich rolách (napríklad rozlíšenie medzi dekanom, rektorom, referentom a inými zamestnancami).

Novovytvorenými modulmi v rámci popisovaného konceptu budú **modul na vytváranie diplomov** a **modul na overovanie diplomov**. Modul pre vytváranie diplomov bude slúžiť na vytvorenie diplomu a pridanie bezpečnostných prvkov. Pomocou modulu na overovanie diplomov bude môcť študent získať elektronickú verziu svojho diplomu a tretia strana bude môcť overiť jeho platnosť.

Modul elektronických schránok podľa Zákona o e-Governmente bude slúžiť ako alternatívne komunikačné rozhranie k modulu na overovanie elektronických diplomov, aby bolo možné odpovedať na prípadné elektronické žiadosti o vydanie kópie/odpisu diplomu alebo potvrdenie jeho pravosti.

4.2.2 Interakcia medzi hlavnými časťami systému

V tejto časti popíšeme spôsob výmeny údajov medzi jednotlivými časťami systému pre správu diplomov, ktorý je graficky znázornený na obrázku 4.1.

[1]Zabezpečeniu transformácie oboch spomínaných autentifikátorov sa vo svojom ročníkovom projekte venuje Lukáš Kiss, KI, FMFI UK

Modul na autentifikáciu Autentifikačný modul bude komunikovať rovnako s modulom pre vytváranie aj overovanie diplomov a bude zabezpečovať identifikáciu a autentifikáciu používateľov.

Modul na archiváciu Do modulov na archiváciu budú exportované údaje z modulu pre vytváranie diplomov po ich úspešnom vytvorení a podpísaní. Naopak, údaje z tohto modulu budú použité pri overovaní diplomu pomocou overovacieho modulu.

Modul elektronických schránok Podľa Zákona o e-Governmente sa komunikácia medzi orgánmi verejnej moci a občanmi má realizovať predovšetkým pomocou elektronických správ, preto treba počítať aj s prípravou systému na komunikáciu s modulom elektronických schránok pre možnosť automatizovaného spracovania prípadných elektronických podaní súvisiacich s diplomami.

Databázy údajov Databázy budú primárnym zdrojom údajov pre modul vytvárania diplomov. Odtiaľ budú čerpané údaje o študentoch, študijných programoch, šablóny pre vytvorenie diplomu. Budú sa tiež získavať údaje o rolách jednotlivých osôb, keďže navrhovaný systém rozoznáva viacero rolí používateľov a bude potrebné riešiť aj autorizáciu. Naopak, aj modul pre vytváranie diplomov môže byť aj zdrojom údajov pre databázy, a to v prípade identifikovania chýb v údajoch potrebných na vytvorenie diplomu.

4.2.3 Funkcie systému

V systéme budeme rozoznávať 5 rolí používateľov, ktoré vychádzajú z našej analýzy agendy spracovávania diplomov z kapitoly 3. K jednotlivým rolám sú priradené rôzne spôsoby interakcie so systémom.

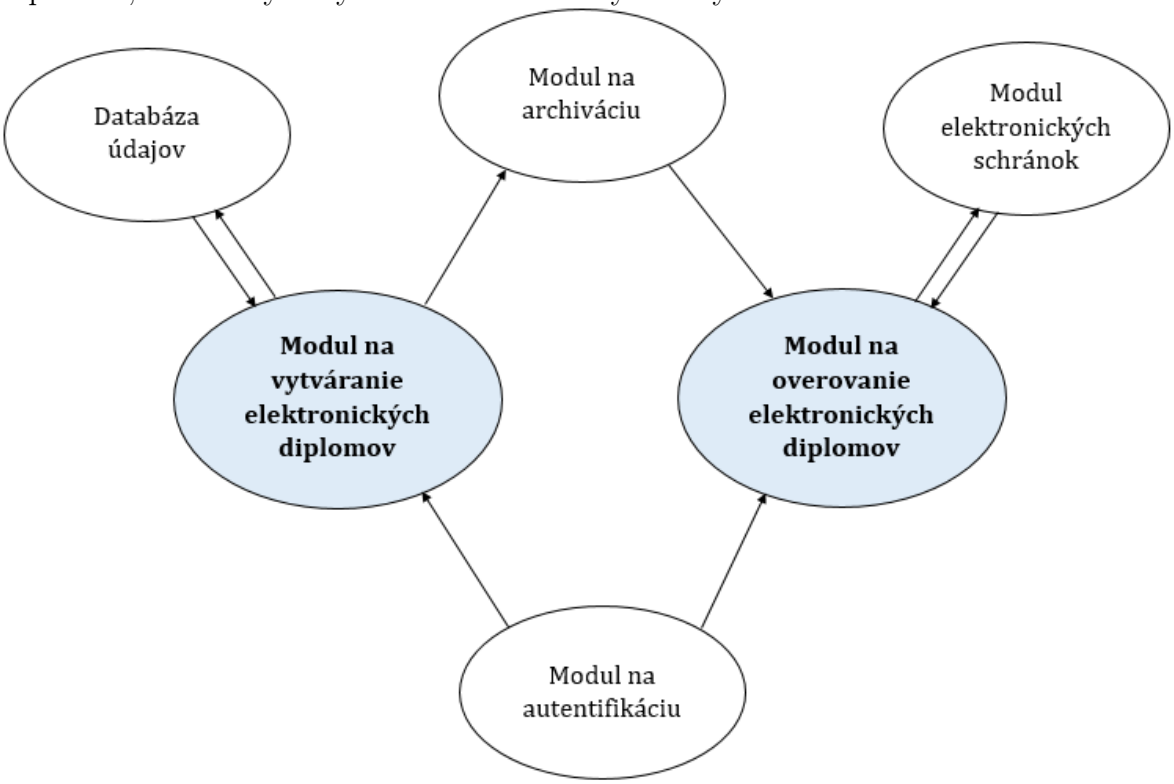
Študent má po autentifikácii prístup k modulu na overovanie diplomov. Pomocou tohto modulu môže zobraziť všetky svoje doteraz získané diplomy a získať ich v elektronickej podobe.

Tretia strana má bez autentifikácie prístup k modulu na overovanie diplomov. Môže zadať identifikačné údaje konkrétneho diplomu, overiť jeho platnosť a stiahnuť si ho v elektronickej podobe.

Referent má po autentifikácii a autorizácii prístup k modulu na vytváranie diplomov. Referent vytvorí diplomy pomocou zvolenia vhodných údajov a šablóny z informačného systému. Po kontrole tieto diplomy elektronicky podpíše, čím sa zaručuje za ich správnosť.

Dekan má po autentifikácii a autorizácii prístup k modulu na vytváranie diplomov, kde môže vidieť všetky diplomy podpísané referentom, ktoré sú určené pre študentov

Obr. 4.1: Obrázok ilustruje informačné systémy zapojené do tvorby elektronických diplomov, a smer výmeny informácií medzi týmito systémami.



jeho fakulty. Dekan tieto diplomy buď podpíše svojím elektronickým podpisom, alebo zamietne.

Rektor má po autentifikácii a autorizácii prístup k modulu na vytváranie diplomov, kde môže vidieť všetky diplomy podpísané dekanom. Rektor tieto diplomy buď podpíše svojím elektronickým podpisom, alebo zamietne.

Diplom teda vytvára referent a po podpísaní referentom, dekanom a rektorom ho môže zobraziť študent, pre ktorého bol diplom vydaný, alebo tretia strana, pokiaľ sú jej známe identifikačné údaje diplomu.

4.3 Zhrnutie

V tejto časti sme popísali náš koncept pre elektronickú verziu spracovávania diplomov. Popísali sme roly a oprávnenia, možné funkcionality systému a jeho hlavné časti. V ďalších kapitolách popíšeme našu modelovú implementáciu tohto konceptu a zhrnieme možné nedostatky a vylepšenia navrhovaného konceptu.

Kapitola 5

Modelové riešenie

V tejto kapitole popíšeme naše modelové riešenie pre vydávanie diplomov elektronicky. V prvej časti sa zameriame na technické detaily implementácie, v ďalších popíšeme jej nedostatky a úlohy, na ktoré bude treba myslieť pri implementácii v reálnom prostredí.

5.1 Detaily implementácie

Naša modelová implementácia vychádza z konceptu na správu elektronických diplomov popísaného v kapitole 4, preto zachováva navrhnuté roly aj funkcionalitu sytému.

Hlavnou časťou systému je webstránka napísaná v jazykoch PHP a JavaScript. Rozdiel v implementácii oproti konceptu je v tom, že modul na vydávanie a modul na overovanie diplomov sú v modelovej implementácii zlúčené do jedného, pričom namiesto komunikácie s ostatnými časťami (modul na archiváciu, databáza údajov...) webstránka komunikuje so svojou databázou (MySQL), ktorá simuluje zvyšné informačné systémy.

Obsahom databázy sú také údaje, ktoré moduly na vytváranie a overovanie diplomov budú potrebovať z iných informačných systémov, teda:

- informácie o používateľoch - meno, priezvisko, rola (študent, referent, dekan, rektor) a obdobie, počas ktorého túto rolu majú priradenú (simulácia CDO),
- zoznam fakúlt (simulácia AiS),
- zoznam šablón pre diplomy (simulácia AiS),
- zoznam už vytvorených a podpísaných diplomov (simulácia archívu).

Na webstránku majú prístup autentifikovaní aj neautentifikovaní používatelia. Používatelia bez autentifikácie (ktorí predstavujú rolu *tretia strana*) môžu využiť možnosť **OVERIŤ DIPLOM.** Na podstránke sa zobrazí formulár, do ktorého treba zadať meno a priezvisko držiteľa diplomu a jeho unikátny identifikátor. Pokiaľ tieto údaje korešpondujú so záznamom v databáze diplomov, vypíšu sa základné údaje o diplome

(držiteľ diplomu, rok vydania a fakulta). K dispozícii na stiahnutie je plná verzia diplomu s digitálnymi podpismi potvrdzujúcimi jeho pravosť. Túto funkcionalitu ilustruje obrázok 5.1.

Obr. 5.1: Overenie diplomu. Pokiaľ tretia strana zadá správne identifikačné údaje, aplikácia overí platnosť im zodpovedajúceho diplomu. Ak bol diplom vydaný, poskytne ho na stiahnutie.

Na prácu s ďalšími časťami systému je potrebná identifikácia a autentifikácia. Tá je realizovaná zadaním používateľského mena a hesla. Používateľské mená a SHA-256 digitálne odtlačky hesla sú uložené v databáze.

Prihlásený používateľ, ktorý má rolu študent (teda je aktuálne študentom alebo už absolventom univerzity) má navyše možnosť **ZOBRAZIŤ MOJE DIPLOMY**. Na tejto podstránke sa študentovi zobrazí náhľad všetkých diplomov, ktoré mu boli vydané v minulosti - názov fakulty a rok vydania. Ukážku tohto výpisu nájde čitateľ na obrázku 5.2. Po kliknutí na príslušnú ikonu si študent môže stiahnuť plnú verziu diplomu.

Študijný referent môže využiť možnosť **VYTVORIŤ DIPLOM**. Po nahraní XML súboru s údajmi pre vytvorenie diplomov a zvolení jednej zo šablón vo formáte XSLT server vykoná nasledujúce kroky:

- parsuje XML súbor a vyberie z neho identifikátor pre každý diplom, jeho držiteľa, fakultu a rok vydania,
- zo súborov s dátami (XML) a šablónou (XSLT) vytvorí súbory vo formáte PDF,
- uloží záznamy o vytvorených diplomoch do databázy.

Po úspešnom vykonaní týchto krokov server informuje o výsledku referenta, tak ako je to znázornené na obrázku 5.3.

XML súbor s údajmi pre vytvorenie diplomu vznikne exportom z informačného systému, v ktorom sú tieto údaje uložené (v našom prípade AiS, to sa však v budúcnosti

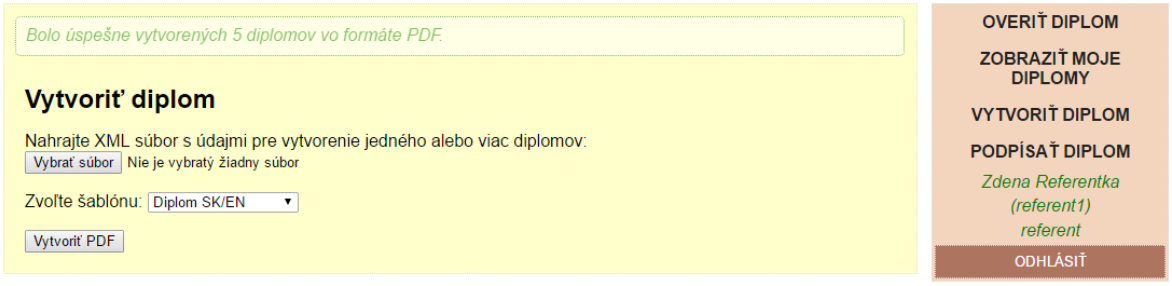
Obr. 5.2: Zobrazenie diplomov študenta. Aplikácia vypíše všetky diplomy, ktoré boli študentovi vydané, pričom študent si ich môže stiahnuť v elektronickej podobe.

môže zmeniť). Šablóny sú súbory, ktoré popisujú, ktoré údaje sa majú na výslednom diplome zobraziť a ako majú byť rozložené.

Na transformáciu týchto súborov do formátu PDF sme použili externý program Apache ™ FOP [6].

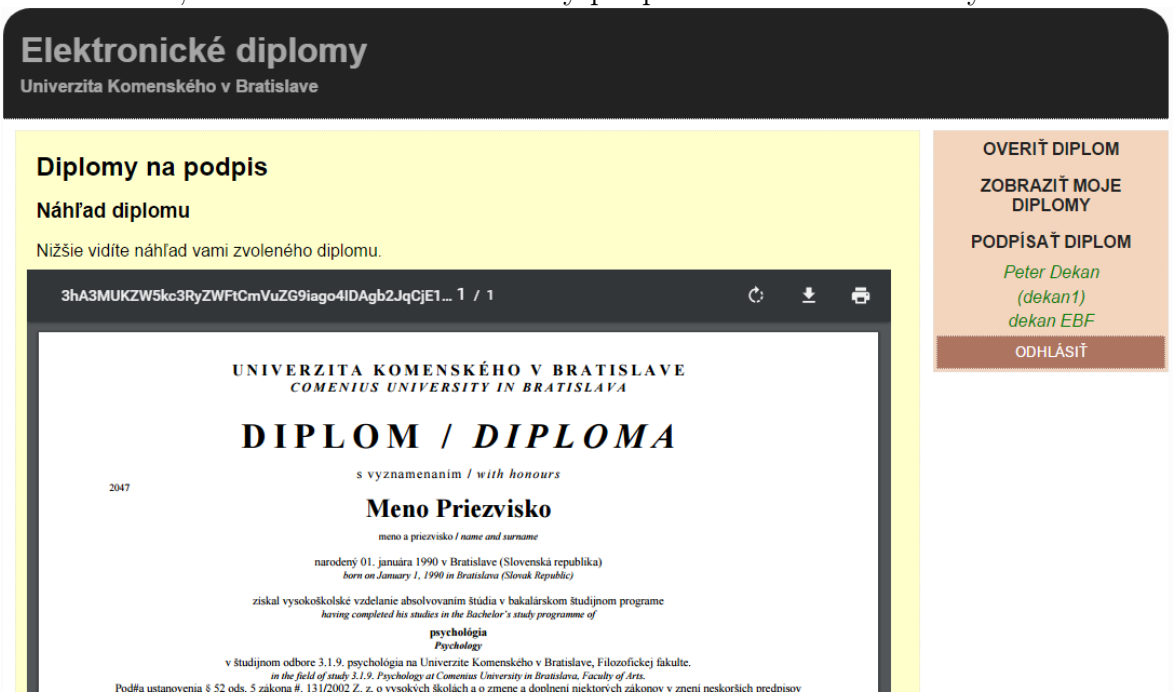
Takto vytvorené diplomy majú v databáze priradený stav 3, t.j. diplom bol vytvorený, avšak nie podpísaný. Tieto diplomy sa nezobrazia študentovi ani tretej strane pri výpise diplomov, resp. pri overovaní vydaných diplomov, nakoľko ešte nejde o finálne verzie diplomov.

Obr. 5.3: Vytvorenie diplomov. Referent má možnosť vytvoriť diplomy vo formáte PDF z importovaných dát a zvolenej šablóny.



Používatelia s rolou referent, dekan a rektor majú navyše možnosť **PODPÍSAŤ DIPLOM**. Na tejto podstránke používateľ vidí zoznam a základné informácie o všetkých diplomoch, ktoré má podpísať. S týmito diplomami môže vykonať niekoľko akcií - zobraziť ich náhľad, zamietnuť podpísanie a odstrániť diplom alebo ho elektronicky podpísať. Tieto činnosti sa dajú robiť buď jednotlivo, alebo pre viaceré diplomy súčasne. Ukážku tejto funkcionality ilustrujú obrázky 5.4 a 5.5. Podpísaním diplomu sa zníži jeho stav o 1 (t.j. 2 - podpísaný referentom, 1 - podpísaný dekanom, 0 - podpísaný rektorom a platný).

Obr. 5.4: Náhľad diplomu. Referent, dekan a rektor majú možnosť zobraziť diplom a rozhodnúť sa, či ho schvália a elektronicky podpíšu alebo zamietnu a vymažú.



Referent vie zobraziť a upravovať všetky diplomy, ktoré predtým vytvoril on alebo iný referent možnosťou VYTVORIŤ DIPLOM. Dekan má prístup k tým diplomom, ktoré sú určené pre študentov „jeho“ fakulty a ktoré už boli podpísané referentom. Rektor vie pristupovať ku všetkým diplomom, ktoré už boli podpísané referentom aj dekanom. Táto schéma je znázornená na obrázku 5.6.

Na tvorbu elektronického podpisu sme použili knižnicu PDFsign.js pre JavaScript [8]. Podpis vytvára používateľ (referent, dekan, rektor) tak, že vyberie diplomy, ktoré chce podpísať, zvolí súbor formátu P12 so svojím súkromným kľúčom a certifikátom verejného kľúča a zadá prístupové heslo k tomuto súboru.

Po vytvorení podpisu sa podpísaný dokument odošle na server a zmení sa stav diplomu v databáze podľa vyššie spomínanej schémy 5.6.

Pri implementovaní webstránky a vytváraní ilustračných obrázkov sme použili ikony z online zdrojov [10], [11], [12], [16], [19], [20].

5.2 Potrebné rozšírenia implementácie

Naša modelová implementácia slúži len na demonštrovanie funkcionality a identifikovanie kľúčových problémov spojených s implementáciou takéhoto systému, preto má nutne mnohé nedostatky, či už ide o funkcionalitu alebo bezpečnosť. V tejto časti popíšeme kľúčové problémy modelovej implementácie a pomenujeme tie časti, ktoré bude potrebné v reálnom systéme vyriešiť inak.

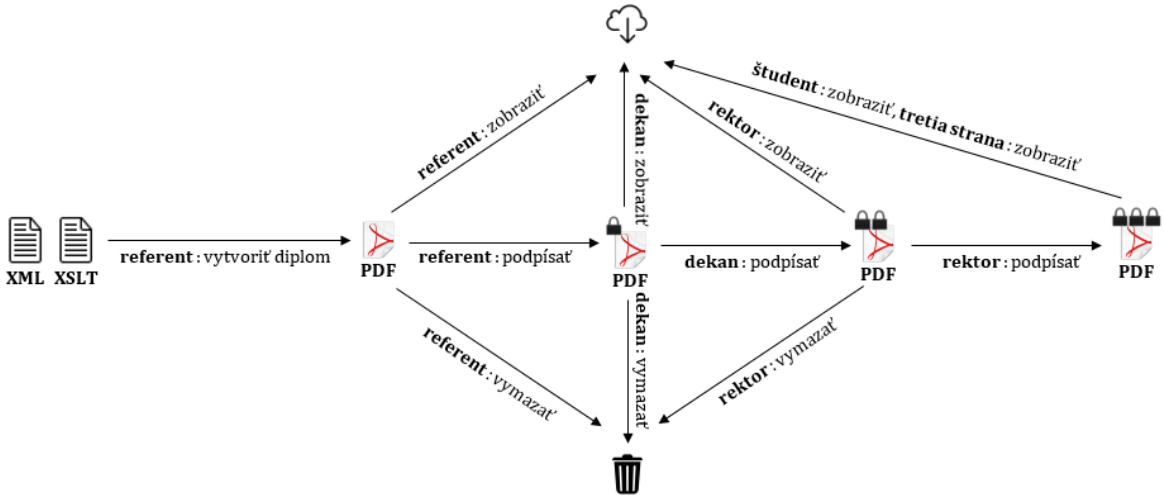
Obr. 5.5: Podpísanie diplomu. Referent, dekan a rektor vytvárajú elektronický podpis zvolením diplomu, súboru s ich súkromným kľúčom a certifikátom verejného kľúča a zadaním hesla k súboru.

Viaceré problémy súvisia s používaním simulovaného prostredia. Rôzne časti systému budú v reálnom prostredí namiesto jednej databázy komunikovať s viacerými informačnými systémami, preto sa zmení spôsob vyhodnocovavnia požiadaviek. V niektorých prípadoch ide o systémy, ktoré v súčasnosti ešte neexistujú a bude potrebné ich vyvinúť, čo je jedným z dôvodov, prečo sa v ukážkovom riešení nevyskytujú.

5.2.1 Identifikácia a autentifikácia

Naša aplikácia na identifikáciu a autentifikáciu používa jednoduché zadanie prihlasovacieho mena a hesla. V reálnom prostredí by mala využívať už existujúci autentifikačný systém Univerzity Komenského (JAS). Tento však podľa Zákona o e-Governmente bude potrebné rozšíriť o možnosť identifikácie a autentifikácie pomocou občianskeho preukazu s čipom, teda pripojením čítačky kariet s eID a zadaním BOK. Transformácia týchto dvoch spôsobov autentifikácie je jednou z požiadaviek vyplývajúcich zo Zákona o e-Governmente, ktoré sme popísali v časti 2.2.

Obr. 5.6: Stavy diplomu. Obrázok ilustruje všetky možné stavy diplomu od jeho vytvorenia až po podpísanie rektorom a vydanie. Šípka medzi dvomi stavmi diplomu zobrazuje možnosť prechodu medzi týmito stavmi, pričom text nad šípkou špecifikuje rolu, ktorá má oprávnenie na prevedenie diplomu zo zdrojového do cieľového stavu a činnosť, ktorou tento prechod vie zrealizovať.



5.2.2 Import dát z informačných systémov

Na vytvorenie nových diplomov naša aplikácia vyžaduje ručný import údajov o diplomoch vo forme XML. Takýto súbor je síce v súčasnosti možné získať exportom z Akademického informačného systému, takže ide o funkčnú možnosť, v reálnom systéme by však takýto ručný import dát bol nielen nepraktický, ale predstavoval by aj určité bezpečnostné riziko, nakoľko by nebolo možné overiť integritu importovaných dát a bolo by možné vytvoriť ľubovoľný diplom.

Navyše, vytvorenie PDF z XML súborov je v našej aplikácii realizované externým programom, pričom v reálnom modeli by sa oň mal postarať samotný systém. V súčasnosti takúto funkcionalitu poskytuje aj AiS. My sme sa pre vlastnú transformáciu súborov XML a XSLT do formátu PDF rozhodli preto, aby sme mali prístup k zdrojovým dátam o diplome v štruktúrovanej forme. Zo súboru vo formáte XML totiž získavame dôležité údaje - identifikátor diplomu, fakulty a študenta, ktorému je vydávaný, aby sme s nimi mohli ďalej pracovať.

Na párovanie diplomu so študentom sme použili údaje z metadát k diplomu získaným z Akademického informačného systému, konkrétne hodnotu *liveID* alebo takzvaný *univerzitný login*. Nakoľko sme nepoznali presnú štruktúru dát z tohto systému (a nemusí ísť teda o povinný údaj), v reálnej implementácii by sme odporúčali využiť na priradenie diplomu k študentovi napríklad jednoznačný identifikátor UOČ (univerzitné číslo študenta), ktorý je identifikátorom študenta do Centrálnej databázy osôb, kde sú o študentovi k dispozícii aj ďalšie údaje.

5.2.3 Pridanie bezpečnostných prvkov na diplom

Na vytváranie elektronického podpisu sme v modelovom riešení použili súkromný kľúč a certifikát verejného kľúča, ktoré sme vygenerovali programom OpenSSL (zvolili sme možnosť 1024-bitového RSA kľúča). V samotnom systéme sme sa nezaoberali vydávaním certifikátov a distribúciou kľúčov, keďže predpokladáme, že v reálnom systéme sa na tvorbu elektronického podpisu použije občiansky preukaz s čipom. O vydávanie certifikátov pre eID, rovnako ako o distribúciu eID, sa postará Ministerstvo vnútra Slovenskej republiky.

5.2.4 Alternatívne komunikačné rozhrania

V našom riešení pripúšťame len jeden možný spôsob prístupu absolventov a tretích strán k vydaným diplomom - prostredníctvom na to určenej webstránky. V reálnom systéme k tomuto spôsobu bude potrebné pridať aj ďalšie rozhranie, a to modul elektronických schránok. Podľa Zákona o e-Governmente by Univerzita Komenského mala vedieť odpovedať na požiadavky občanov doručené do jej elektronickej schránky, pričom takou požiadavkou môže byť aj poslať „kópiu“ alebo „odpis“ diplomu (táto terminológia má význam len pre diplomy v listinnom svete, v tom elektronickom by, samozrejme, išlo o ten istý elektronicky podpísaný dokument). Systém preto bude potrebné vhodne prepojiť aj s modulom elektronických schránok.

Nie je však jasné, ako bude fungovať posielanie diplomov pomocou modulu elektronických schránok. Podľa Zákona o e-Governmente by elektronický dokument mal vzniknúť vyplnením príslušného elektronického formulára z modulu elektronických formulárov. Avšak, každá univerzita má na diplomy niekoľko vlastných šablón a každá môže definovať rôzne údaje, ktoré diplom obsahuje a rozloženie údajov na týchto diplomoch, čo by v konečnom dôsledku mohlo znamenať priveľké množstvo elektronických formulárov.

Prijateľnejšou možnosťou by preto mohlo byť vytvorenie a používanie elektronického formulára, ku ktorému bude možné pripojiť ako prílohu už hotový a podpísaný diplom vo formáte PDF vytvorený internými systémami univerzity.

5.2.5 Archivácia diplomov

V modelovej implementácii systému používame na archiváciu diplomov vlastnú databázu. Toto bude potrebné rozšíriť o ukladanie v elektronickom archíve UK (ktorý bude potrebné zriadiť), prípadne v module dlhodobého uchovávania podľa Zákona o e-Governmente.

5.3 Nedostatky a chýbajúca funkcionalita

V tejto časti popíšeme ďalšie nedostatky, ktoré má naša implementácia a navrhneme spôsob ich odstránenia v budúcom reálnom systéme.

5.3.1 Nesprávne kódovanie údajov

V našom riešení sa vyskytujú dva nedostatky súvisiace s nesprávnym kódovaním údajov. Jedným z nich je nesprávne zobrazená diakritika pri generovaní diplomu z formátov XML a XSLT do formátu PDF. Toto je spôsobené nesprávnou konfiguráciou externého programu, ktorý túto transformáciu vykonáva (zvolený font nepodporuje niektoré symboly).

Druhým problémom môže byť nesprávne kódovanie údajov v databáze. To je v našom modelovom riešení nastavené na slovenčinu, a teda by mohlo spôsobiť nesprávne zobrazenie napríklad mien zahraničných študentov. Predpokladáme však, že tento problém je správne vyriešený v už existujúcich informačných systémoch Univerzity, najmä CDO a JAS, ktoré obsahujú údaje o menách osôb, preto by v reálnych podmienkach pri správnej spolupráci existujúcich systémov mal byť tento problém eliminovaný.

5.3.2 Nekonfigurovateľnosť systému

V našom modelovom riešení nepripúšťame možnosť opravovania chýb vo vygenerovanom diplome. Takýto diplom je možné len podpísať alebo zahodiť, pričom zmenu údajov v ňom môžeme dosiahnuť len tak, že opravíme údaje v AiSe a následne do systému na vytváranie diplomov importujeme už opravené údaje. V reálnom riešení je možné pridať do systému možnosť opravovania chybných údajov, je však nutné, aby sa tieto údaje zároveň opravili aj v AiSe - zdrojovom informačnom systéme pre vytváranie diplomov, aby sa predišlo možným nekonzistentnostiam.

V modelovom riešení tiež nie je možnosť dodefinovania ďalších osôb, fakúlt, šablón pre diplomy a podobne. Hoci takáto možnosť sa javí ako dôležitá, v reálnom systéme všetky tieto údaje bude systém získavať z iných systémov a nie zo svojej internej databázy, preto sme túto možnosť nepripustili ani teraz a predpokladáme, že nami používaná databáza je len simuláciou spomínaných systémov, ku ktorým by modul na správu diplomov mal mať len read-only prístup.

5.3.3 Pohľad používateľa

V našom modelovom riešení sme sa sústredili najmä na demonštráciu funkcionality, a to aj na úkor ďalších aspektov implementácie.

Nekládli sme veľký dôraz na grafické rozhranie ani príjemnú ovládateľnosť používateľmi systému. Preto napríklad pri prezeraní diplomov určených na podpis sú všetky položky vypísané v jednom zozname, bez možnosti filtrovania alebo zoradzovania podľa rôznych kritérií (podľa ročníkov, študijných odborov...), možnosti prezerania viacerých diplomov pred podpisom ako v galérii či rozdelenia zoznamu na viacero strán.

Na implementáciu sme používali len jednoduché technológie - PHP a JavaScript - bez pokročilejších metód a frameworkov, hoci posielanie požiadaviek cez formuláre a neustále obnovovanie stránky môže byť používateľsky menej príjemné.

Keďže naše riešenie slúžilo len ako pomôcka na demonštrovanie funkcionality, nezaoberali sme sa jeho efektivitou, takže čas vykonania jednotlivých operácií môže presiahnuť únosnú mieru (napríklad vytváranie väčšieho počtu diplomov naraz).

V reálnej implementácii bude však potrebné myslieť aj na pohľad používateľa, preto dávame do pozornosti aj tieto námety na vylepšenie.

5.4 Bezpečnosť systému

Osobitnou stránkou implementácie systému pre vydávanie a správu diplomov je splnenie bezpečnostných požiadaviek, ktoré sme popísali v kapitole 1:

- integrita systému - znemožniť vytvorenie ľubovoľného diplomu oprávnenou aj neoprávnenou osobou a znemožniť nesprávne vyhlásenie neplatného alebo neexistujúceho diplomu za právoplatne vydaný,
- dôvernosť údajov - znemožniť prístup neoprávnených osôb k diplomu v stave, na prístup ku ktorému nemajú oprávnenie,
- dostupnosť systému - zabezpečiť možnosť prístupu oprávnených používateľov rovnako k modulu na vytváranie, ako aj modulu na overovanie diplomov,
- autentickosť diplomov - zabezpečiť, že k vydaným diplomom bude možné jednoznačne a nespochybniteľne priradiť Univerzitu Komenského a jej štatutárov, ktorí diplom podpísali.

V našom modelovom riešení sme implementovali len niekoľko základných bezpečnostných opatrení, implementácia reálneho systému si však bude vyžadovať vypracovanie a aplikovanie *bezpečnostného projektu*, teda dôkladnú analýzu systému z hľadiska bezpečnosti, navrhnutie a použitie bezpečnostných opatrení na zabezpečenie spomínaných bezpečnostných požiadaviek.

Na zabezpečenie dôvernosti a integrity je nutný spoľahlivý mechanizmus na identifikáciu a autentifikáciu používateľov. Náš systém podporuje len jednoduché prihlasovanie pomocou mena a hesla, a hoci heslo neprenášame po sieti ako otvorený text, ale len jeho

digitálny odtlačok, autentifikačný modul reálneho systému bude musieť implementovať pokročilejšie bezpečnostné mechanizmy.

Aby sme znemožnili neoprávneným osobám pristupovať k existujúcim vydaným diplomom, pri sťahovaní dokumentov (v možnostiach ZOBRAZIŤ MOJE DIPLOMY a OVERIŤ DIPLOM) nie je k dispozícii priamy link na umiestnenie dokumentu, ale kliknutie na odkaz spôsobí odoslanie dokumentu prehliadaču vo forme surových dát. Rovnako pri možnosti OVERIŤ DIPLOM nezverejníme diplom, pokiaľ používateľ nezadá spolu s menom a priezviskom aj jeho identifikačné číslo, čo znemožní jednoduché enumerovanie vydaných diplomov bez znalosti špecifických údajov.

Aby sme predišli neoprávnenému získaniu diplomu, na ktorý nemáme nárok (t.j. jeho držiteľ nám neposlal jeho identifikačné údaje a nedal nám tým právo naň nahliadnuť), bude v reálnom systéme potrebné, aby bol identifikátor diplomu dostatočne dlhý a aby sa tak predišlo možnému útoku hrubou silou (skúšaním všetkých možných identifikátorov s daným menom absolventa). Okrem toho bude nutné zabezpečiť, aby prideľovanie identifikátorov diplomov nebolo predvídateľné, teda aby jednotlivé identifikačné čísla nenasledovali sériovo za sebou.

Kľúčovou požiadavkou na systém je zabezpečenie jeho integrity. V tomto ohľade má naše modelové riešenie viacero rezerv. V modelovom riešení sme pre jednoduchosť používali len jednu databázu na ukladanie všetkých údajov. Rovnako sme zlúčili funkcionalitu vytvárania a overovanie diplomov do jedného modulu.

V reálnom systéme bude nevyhnutné jednotlivé časti striktne oddeliť. Modul na vytváranie diplomov by mal byť kvôli bezpečnosti prístupný len v rámci internej siete Univerzity, pričom cez Internet by mal byť prístupný len modul na overovanie diplomov.

Alternatívnou možnosťou realizácie dvoch hlavných modulov by mohlo byť vytvorenie modulu na overovanie diplomov ako webstránku a modul na vytváranie diplomov ako lokálnu aplikáciu. Výhodou by bolo, že hoci ostatné súčasti modulu budú prístupné cez Internet (AiS, CDO, archív), s vytváraním diplomov by sme mohli pracovať v chránenom prostredí. Nevýhodou je komplikovaná správa inštalácií potrebnej aplikácie na počítačoch všetkých zúčastnených, ktorí budú potrebovať s modulom pracovať, rovnako ako aj technické komplikácie (dvojitá autentifikácia v aplikácii aj v ostatných systémoch, prenos údajov medzi aplikáciou a databázami).

Modul na overovanie diplomov by mal mať k archívu len read-only prístup, pričom len z modulu na vytváranie diplomov by malo byť možné do archívu zapisovať. Dôležité je aj oddelenie rôznych databáz (študentov, diplomov), predpokladáme však, že toto bude vyriešené automaticky rozdelením funkcionalít medzi rôzne systémy, ktoré budú navzájom komunikovať (autentifikačné moduly, CDO, archív...).

Okrem použitia silných kryptografických algoritmov a protokolov bude potrebné zaistiť bezpečnú (šifrovanú) komunikáciu medzi jednotlivými časťami systému. V na-

šej implementácii sa napríklad dáta pre vytvorenie nového diplomu získavajú ručným importom, čo poskytuje viaceré možnosti manipulácie s ich obsahom. Toto vyrieši zabezpečené spojenie medzi databázou a modulom na vytváranie diplomov.

Ďalšia kontrola v našom modelovom riešení chýba pri samotnom podpisovaní diplomu. Systém sa spolieha na to, že používateľ (referent, dekan, rektor) na podpisovanie použije svoj súkromný kľúč, tento podpis však neoveruje a nekontroluje, či certifikát naozaj patrí deklarovanej osobe. Systém síce vytvára záznamy (logy) o všetkých dôležitých operáciách, ktoré v ňom prebehnú, do databázy však ukladá podpísané dokumenty bez ich kontroly.

Navyše, v modelovom riešení nepoužívame najvyššiu úroveň elektronického podpisu, keďže používateľovi je známy jeho súkromný kľúč. Ten sa síce po sieti neprenáša, keďže podpisovanie sa realizuje na strane klienta, avšak je známy jeho vlastníkovi, ktorý by ho mohol kompromitovať.

Tento problém bude v praxi vyriešený tým, že na podpisovanie bude použitý eID a čítačka kariet, ktorým sa používateľ autentifikuje a použije ho na vytvorenie elektronického podpisu. Systém bude poznať verejný kľúč príslušného používateľa, a bude tak môcť podpis overiť. Zároveň vlastník eID nebude vedieť zistiť svoj súkromný kľúč.

Na overenie integrity diplomu by sme mohli pridať ďalšiu kontrolu - pri overovaní diplomu sa naše modelové riešenie rovnako spolieha na správnosť údajov v databáze. Mohli by sme však pridať ďalšiu kontrolu všetkých podpisov prítomných na diplome, a to ešte pred tým, ako diplom označíme za vydaný a platný.

Ďalšou požiadavkou, ktorá nielen súvisí s bezpečnosťou, ale zabezpečuje aj korektnosť systému, je atomickosť operácií - teda vlastnosť, kedy každá operácia sa buď vykoná kompletne, alebo sa nevykoná vôbec. Ani toto od nášho modelového riešenia nemožno očakávať, bude to však nevyhnutné v budúcej reálnej implementácii.

5.5 Zhrnutie

V tejto kapitole sme popísali hlavné časti nášho modelového riešenia a hlavné problémy, ktoré sme identifikovali pri jeho implementácii a ktoré bude potrebné v reálnom prostredí vyriešiť. Špeciálne sme sa venovali bezpečnostným požiadavkám na systém, keďže tento pracuje s citlivými dátami a jeho kompromitácia by mohla mať ďalekosiahle následky.

Kapitola 6

Diskusia

V predošlých kapitolách sme popísali nutnosť informatizácie procesov na Univerzite Komenského a navrhli a implementovali sme koncept na správu elektronických diplomov. Výhodami tohto riešenia je predovšetkým zefektívnenie, zrýchlenie procesu a zvýšenie jeho bezpečnosti.

V kapitole 5 sme okrem technických detailov modelovej implementácie poskytli aj výpočet jej hlavných nedostatkov a návrhov na vylepšenie. V tejto kapitole sa, podobne, budeme venovať možným nedostatkom a otvoreným otázkam, avšak budeme sa zaoberať konceptom samotným, pričom abstrahujeme od implementačných detailov.

Popíšeme možné slabé miesta nami navrhnutého konceptu a navrhneme možné riešenia pre problémy a otázky, ktoré sa ho týkajú, ale na ktoré doposiaľ nepoznáme odpoveď.

6.1 Návrhy na vylepšenia a rozšírenia konceptu

V tejto časti popíšeme možné vylepšenia alebo iné riešenia niektorých čiastkových problémov, s ktorými sme sa stretli pri navrhovaní konceptu na správu diplomov.

6.1.1 Pridanie filtrov na vyhľadávanie diplomov

Modul na overovanie diplomov by okrem možnosti overenia konkrétneho diplomu mohol poskytovať možnosť vyhľadávania v diplomoch vydaných univerzitou v minulosti. Túto funkcionalitu v súčasnosti poskytuje webstránka univerzity. Verejnosť by si pomocou tohto modulu mohla vyhľadať absolventov podľa odborov, roku ukončenia štúdia alebo mena, pričom by im mohli byť zobrazené buď celé elektronické diplomy, alebo len stručné informácie o týchto dokumentoch.

6.1.2 Vydávanie diplomov duálne

Okrem popísaného spôsobu vydávania a distribúcie diplomov elektronicky by bolo možné vydávať diplomy aj duálne. V takom prípade by sme do existujúceho systému pridali možnosť hromadnej tlače diplomov podpísaných rektorom. Papierové diplomy by mohli mať len informatívny charakter, pričom by obsahovali odkaz na webstránku, na ktorej bude možné si ich platnosť overiť (teda odkaz na modul na overovanie diplomov). Okrem toho by sme na papierovú formu diplomu mohli pridať ďalšie prvky, napríklad QR kód s odkazom na elektronickú verziu diplomu.

Druhou možnosťou je okrem elektronického diplomu vydávať aj riadne podpísaný diplom v listinnej podobe. Takéto riešenie by však bolo nepraktické, nakoľko by si vyžadovalo dvojité úsilie - podpisovanie dokumentov ako v elektronickej, tak aj listinnej podobe, prípadne podpísanie jedného z týchto formátov a vykonanie zaručenej konverzie.

V každom prípade by do existujúceho modelu bolo potrebné pridať možnosť hromadného exportu a tlače hotových elektronických diplomov zo systému, a to podľa rôznych kritérií (všetky diplomy, diplomy podľa ročníka, študijného odboru...).

6.1.3 Rozšírenie o notifikačný modul

Keďže vydanie diplomu pozostáva z niekoľkých fáz, ktoré na seba priamo nadväzujú, mohlo by byť vhodné doplniť možnosť notifikácie jednotlivých osôb o tom, že predošlá fáza bola ukončená. Tak by sa napríklad dekan dozvedel o tom, že študijný referent vytvoril a podpísal diplomy pre študentov jeho fakulty a že by ich mal skontrolovať a podpísať aj on. Rovnako by notifikácia prišla rektorovi, ak by nejaké diplomy čakali na jeho podpis, ale aj študentovi pri úspešnom vydaní jeho diplomu.

Zasielanie notifikácií by malo byť automatické, preto by mohlo byť užitočné systém rozšíriť o ďalší modul - či už notifikačný modul podľa Zákona o e-Governmente, ktorý doručí notifikáciu do elektronickej schránky občana, alebo o vlastný notifikačný modul, ktorý sa postará o notifikovanie používateľa iným spôsobom (napríklad poslaním e-mailu na jeho univerzitné konto).

6.2 Otvorené otázky

V tejto časti popíšeme otvorené otázky, ktoré vznikli pri návrhu konceptu riešenia a odpoveď na ktoré nám doposiaľ známa nie je. Ponúkame však niekoľko riešení v prípade rôznych odpovedí na ne.

6.2.1 Ochrana osobných údajov

V našom návrhu umožňujeme neautentifikovaným osobám získať elektronickú verziu diplomu, pokiaľ správne zadajú meno a priezvisko držiteľa diplomu a identifikačné číslo diplomu. Takáto možnosť je súčasťou online overovania platnosti diplomu.

Je však otázne, či by takéto konanie v reálnom systéme nebolo v rozpore so Zákonom o ochrane osobných údajov [2], nakoľko diplom obsahuje okrem mena a priezviska študenta a informáciách o študijnom programe aj dátum narodenia a informáciu o tom, či študent skončil štúdium s vyznamenaním.

Pokiaľ by sa zverejňovanie takýchto informácií len na základe zadania menovaných údajov ukázalo ako protiprávne, mohli by sme na overovanie platnosti diplomu pre verejnosť zvoliť inú možnosť.

Jednou možnosťou by bolo namiesto poskytnutia celého diplomu ako odpoveď na požiadavku vrátiť redukovanú verziu diplomu, ktorá by obsahovala len základné informácie o diplome (meno a priezvisko študenta, názov študijného programu, rok vydania diplomu...). Aby aj v tomto prípade bola zabezpečená integrita a autentickosť údajov na diplome (na zaručenie ktorej potrebujeme kryptografiu), aj redukovaná verzia diplomu by musela byť elektronicky podpísaná. Mohlo by ísť opäť o dokument formátu PDF alebo XML. V takom prípade by sme ale tvorbu tohto dokumentu museli zahrnúť do procesu tvorby diplomu a spolu s vytváraním a podpisovaním plnej verzie diplomu by sa musela automaticky vytvárať aj redukovaná verzia pre účely overovania platnosti diplomu.

Druhou možnosťou by bolo doplniť vyhľadávanie o ďalší parameter. Ak si chce neautentifikovaný používateľ overiť platnosť diplomu, musí okrem identifikačného čísla diplomu a mena a priezviska študenta zadať aj dátum jeho narodenia (prípadne ďalšie problematické údaje). V takom prípade by už zverejnením elektronickej verzie diplomu neboli prezradené žiadne také údaje, ktoré by danému používateľovi už neboli predtým známe, čo by tiež mohlo vyriešiť problematiku prezrádzania osobných údajov.

6.2.2 Rušenie diplomov

V časti 1.3 sme popísali možnosť rušenia certifikátov v PKI. Obdobná možnosť sa ponúka aj pri elektronických diplomoch - bolo by vhodné doplniť do systému možnosť zrušenia diplomu po tom, ako bol vydaný a podpísaný? Napríklad kvôli prípadom, kedy diplom bol podpísaný neúmyselne alebo v ňom bola dodatočne nájdená chyba, prípadne sa zistí, že diplom bol získaný podvodom (napríklad za odkopírovanú záverečnú prácu).

Zákon o vysokých školách, ktorý popisuje vydávanie dokladov o vzdelávaní, v súčasnosti termín rušenie diplomu nepozná. Ak sa však zistí, že diplom bol vydaný chybne (napríklad s preklepom v mene študenta), v analógovom svete je jednoduché diplom fyzicky zničiť a vydať nový. Pri elektronickej verzii diplomov by bolo nutné zaviesť

mechanizmus rušenia diplomov, čo by však v konečnom dôsledku mohlo byť v rozpore so zákonom.

Elektronický podpis považujeme za analógiu vlastnoručného podpisu, teda za prejav vôle podpisujúceho, preto by nemala nastať situácia „neúmyselného“ podpísania. Nemôžeme však úplne eliminovať možnosť, že osoba interagujúca so systémom na podpisovanie diplomov nedostatočne skontroluje údaje na ňom, prípadne pri výbere viacerých diplomov na podpis omylom zvolí diplom, ktorý nemal byť určený na podpisovanie. V prípade referenta alebo dekana neúmyselné podpísanie nemusí predstavovať problém, pokiaľ sa identifikuje dostatočne skoro - takto podpísané diplomy totiž nie sú platné, ak neobsahujú aj nadradený podpis rektora, pričom rektor má možnosť rozhodnúť, ktoré z diplomov podpísaných referentom a dekanom podpíše a ktoré budú odstránené. Problém by mohol nastať, ak by diplom chybne podpísal rektor, keďže jeho podpisom sa diplom nenávratne stáva platným.

Jednou možnosťou je akceptovať tento fakt a finálne podpisovanie diplomov podmieniť dôraznou kontrolou všetkých údajov študijným referentom v prvom kroku. Druhou možnosťou je doplniť proces vytvárania diplomov o ďalší krok - potvrdenie údajov samotným študentom, prípadne podrobná kontrola údajov na diplome na študijnom oddelení na rektoráte Univerzity (ako to funguje aj v súčasnosti). V takomto prípade by diplom mohol byť vytvorený študijným referentom, následne by bol jeho obsah skontrolovaný a odsúhlasený, a až potom by mohol byť podpísaný dekanom a rektorom, pričom takto vydaný diplom by už nebolo možné zrušiť.

Poslednou možnosťou je pridať možnosť rušenia už vydaných diplomov. V takom prípade by však bolo nutné ošetriť, za akých okolností sa takáto možnosť môže využiť, pričom tento úkon by musel byť patrične ošetrený aj legislatívne.

6.2.3 Spolupráca s vládnymi modulmi

Elektronický diplom podľa nášho konceptu obsahuje tri elektronické podpisy - referenta, dekana a rektora. Naproti diplomu v listinnej podobe sme pridali podpis referenta, ktorý pridáva záruku integrity a autentickosti údajov pri transformácii z podoby v informačnom systéme do podoby diplomu. Rovnaký efekt by sme dosiahli aj vtedy, ak by podpis referenta nebol vložený priamo do elektronického diplomu, ale bol uložený v databáze vytvorených diplomov a skontrolovaný pred tým, ako je diplom zobrazený na podpísanie v ďalšom kroku (dekanovi). Tým by sme dosiahli, že elektronický diplom bude obsahovať dva podpisy, rovnako ako listinný, pričom neprichádzame o bezpečnostné záruky.

Problémom by mohlo byť, že podľa Zákona o e-Governmente sú elektronické správy podpisované jedným elektronickým podpisom, pričom viacnásobné podpisovanie sa nespomína. Ak by takéto podpisovanie možné nebolo, museli by sme naše riešenie upraviť

tak, aby aj elektronický diplom obsahoval len jediný elektronický podpis - podpis rektora. Medzikrok s odsúhlasením diplomu dekanom by sme mohli vyriešiť rovnako ako medzikrok s odsúhlasením a podpísaním diplomu referentom.

Otázna je aj kompatibilita nášho formátu diplomu, ktorým je digitálne podpísané PDF, s formátom elektronických úradných správ podľa Zákonu o e-Governmente, ktoré sú vytvárané vo forme digitálne podpísaných XML súborov. Za istých okolností bude možno potrebné prehodnotiť spôsob vydávania diplomov a zjednotiť ho na ten istý formát.

6.3 Zhrnutie

V tejto kapitole sme sa na rozdiel od tej predošlej nevenovali implementácii systému pre správu elektronických dokumentov, ale zamerali sme sa na navrhnutý koncept samotný. Popísali sme jeho možné zmeny, doplnenia a problémy, ktoré zostávajú nevyriešené.

Záver

V tejto práci sme sa venovali dôsledkom Zákona o e-Governmente pre Univerzitu Komenského ako orgán verejnej moci. Identifikovali sme požiadavky, ktoré sú na Univerzitu kladené a preskúmali sme, aký dosah bude mať ich implementácia v praxi.

Univerzita Komenského je podľa Zákona o e-Governmente povinná zriadiť si elektronickú schránku, elektronickú podateľňu a zaviesť organizačné pravidlá ich používania. Elektronickú schránku môže mať zriadená nielen Univerzita, ale aj jej jednotlivé časti.

Univerzita je povinná poskytnúť súčinnosť pri prepojení jej informačných systémov s informačnými systémami ostatných orgánov verejnej moci a centrálnymi databázami údajov. To jej umožní naplniť požiadavku zákona „jedenkrát a dosť“ - teda používať už známe údaje namiesto toho, aby ich od občanov pýtala znova.

Najväčšie zmeny však Univerzita Komenského bude musieť vykonať vo vlastnej réžii vo vlastných informačných systémoch, ktoré bude potrebné prispôsobiť výkonu verejnej moci elektronicky, a v neposlednom rade v procesoch, ktoré na Univerzite prebiehajú, a ktoré bude taktiež potrebné prispôsobiť informatizácii.

V prvom kroku bude musieť UK prispôsobiť svoj autentifikačný modul tak, aby sa občania (študenti, zamestnanci, verejnosť) mohli pri používaní systémov Univerzity autentifikovať aj pomocou občianskeho preukazu s čipom. Univerzita bude musieť tiež zriadiť a spravovať elektronický archív pre dlhodobé uchovávanie ňou vydaných či prijatých elektronických dokumentov.

Ďalej bude musieť upraviť ďalšie časti svojich systémov tak, aby mohla svoju činnosť vykonávať elektronicky a automatizovane - či už pôjde o prijímacie konanie alebo vydávanie diplomov. V práci sme sa zaoberali skúmaním agendy Univerzity a procesov, ktoré bude potrebné elektronizovať, najviac sme sa ale zamerali práve na oblasť vydávania dokladov o vzdelaní.

Preskúmali sme, ako tento proces prebieha v súčasnosti a navrhli a popísali sme možný spôsob jeho informatizácie. Popísali sme výhody a nevýhody tohto konceptu, rovnako ako otvorené otázky, ktoré bude nutné konzultovať s ďalšími odborníkmi.

Navrhli sme systém, ktorý umožní okrem vydávania diplomov aj ich jednotnú správu, ktorá by mohla v budúcnosti byť analógiou dnešnej tvorby kópií, overovania

platnosti diplomov či ich bezpečnej archivácie. Aby sme identifikovali problematické časti, implementovali sme modelové riešenie takéhoto systému v simulovanom prostredí, a toto riešenie sme popísali. Pomenovali sme hlavné problémy, s ktorými sme sa pri implementácii stretli a navrhli sme ich možné riešenie.

Pre úspešné zavedenie Zákona o e-Gov na Univerzite Komenského bude v ďalších krokoch potrebné navrhnuté riešenia implementovať v reálnom prostredí, zaviesť do praxe a začať ich používať. Pre oblasť vydávania elektronických diplomov si to bude vyžadovať nielen zavedenie nových modulov do informačného systému Univerzity, ale aj zabezpečenie ich spolupráce s už existujúcimi systémami, splnenie bezpečnostných požiadaviek pre jeho bezproblémové fungovanie, ale v neposlednom rade aj predefinovanie existujúcich procesov a zaškolenie zamestnancov a študentov Univerzity.

Rovnakú úlohu bude následne potrebné splniť nielen pre ďalšie procesy študijnej agendy Univerzity, ale aj pre procesy vedeckej agendy Univerzity Komenského, ktorá taktiež spadá pod výkon verejnej moci. Zavádzanie Zákona o e-Governmente na Univerzite Komenského je veľkou, nie však nezvládnuteľnou úlohou, ktorá pri systematickom zapojení zamestnancov a spolupracovníkov Univerzity môže už v krátkej dobe priniesť želané zefektívnenie nielen komunikácie s Univerzitou, ale aj samotných procesov, ktoré v nej prebiehajú.

Dodatok A

Analýza Zákona o e-Governmente

Príloha obsahuje analýzu Zákona o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov v znení č. 214/2014 Z. z., 29/2015 Z. z., 130/2015 Z. z., 273/2015 Z. z., 272/2016 Z. z., 374/2016 Z. z., z pohľadu Univerzity Komenského ako orgánu verejnej moci.

Dokument obsahuje plné znenie prvého článku Zákona o e-Governmente. Pre každý odsek či písmeno zákona je text doplnený trojicou polí – povinnosti, právomoci a poznámky. Pole povinnosti obsahuje skutočnosti, ktoré pre UK priamo vyplývajú zo zákona. Pole právomoci obsahuje skutočnosti, ktoré zákon UK umožňuje vykonať alebo zabezpečiť. Pole poznámky obsahuje otvorené otázky alebo doplňujúce informácie k textu.

Dokument nájde čitateľ na priloženom CD nosiči pod názvom **eGovAnalyza.pdf**.

Dodatok B

Zdrojový kód vzorovej implementácie

Príloha obsahuje kompletný zdrojový kód modelovej implementácie systému na správu diplomov, ktorý sme popisovali v kapitole 5.

Archív so súbormi so zdrojovým kódom, dokumentáciou a ukážkami nájde čitateľ na priloženom CD pod názvom **ediplomy.zip**. Inštrukcie pre ľahšiu orientáciu sa nachádzajú v spomínanom archíve v súbore s názvom **README.txt**.

Literatúra

[1] Zákon č. 131/2002 z. z. o vysokých školách a o zmene a doplnení niektorých zákonov, 2002.

[2] Zákon č. 122/2013 z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, 2013.

[3] Zákon č. 305/2013 z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov, 2013.

[4] 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 (nariadenie eIDAS), 2014.

[5] Zákon č. 272/2016 z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov, 2016.

[6] Apache Software Foundation. Apache™ fop v2.1. `https://xmlgraphics.apache.org/fop/`, 2016.

[7] Matt Bishop. *Introduction to Computer Security.* Pearson Education, Inc., 2005.

[8] Communication-Systems-Group. pdfsign.js. `https://github.com/Communication-Systems-Group/pdfsign.js`, 2015.

[9] Ministerstvo financií Slovenskej republiky. Dôvodová správa k návrhu zákona č. 305/2013 - všeobecná časť, 2013.

[10] First Styles. Business & finance Vol 12. `https://www.iconfinder.com/icons/2135797/bin_trash_bin_icon#size=32`, 2017.

[11] Icon Coon. Colourful Education. `https://www.iconfinder.com/icons/1511311/award_graduation_graduation_ceremony_icon#size=32`, 2016.

[12] Ionicons. Ionicons. `https://www.iconfinder.com/icons/211719/cloud_download_icon#size=32`, 2013.

[13] David Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Simon and Schuster, 1996.

[14] Richard Kissel. Glossary of Key Information Security Terms. National Institute of Standards and Technology, Revision 2, 2013.

[15] Richard D. Kuhn, Vincent C. Hu, Timothy W. Polk, and Shu-Jen Chang. Introduction to Public Key Technology and the Federal PKI Infrastructure. National Institute of Standards and Technology, U.S. Government publication, 2001.

[16] Oxygen Team. Mimetypes application pdf Icon. `http://www.iconarchive.com/show/oxygen-icons-by-oxygen-icons.org/Mimetypes-application-pdf-icon.html`, 2011.

[17] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C.* John Wiley & Sons, Inc., 1996.

[18] Douglas R. Stinson. *Cryptography Theory and Practice.* Chapman Hall/CRC, 2006.

[19] The Pictographers. Orbicons (Free). `https://www.iconfinder.com/icons/667370/contract_document_paper_pen_sign_signature_icon#size=32`, 2015.

[20] Yannick Lung. Hawcons. `https://www.iconfinder.com/icons/314895/document_text_icon#size=32`, 2014.