VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Darya Ivanchanka

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ELEKTRONICKÝ PODPIS VE VEŘEJNÉ SPRÁVĚ
ELECTRONIC SIGNATURE IN PUBLIC ADMINISTRATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Darya Ivanchanka
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Václav Zeman, Ph.D.
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Darya Ivanchanka ***ID:*** 195153
Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Elektronický podpis ve veřejné správě

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je zmapovat současný stav využívání elektronického podpisu a elektronické komunikace ve veřejné správě států EU, případně států dalších. Uveďte definice a vysvětlení pojmů, které se využívají pro oblast služeb elektronické komunikace, a popište technické prostředky, které služby zajišťují. Na základě rozboru navrhněte výukovou aplikaci, která studentům umožní pochopit fungování elektronického podpisu a jejího využití ve veřejné správě.

DOPORUČENÁ LITERATURA:

[1] DOSTÁLEK, Libor. - VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Vyd. 2. Brno : Computer Press, 2010. 544 s. ISBN 978-80-251-2619-6.

[2] Zákon č. 297/2016 Sb. Zákonu o službách vytvářejících důvěru pro elektronické transakce. Sbírka zákonů České republiky. 2016, částka 115, s. 4466-4504. ISSN 1211-1244.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Téma bakalářské práce zahrnuje problematiku elektronického podpisu a jeho vymezení v teoretické rovině a následně z hlediska komparace u vybraných států, které jsou uvedeny v praktické části práce. V teoretické části práce jsou zpracovány hlavní pojmy a problémy jako pojem, funkce a technologie elektronického podpisu, stejně jako problematika e-governmentu a veřejné správy, která je pro řešení daného tématu také významné. Praktická část bakalářské práce zahrnuje komparaci elektronického podpisu ve vybraných zemích, jako je konkrétně Rusko, Bělorusko a vybrané státy Pobaltí. V praktické části je rozpracován také pohled evropského práva k problematice elektronického podpisu, jeho požadavkům a funkcím, které by měl elektronický podpis splňovat v zemích EU. V praktické části taky je popsána výuková aplikace, která byla vypracovaná v rámci bakalářské práci. Výuková aplikace studentům umožní pochopit fungování elektronického podpisu a jejího využití ve veřejné správě.

KLÍČOVÁ SLOVA

Digitalizace veřejné správy, e-Government, elektronický podpis, Evropské právo, informační technologie, veřejná správa.

ABSTRACT

The theme of the bachelor thesis includes the issue of electronic signature and its definition at the theoretical level and subsequently in terms of comparison for selected countries, which are listed in the practical part of the bachelor thesis. The theoretical part deals with the main concepts and problems such as the concept, function and technology of electronic signature, as well as the issue of e-government and public administration, which is also important for the solution of the selected theme. The practical part of the bachelor thesis includes a comparison of electronic signature in selected countries, such as Russia, Belarus and selected Baltic States. In the practical part is also elaborated the view of European law on the issue of electronic signature, its requirements and functions that the electronic signature should fulfill in EU countries. The educational application developed within the bachelor's thesis is described in the practical part as well. This application will enable students to understand working of electronic signatures and its use in public administration.

KEYWORDS

Digitization of public administration, e-Government, European law, electronic signature, information technology, public administration.

IVANCHANKA, Darya. *Elektronický podpis ve veřejné správě*. Brno, 2020, 76 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav elektroenergetiky. Vedoucí práce: doc.Ing. Václav Zeman

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Elektronický podpis ve veřejné správě“ jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu bakalářské práce panu doc. Ing. Václavu Zemanovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Úvod

Tématem bakalářské práce je problematika elektronického podpisu ve veřejné správě. Toto téma bylo vybráno zejména z toho důvodu, že v dnešní moderní době si málo kdo dokáže představit život bez moderních informačních technologií na PC a mobilních zařízeních a internetu, který se dynamicky rozvíjí a je ovlivněn moderními informačními technologiemi a inovacemi v této oblasti. V dnešní době je internet používám ke každodenním činnostem jednotlivců, a to jak k soukromým účelům, tak v komunikaci s veřejnými institucemi. Internet je prostředek, který nabízí vzájemnou komunikaci všem zainteresovaným subjektům ve vztahu k jednotlivci. V dnešní době je vývoj v oblasti počítačové techniky a internetu dynamický. Internetové pokrytí v rámci ČR se pohybuje již a téměř 100 % hodnotě, a to zejména v souvislosti s možnostmi internetového připojení od mobilních operátorů působících v ČR, jako je Vodafone, O2 nebo Z-Mobile, což má svoje pozitiva, ale také negativa. Příkladem komunikačních prostředků, které používá v podstatě každý jednotlivce je například e-mail, Facebook, ICQ, Skype nebo datová schránka.

Elektronická komunikace je mimo jiné určena také ke komunikaci s veřejnou správou a jejími institucemi fungující prostřednictvím elektronického podpisu nebo datových schránek. Díky vzniku elektronického podpisu, který se do praxe dostal v roce 2000, se zjednodušila komunikace s úřady. Prostřednictvím elektronického podpisu je možno zajistit průkazné předávání a automatické zpracovávání nejen externí, ale také interní komunikaci. V současnosti využívají elektronický podpis především subjekty, které mají tuto povinnost uloženou z hlediska platné právní úpravy. Jednotlivec si také může zřídit datovou schránku i elektronický podpis při splnění zákonem předepsaných požadavků. Například v současné době epidemie Covid-19 je tato elektronická forma komunikace s úřady výhodná v tom, že jednotlivec nemusí na jednotlivé veřejné úřady docházet osobně, ale může komunikovat s dotčenými úřady v elektronické podobě. Stejně tak výhodná je tato forma komunikace pro obchodní korporace, které tak mohou poměrně spolehlivě komunikovat s dodavateli nebo odběrateli, případně také s dalšími zainteresovanými subjekty ve vztahu k podnikatelské činnosti daných obchodních korporací.

Bakalářská práce je členěna do dvou hlavních celků, a to teoretickou a praktickou část. V teoretické části jsou zpracovány hlavní teoretické pojmy a problémy, které jsou dále aplikovány v praktické části práce. Jsou to zejména pojmy elektronického podpisu a komunikace s veřejnou správou v ČR, ale také služby elektronické komunikace v rámci ČR, technické prostředky komunikace, využívání elektronického podpisu ve veřejné správě a další relevantní teoretické problémy a pojmy. V praktické části práce jsou pak aplikovány některé z uvedených teoretických problémů a pojmů, a to s ohledem na elektronický podpis a služby elektronické komunikace ve

státní správě v Rusku, Bělorusku a vybraných státech Pobaltí. Tyto vybrané státy jsou komparovány s podmínkami a možnostmi v rámci ČR a v návaznosti této komparace jsou pak formulována relevantní doporučení a návrhy pro budoucí právní úpravu a využití elektronického podpisu ve veřejné správě v rámci ČR.

Cíl práce je stanoven jednak na definování zvolené problematiky v teoretické rovině, zejména pak elektronický podpis ve veřejné správě a v této souvislosti je pak cílem práce také zhodnocení a komparace dané problematiky na zvolených státech, jako je Rusko, Bělorusko a Pobaltské země, kdy zjištěná výstupy jsou pak aplikovány pro formulaci návrhů z hlediska budoucí právní úpravy elektronického podpisu ve veřejné správě v ČR.

V rámci bakalářské práci je realizována výuková aplikace, která je popsána v praktické části. Výuková aplikace studentům umožní pochopit fungování elektronického podpisu a jejího využití ve veřejné správě.

Metodologie práce je založena na analytickém zpracování odborné tuzemské a zahraniční literatury, která je uvedena v seznamu použité literatury v závěru bakalářské práce. V textu jsou využity také komparativní metody, a to hlavně v souvislosti komparativní studie vybraných zemí v praktické části práce s podmínkami elektronického podpisu ve veřejné správě. Aplikována je také metoda právní analýzy související s rozborem relevantních právních předpisů a sekundárního práva EU ve vztahu k hodnocení relevantních směrnic a nařízení týkající se řešené problematiky.

1 Elektronický podpis a jeho vymezení

1.1 Elektronický podpis

Elektronický podpis je v rámci informačních technologií termínem pro značení specifických dat, které v elektronickém zařízení, typicky PC, nahrazují klasický vlastnoruční podpis osoby. Případně také vlastnoruční ověřený podpis jednotlivce. Elektronický podpis je připojen k datové zprávě, jedná se o logické spojení, které umožňuje ověření totožnosti podepsané osoby ve vztahu k dané datové zprávě. Elektronický podpis je také prostředek k tomu jak v online prostředí ověřit totožnost odesílatele datové elektronické zprávy [1].

Elektronický podpis je vytvořen za účelem konkrétních data a je možné za pomocí počítačových technologií ověřit, zda je platný. Stejně tak, zda jsou data v relevantní podobě, ve které byla podepsána. Součástí elektronického podpisu je také identifikace toho, kdo elektronický podpis vytvořil. Ověření elektronické podpisu tak zahrnuje následující [2]:

- matematické operace relevantní k ověření elektronického podpisu,
- transkripce důvěry z důvěryhodné třetí strany na tvůrce podpisu,
- důvěryhodnost elektroniky podepsaného dokumentu.

K tomuto účelu se využívá elektronických certifikátů, certifikační autority a sítě důvěry. V rámci ČR existují tři subjekty oprávněné vydávat elektronický podpis [3]:

- První certifikační autorita, a. s.,
- Česká pošta, s. p.,
- eIdentity, a. s.

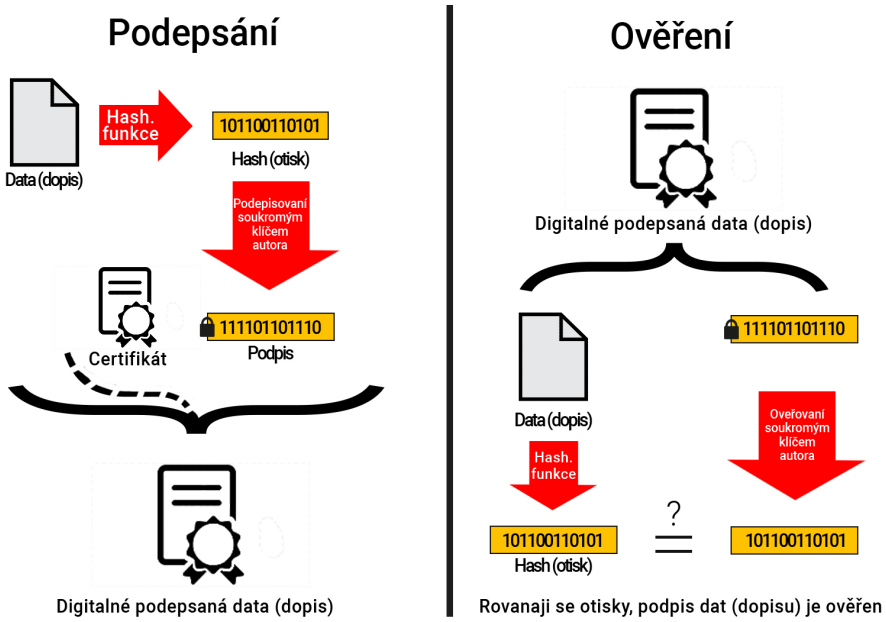
Proces použití elektronickýho podpisu začíná hashováním dat. Existuje zvláštní kategorie funkcí označované jako hashovací funkce. Tyto hashovací funkce berou data s proměnnou délkou, a to od zpráv s nulovou délkou po opravdu velké celky, jako celé obrazy jednotek představující vstup a vytvářejí konstantní délku výstupu, který je relativně krátký. Výstup je označován jako přehled zpráv nebo někdy se označuje jako hash. Celá původní zpráva musí být nějakým způsobem zajištěna z hlediska integrity dat při používání hash to umožňuje zmenšit velikost podpisu a čas potřebný vytvoření a ověření elektronického podpisu [4].

Je však nutné uvést, že ne všechny hashovací funkce jsou vhodné v kontextu elektronických podpisů. Se zabezpečenými hashovacími funkcemi je výpočetně nemožné [3]:

- identifikovat dvě různé zprávy, které budou produkovat přesně stejný výstup hashovací funkce,

- najít jinou zprávu, než je ta, která bude mít za následek stejný výstup hashovací funkce.

Pokud hovoříme o bezpečných hašovacích funkcích, je také důležité si uvědomit že SHA-1 je již považován za zastaralý a další hashovací funkce by měly aplikovány namísto SHA-1. Dalším důležitým konceptem je šifrování, a to zejména asymetrické šifrování. V takovém případě je pracováno se dvěma klíči. Jeden se nazývá veřejný klíč a je možné jej sdílet se všemi ostatními. Tento se používá pro šifrování dat. Jiný klíč se nazývá soukromý klíč, musí být uchován v tajnosti a původní data mohou být obnovena pouze se znalostí tohoto soukromého klíče [3]. V typickém případě ji poskytuje jeden subjekt, veřejný klíč přes (možná nezabezpečený) kanál k ostatním subjektům. Proces podpisu se však provádí pomocí soukromého klíče a ověření veřejným klíčem. Podepisování je ve skutečnosti šifrování hash funkcí pomocí soukromého klíče a přiřazení hodnoty k původním zdrojovým datům, jak bylo uvedeno výše. A ověření elektronickýho podpisu zahrnuje dešifrování podpisu a porovnání s vypočtenou hodnotou stejných dat. Fáze podpisu a fáze ověření je uvedena na obrázku níže (viz obr. 1.1).



Obr. 1.1: Podpis a ověření elektronického podpisu.

1.1.1 Struktura veřejného klíče

Infrastruktura veřejného klíče (dále jen PKI) zahrnuje celý komplexní systém, k němuž má dojít umožněním bezpečné komunikace v nedůvěryhodném prostředí bez předchozí interakce. Cena spočívá v tom, že obě strany musí důvěřovat jinému certifikačnímu subjektu, obvykle nazývanému certifikační úřad nebo certifikační autorita (dále jen CA). CA je subjekt odpovědný za ověření totožnosti koncového uživatele a pro vydávání a rušení certifikátů. Osvědčení se skládá z veřejného klíče a identifikace držitele, zahrnuje také sériové číslo, vytvořená data a uplynutí platnosti a další relevantní informace. Toto vše digitálně podepsané soukromým klíčem emitenta.

Důležité je, že subjekty navzájem neví o soukromém klíči držitele. Provede se ověření pomocí certifikátu emitenta, který obsahuje veřejný klíč. Ve skutečném světě aplikací, CA obvykle nepodepisuje certifikát koncového uživatele přímo, protože v případě ohrožení soukromého klíče mohou všechny vydané certifikáty už nebýt platné. Obvykle je nastavena jedna nebo více zprostředkujících CA. A cílem je vytvořit řetěz důvěry vedoucí ke kořenové certifikační autoritě. Soukromý klíč se používá jen zřídka a lze jej bezpečně uložit. Ověření musí sledovat celý řetězec až po společně dohodnutý kořenový CA. Protokol ke kontrole zrušených certifikátů by měl být nedílnou součástí celého systémového procesu.

1.1.2 Vlastnosti elektronického podpisu

Lze specifikovat následující vlastnosti elektronického podpisu, které je možné shrnout do několika hlavních oblastí, konkrétně [5] :

- **autenticita** – představuje způsoby, jak je možné ověžit identitu subjektu, kterému patří elektronický podpis, autenticita je realizována na základě přenosu důvěry, což je také vlastnost elektronického podpisu,
- **integrita** – je možné ji ověřit s vytvořením elektronického podpisu a cílem je, aby nedošlo k žádné změny v podepsaném dokument. Je tedy možné uvést, že dokument – podepsaný soubor, není úmyslně či neúmyslně poškozen,
- **nepopiratelnost** – představuje skutečnost, že autor dokumentu nemůže argumentovat, že elektronický podpis příslušný k dokumentu nevytvořil. Tuto skutečnost deklaruje akt, že k vytvoření elektronického podpisu je nutné mít k dispozici privátní klíč, který je provázán s veřejným klíčem, jak je uvedeno v dalších navazujících kapitolách. Bez přístupu k privátnímu klíči není možné elektronický podpis vytvořit a ověřit tak elektronický podpis, což je možné realizovat jen veřejným klíčem, které k tomuto patří,

- **časová platnost** – elektronický podpis může obsahovat také tzv. časové razítko, které deklaruje datum a čas podpisu dokumentu. Časové razítko vydává důvěryhodná autorita, jako třetí strana, je také součástí elektronického podpisu a je možné ji ověřit stejným postupem, jako elektronicky podepsaný dokument,
- **certifikační autorita** - v asymetrické kryptografii subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče), čímž usnadňuje využívání PKI (Public Key Infrastructure) tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Na Internetu působí mnoho komerčních certifikačních autorit, které obvykle mají své veřejné klíče umístěny přímo ve webových prohlížečích a dalších programech, čímž mohou uživateli zjednodušit rozhodování o míře důvěry webových serverů, ke kterým se připojuje (ale též digitálně podepsaných e-mailů i jiných dat). Existují též bezplatné certifikační autority nebo takové, které se řídí zákony daného státu, vnitřními předpisy organizace a podobně,
- **přenos důvěry** - běžně se využívá v reálném světě, čtením časopisů, novin, hovorem s ostatními lidmi, sledováním televize. Pokud se člověk dozví něco nového, přikládá této informaci váhu podle toho, z jakého důvěryhodného zdroje informace pochází. Přenášíme tak důvěryhodnost zdroje informací na jím poskytovanou informaci. Je-li certifikační autorita důvěryhodná, lze věřit informacím uvedených v digitálních certifikátech, které vydala (resp. digitálně podepsala). V počítači jsou šifrovací klíče uloženy v úložišti certifikátů nebo v klíčence. Při ověřování autentičnosti veřejného klíče lze využít toho, že klíč je digitálně podepsán důvěryhodnou certifikační autoritou (jinou osobou atp.). Pokud je digitální podpis certifikátu platný a důvěřujeme certifikační autoritě, která klíč podepsala, přeneseme důvěru a věříme v důvěryhodnost neznámého veřejného klíče. Pro usnadnění přenosu důvěry jsou v počítači obvykle předem přítomny kořenové klíče certifikačních autorit, které jsou distribuovány buď přímo s operačním systémem (Microsoft Windows) nebo s příslušnou aplikací (Firefox, Opera, Thunderbird atd.). Do úložiště je možné přidávat další certifikáty a následně důvěřovat certifikátům, které jsou jimi ověřitelné.

1.2 Funkce elektronického podpisu

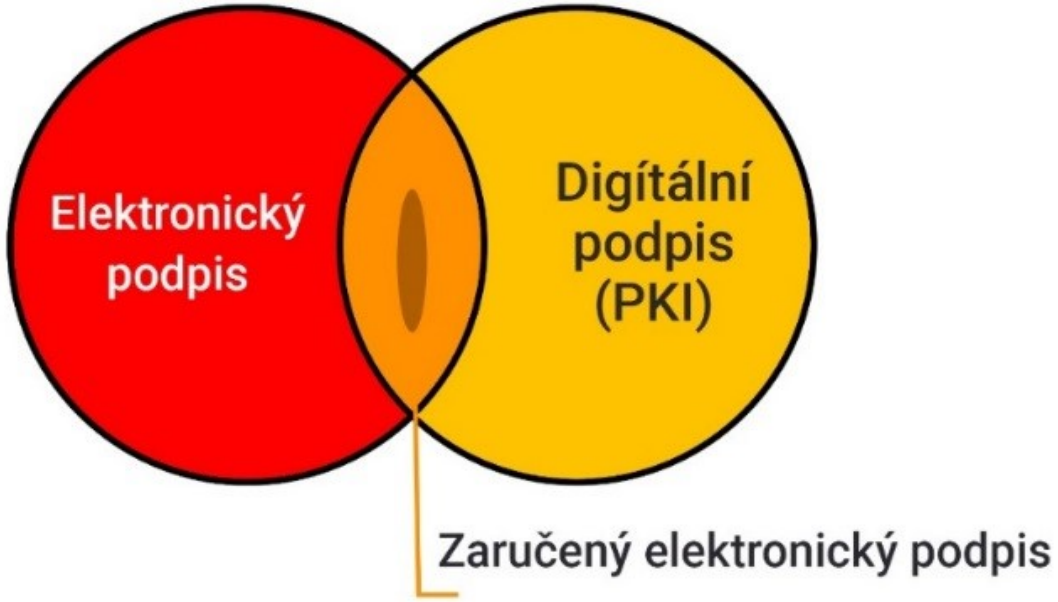
Co se týká funkcí elektronického podpisu, ty zohledňují především technické implementace a právní definice. Elektronický podpis má hned několik funkcí, které však mají odlišný stupeň důležitosti. Mezi funkce pak patří funkce ověřovací, identifikační, pravostní důkazní a varovací [6]. Velmi důležitou otázkou, kterou je při

důvěryhodném zpracování elektronických dat potřeba dodržet, je ověřování osoby, která tato data podepsala. Úkol jednotlivých funkcí je následující:

- **důkazní funkce** - elektronická data jsou definována jako soubor původních dat, které není možné v žádném případě zaměnit, zajišťuje se pomocí asymetrické kryptografie nebo elektronického podpisu,
- **varovací funkce** - jedná se o funkci, díky které elektronický podpis posiluje právní povahu daného dokumentu,
- **ověřovací** (verifikační) funkce - autenticitu dokumentu dokládá tzv. autentizace, která prokazuje identitu podepisujícího; takový způsob ověřování dokumentu přinesly právě elektronické dokumenty; autentizace se pak skládá z několika aspektů, mezi které patří primární a sekundární funkce poskytující spolehlivý důkaz toho, že ten, kdo dokument podepisuje, jej současně schvaluje a přijímá obsah dokumentu a tím se pro všechny strany stává závazný a může tak nabýt právního účinku; dalším aspektem autentizace je deklarovaný obsah odpovídající vůli podepisujícího a je považován za výsledek ústního vyjednávání, které mu předcházelo, nebo obecně vyjadřuje vůli přijetí či souhlasu interních podmínek užití. Autentizace je také považována za sekundární důkazní funkci elektronického podpisu, který umožňuje autentizaci podepisující osoby [7],
- **identifikační funkce** - identita v tomto kontextu znamená to, že podepisující osoba je takovou osobou, za kterou se vydává; každý jedinec je jako individuální entita unikátní, vyznačuje se rozeznatelnými principy, kterými se od ostatních liší,; pokud by nastal okamžik; kdy by jednotlivce nebylo možné identifikovat, nebyl by nikdo zodpovědný za své činy; mezi jeden důležitý identifikační nástroj patří elektronický podpis, kde se identita prověřuje pomocí privátního a veřejného klíče v rámci vytváření a ověřování elektronického podpisu; ke správnému ověření identity pak stačí to, aby privátní i veřejný klíč využila jedna osoba žádající o certifikát; národní systémy elektronické identifikace umožňují úspěšně rozpoznávat jedinečné atributy identity jednotlivce a slouží také k bezpečné komunikaci po internetu nebo také online služby [8],
- **autentifikační funkce** - pravost neboli integrita potvrzuje pravost dat elektronického dokumentu; ověřený elektronický podpis znamená, že celý elektronický dokument je podepsán od té pravé osoby a je důkazem toho, že v dokumentu nedošlo k žádné změně; význam integrity především při soudních řešení sporů.

1.3 Zaručený elektronický podpis

Elektronickým podpisem je rozuměn podpis, který se vytváří na základě asymetrické kryptografie a lze jej použít jako důkaz pravosti dokumentu a za konkrétních podmínek se používá místo ručního podpisu a lze její využít jako plnohodnotnou náhradu rukou psaného podpisu viz obr. 1.2.



Obr. 1.2: Zaručený elektronický podpis.

Za zaručený elektronický podpis se považuje podpis splňující následující požadavky:

- jednoznačně se spojuje s podepisující osobou,
- lze podle něj identifikovat osoby, které datovou zprávu podepisují,
- k datové zprávě se připojuje prostřednictvím prostředků, podle kterých dokáže podepisující osoba udržet svou kontrolu pod výhradním vlastnictvím,
- elektronický podpis je k datové zprávě připojen tak, že je možno zjistit zjistit jakoukoliv následnou změnu dat [9].

Co se týká jednotlivých podmínek, za kterých lze tento zaručený elektronický podpis vytvořit, jsou dány kryptografickými parametry a organizačními opatřeními spojenými s bezpečnou generací a správou párů klíčů, ale zejména legislativními podmínkami státu, ve kterém chceme příslušný zaručený podpis uplatnit. Zaručený elektronický podpis by tak měl splňovat následující vlastnosti: integrita, identifikace,

nepopiratelnost a právní akceptovatelnost a operační systém, jehož prostřednictvím se dokument podepisuje, by měl být důvěryhodný [10]. Na druhou stranu se u tohoto podpisu nevyžaduje žádné časové razítko a ani není nařízeno používání certifikátu sloužící ke zveřejnění dat důležitých pro ověření pravosti podpisu, a to stejně jako není striktně dán požadavek na ověřovací či popisovací prostředek. Zaručený elektronický podpis stejně jako ten obyčejný pro příjemce nic moc neznamená, ale slouží spíš pouze o jeho informování. Hlavní rozdíl mezi obyčejným a zaručeným elektronickým podpisem je stejný jako mezi úředně neověřeným a ověřeným vlastnoručním podpisem.

Kvalifikovaný elektronický podpis musí k elektronickému podepisování dokumentů– podle nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu – eIDAS [11], se za tento podpis považuje zaručený elektronický podpis vytvořený kvalifikovaným prostředkem určeným pro vytváření elektronických podpisů. Základem tohoto podpisu je kvalifikovaný certifikát určený pro elektronické podpisy. Povinnost používání kvalifikovaných prostředků byla zmírněna posledním dvouletým přechodným obdobím. Po celou tuto dobu se postupně rozšiřovala nabídka kvalifikovaných prostředků, které byly pro platnost podpisu nezbytné. V současnosti již není přístupné to, aby orgány veřejné správy používaly certifikáty na původních úložištích nebo ty přímo v počítači v rámci operačního systému. Současné požadavky na kvalitu kvalifikovaných prostředků jsou určeny evropskými předpisy a normami, které jsou primárně upravovány předpisem k nařízení eIDAS [10].

1.4 Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis je také upravován souhrnně podle zákona č. 297/2016 Sb., jelikož nové nařízení eIDAS tento pojem vůbec nezná. Dne 19. 9. 2018 skončila pro veřejnou správu povinnost podepisovat dokumenty pouze zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu pro elektronické podpisy. Od 20. 09. 2018 tak musí veřejná správa používat tzv. kvalifikovaný elektronický podpis. Podle nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES je kvalifikovaný elektronický podpis nejvyšší formou elektronického podpisu. Agendy, u kterých je použití kvalifikovaného elektronického podpisu vyžadováno jsou následující:

- výpis z rejstříku trestů,
- autorizovaná konverze,

- agendy zvláštních matrik, agendy soudy, agendy ohlašovny, agendy obcí III. typu [11].

Jedná o zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření podpisu. Zpravidla se používá pro komunikaci občanů se státní správou a samosprávou, tak pro komerční aplikaci. Tento druh podpisu se od předchozího liší tím, že je pro něj požadováno použít prostředky pro to, aby byl podpis bezpečně vytvořen. Prostředky pro bezpečné vytváření a ověřování podpisu musí umět to, aby se data pro vytváření podpisu:

- vyskytovala se jen jednou a bylo náležitě zajištěno jejich utajení,
- mohla odvodit ze znalostí jejich vytváření a podpis je tak chráněn proti padělání,
- byla spolehlivě chráněna proti zneužití.

Bezpečné vytváření podpisu spočívá v tom, že nesmí být měněna podepisující data a nesmí být ani zabráněno tomu, že by si podepisující strana nemohla podepisovaný dokument před podpisem zkontrolovat. Prostředky používané pro bezpečné ověřování podpisu, musí zajistit především to, aby:

- data užívaná pro ověřování podpisu odpovídala datům, která jsou dostupné pro ověření,
- byl podpis spolehlivě ověřen a jeho výsledek byl správně zobrazen,
- bylo možno spolehlivě zjistit obsah podepsaných dat ověřující osobou,
- byla zajištěna pravost a platnost certifikátu,
- došlo k řádnému ověření podepisující osoby,
- byl jasně uveden používaný pseudonym, jako jasné označení toho, pod jakým jménem uživatel vystupuje,
- byla možnost zjištění všech změn, které ovlivňují bezpečnost podpisu [10].

Tento druh podpisu je z hlediska důvěry považován za ten nejvhodnější, jelikož má pro příjemce vysokou vypovídací hodnotu. Co se týče jeho právní účinnosti, má stejné účinky jako vlastnoruční podpis ve všech členských státech.

1.5 Elektronická pečeť a elektronické časové razítko

Elektronická pečeť má synonymum také jako elektronická značka. Je definována v uvedeném evropském nařízení eIDAS a je definována jako *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi*

logicky spojena s cílem zaručit jejich původ a integritu.“ Elektronické pečetě by tedy měly sloužit jako důkaz toho, že elektronický dokument vydala určitá právnická osoba, a poskytovat jistotu o původu a integritě tohoto dokumentu. Mimo tohoto je možné ověřit pravost dokumentu také softwarový kód či virtuální server. Elektronickou pečeť je také možné podepisovat i elektronickým časovým razítkem Vytváření, uchovávání, ověřování shody a platnosti elektronických pečetí patří mezi takzvané služby vytvářející důvěru, součást E-governmentu, což je uvedeno v samostatné kapitole níže [12].

Elektronické časové razítko je služba poskytovaná certifikační autoritou, která umožňuje prokázat čas vytvoření dokumentu. Časové razítko je vhodné použít u elektronických dokumentů, kde je nutné prokázat čas jejich vzniku, jako jsou například účetní doklady. Samotný elektronický podpis prokazuje identitu tvůrce, ale neumožňuje dokázat, že je čas vytvoření dokumentu správný. Pro odstranění tohoto nedostatku bylo vytvořeno časové razítko. To však nezastupuje roli elektronického podpisu, jedinou jeho funkcí je prokázat čas vzniku dokumentu. Rovněž se nijak neovlivňuje s případným použitím elektronického podpisu na jednom jediném dokumentu. Kdo chce zajistit u dokumentu prokazatelnost jak osoby, která ho vytvořila, tak času, kdy vznikl, aplikuje na daný dokument zároveň elektronický podpis, který prokáže identitu tvůrce, tak i časové razítko, které prokáže čas vzniku [12].

1.6 Evropská právní úprava elektronického podpisu

Nařízení EU o elektronické identifikaci a důvěryhodných službách na vnitřním trhu 910/2014 / EU a důrazné schvalování elektronických podpisů vedlo k rostoucí poptávce po webových platformách elektronického podpisu. Přední platformy, jako jsou DocuSign a Adobe Sign, mění způsob, jakým se podnikání provádí v elektronický éře, a jsou nedílnou součástí úspěchu strategie jednotného elektronickýho trhu Evropské komise.

V souvislosti s evropskou právní úpravou elektronického podpisu je možné vymezit:

- nový zákon EU o elektronických podpisech,
- tři typy elektronického podpisu uznávané právem EU a jejich vlastnosti,
- klíčové právní problémy, které subjekty musí splnit, když uzavírají smlouvu o používání elektronického podpisu, případně nějaké související platformy.

Akt o jednotném trhu předložený Evropskou komisí v roce 2011 stanovil dvanáct politických iniciativ na podporu růstu a posílení hospodářství v Evropě. Zahrnovaly revizi směrnice o elektronických podpisech 1999/93 / ES. Směrnice poskytla

členským státům EU prostor pro uvážení při provádění jejích ustanovení do jejich vnitrostátního práva. Bohužel to mělo za následek spleti odlišných zákonů o elektronickém podpisu a neschopnost dohodnout se na společných technických normách upravujících přeshraniční elektronický obchod.

Evropská komise si také uvědomovala, že směrnice neudržela krok s technologiemi a jejich dynamickým rozvojem a inovacemi. Už to nebylo vhodné pro elektronický věk, ve kterém cloudové a mobilní technologie mění způsob podnikání. Směrnice například předpokládala vytvoření elektronických podpisů pomocí fyzických čipových karet a tokenů USB; ale cloudová technologie nyní umožňuje a nařízení výslovně umožňuje signatářům vytvářet a ověřovat elektronický podpisy pomocí mobilního zařízení, jako je smartphone či jiné mobilní zařízení. Tato směrnice vstoupila v platnost dne 1. července 2016, zrušila stávající směrnici a stanovila právní rámec pro elektronické podpisy v celé EU a řadu dalších důvěryhodných služeb, včetně elektronických pečetí a časových razítek.

Cílem nové stávající právní úpravy v EU je pomoci podnikům, spotřebitelům a subjektům veřejného sektoru při provádění pohodlných a bezpečných elektronických transakcí v celé EU a pokročit ve stěžejní strategii jednotného elektronickýho trhu Evropské komise. Praktické změny v platné právní úpravy poskytuje právníkům pokyny ohledně právních požadavků na elektronické podpisy v obchodních transakcích nejenom v rámci evropského práva, ale také v souladu s právem Velké Británie.

2 E-Government

Pojem e-government představuje elektronizace státní správy a samosprávy. E-government je definován jako transformace vnitřních a vnějších vztahů veřejné správy, a to za pomoci informačních a komunikačních technologií, díky kterým lze optimalizovat interní procesy. Digitalizace státní správy má především zrychlit a zlevnit poskytování služeb veřejné správy, a to zejména pro nejširší veřejnost. Za základní výhody lze považovat:

- rychlení a zkvalitnění služeb pro občany,
- přívětivé a jednoduché užívání služeb státní správy,
- možnost využití úředních hodin po celý den a týden,
- úspory z finančního hlediska,
- transparentní procesy a rozhodování [13].

Důležitou součástí e-governmentu je bezpochyby elektronická komunikace, která zjednošuje celý proces podání příslušného formuláře. Pro správný rozvoj e-Governmentu je jednoznačně potřeba legislativní podpora, v rámci které je třeba zařadit mezi nejprogresivnější země Rakousko, kde v roce 2004 zavedli revoluční zákon o elektonické veřejné správě. Klíčovými pojmy rakouského zákona je především identifikace, elektronický podpis a elektronické doručování.

První elektronickou službou, kterou mohli občané České republiky prostřednictvím elektronické pošty využívat, byla podávání žádostí o informace. Stejný rok došlo ke schválení první strategie zaměřené na informační gramotnosti, elektronický obchod a na informatizaci veřejné správy. Jednalo se o Státní informační politiku – cesta k informační společnosti [14]. Institut elektronického podpisu byl do českého právního řádu implementován v roce 2000. K tomuto zákonu pak vznikly další prováděcí právní předpisy, které zavedli funkci elektronického podpisu do praxe, ale až o rok a půl později. Již v této době bylo možné využívat elektronickou komunikaci v řadě správních agend. V praxi to však znamenalo, že na tuto možnost nebylo příliš úřadů připraveno [14].

V roce 2003 došlo k zániku Úřadu pro veřejné informační systémy, který byl založen v roce 2000, a jehož povinnosti přebralo Ministerstvo informatiky. Kromě převzetí Úřadu pro veřejné informační systémy, ministerstvo připravilo a prosadilo hned několik novel právních předpisů, jakou je například zákon o elektronickém podpisu kladoucí všem úřadům povinnost provozovat elektronické podatelny a zavedla orgán elektronické značky. O rok později pak byla schválena Státní informační a komunikační politika, nahrazující Národní telekomunikační politiku a Státní informační politiku.

Řada cílů v ní stanovených nebyla splněna. V roce 2005 došlo k vypracování a

přijetí Národní politiky pro vysokorychlostní přístup a národní strategie pro informační bezpečnost. V tu dobu mělo Ministerstvo informatiky relativně slabé postavení a spíše představovalo marketingového propagátora elektronické formy komunikace. Aplikace z oblasti eGovernmentu aplikuje každé ministerstvo samostatně, a to s různou intenzitou zavádění. V roce 2007 došlo ke zrušení Ministerstva informatiky a všechny náležitosti převzalo Ministerstvo vnitra [14].

V roce 2008 došlo ke spuštění projektu Czech POINT představující český podací ověřovací informační národní orgán. Jedná se o projekt, redukující přílišnou byrokracii ve vztahu občan-veřejná správa, přičemž Czech POINT funguje jako asistované místo výkonu veřejné správy, které umožňuje komunikaci se státem prostřednictvím jednoho místa. Cílem Czech Pointu je to, že se snaží vytvořit garantovanou službu určenou ke komunikaci se státem prostřednictvím jednoho univerzálního místa, ve kterém je možné získat a ověřit data z veřejných a neveřejných informačních systémů veřejně správy, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů [15].

V roce 2009 byl na základě zákona č.200/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, spuštěn informační rganu datových schránek, který představuje informační rganu veřejné správy ve smyslu zákona č. 365/2000 Sb. O informačních systémech veřejné správy, v platném znění. Datové schránky změnili prostřednictvím informačních technologií způsob doručování úředních dokumentů. Prostřednictvím datových schránek je možno rganum veřejné správy zasílat dokumenty v elektronické podobě a stejně tak jej od nich naopak přijímat. Komunikace prostřednictvím datových schránek vystřídala klasický způsob doručování v listinné podobě.

Hlavním cílem datových schránek je především zefektivnění veřejné správy, mezi které patří rychlost, zlevnění a spolehlivost veřejné správy, které je výhodné i pro občany. Těm, kteří datovou schránku potřebují ze zákona, ji zřizuje automaticky Ministerstvo vnitra. Všichni ostatní si o jejich zřízení musí zažádat osobně na Czech POINTU, písemně v listinné podobě s úředně ověřeným podpisem Ministerstvu vnitra či elektronickou poštou. Povinnost zřídit datové schránky mají ze zákona následující subjekty:

- orgán veřejné moci,
- fyzická osoba, která je v roli veřejné moci,
- fyzická osoba, která podniká a současně je v roli veřejné moci,
- právnická osoba, která je v roli veřejné moci,
- právnická osoba, která je zapsána v obchodním rejstříku,
- fyzická osoba, která podniká jako advokát, daňová poradce, statutární auditor či insolvenční správce [16].

2.1 Aktuální trendy v e-Governmentu

Místní, státní a federální vlády používají moderní informační technologie ke zlepšení života svých občanů. Od automatizace až po používání internetu věcí, aby byla města chytřejší, tyto subjekty již reálně objevily, jak používat technologie ke zlepšení efektivity na pracovišti a zlepšení života občanů.

2.1.1 Města propojená v rámci tzv. internetu věcí (IoT)

S využitím vestavěných senzorů v automobilech, pouličních osvětleních, dopravních kamerách a elektrických sítích se automaticky shromažďují a distribuují data a informace. Běžné využití IoT jsou inteligentní měřiče, které komunikují se společnostmi zabývajícími se energií, aby šetřily energii a silniční senzory, které sledují a spravují dopravní vzorce.

Kromě těchto infrastrukturních projektů IoT pracuje také v pozadí servisních snah, jako je veřejná doprava, veřejná bezpečnost a udržitelnost. Zatímco menší, lokalizované vládní projekty je obtížnější realizovat kvůli nedostatku finančních prostředků a technické podpory, některé státy využívají IoT roky, aniž by si to uvědomovaly. Propojená města zlepšují efektivitu a životy svých občanů i s ohledem na propojení s veřejnou správou a e-Governmentem, i když toto je v podmínkách ČR stále ještě se dynamicky rozvijící se segment.

2.1.2 Automatizace

Každá organizace ve veřejné správě bude postupně potvrzovat pravidlo rozpočtování 80/20. Na základě tohoto konceptu je 80 % rozpočtu určeno na běžný provoz instituce ve veřejné správě, zatímco pouze 20 % je věnováno na inovace.

Automatizace je řešením, jak uvolnit více finančních prostředků rozpočtu v institucích veřejné správy. Vládní sektory, využívající výhody automatizace, využívaly technologie jako AI a tzv. chatboty k vytvoření více občansky zaměřené komunikace. Je nutné uvést, že chatboty již poměrně dobře fungují také v komerční podnikatelské sféře. Chatboty ve veřejné správě v komunikaci s občany mohou řešit rutinní dotazy, které se pravidelně opakují a zefektivnit tak činnost zaměstnanců institucí veřejné správy.

Automatizovaná call centra v sociálních službách jsou příkladem toho, jak chatboti modernizují a zefektivňují komunikaci institucí pod vedením Ministerstva práce

a sociálních věcí ČR. Tato technologie, která šetří pracovní sílu a celkově zefektivňuje práci, kdyý chatboti mohou účinně řešit rutinní činnosti a dotazy klientů dané instituce. I když automatizace ještě není začleněna do vládních postupů, budoucnost se zdá být slibná, zejména pokud zvažujete možnost, že AI potenciálně uvolní podle kvalifikovaných odhadů až 30 % vládní pracovní síly za méně než deset let.

2.1.3 Zabezpečení a ochrana

Útoky na kybernetickou bezpečnost jsou formou významné kybernetické hrozby v 21. Století, a proto vlády jednotlivých států nepřetržitě pracují na ochraně občanských dat a infrastruktury. Se zvýšenou virtuální přítomností občanů a velkým množstvím vysoce citlivých informací, které jsou nyní uloženy online, všechny sektory nadále vylepšují kybernetickou bezpečnost a ochranu. Pochopení toho, že přístup založený na riziku je nejlepší pomoci při informovaném rozhodování vlád, se nyní technologie nepoužívá pouze k obraně, ale také k detekci.

2.1.4 Zlepšení a zefektivnění mobility

Odborné zdroje a zkušenosti z veřejné správy deklarují, že v letech 2020 – 2021 bude mobilní více než 70 % pracovní síly ve vyspělých západních společnostech. Tím se zefektivní nespočet postupů a procesů na státní a místní úrovni. Cílem aplikací zaměřených na občany je poskytovat veřejné služby a zapojovat komunity. Aplikace pro veřejné knihovny, parky a rekreace a motorová vozidla poskytují informace a služby rychleji než kdykoli předtím.

Podnikově orientované aplikace zvyšují efektivitu vlády tím, že omezují množství času, který lidé tráví papírováním a dalšími běžnými úkoly, které lze automatizovat a zpracovávat online. Občané mohou například požádat o správní služby a ptát se ice, což je výrazně efektivnější než nutnost osobní návštěvy instituce nebo telefonické dotazování.

. Rozdílně od původního přesvědčení, že přesun těchto entit na mobilní zařízení by znevýhodnil populaci s nízkými příjmy, současný výzkum podporuje opak. Vylepšená mobilita skutečně překlenula elektronický propast, protože pro mnohé je smartphone jedinou technologií, kterou vlastní. Nyní může vláda na všech úrovních oslovit více lidí a změnit vztah mezi občany a jejich institucemi veřejné správy.

2.1.5 Sběr dat a analytika

To, co bylo kdysi rigidním a zdlouhavým procesem s velkým zpožděním v reportingu, je nyní zjednodušeno, autonomní proces, který poskytuje data v reálném čase o všem, od sledování provozu až po správní činnosti. Sběr dat a analytika stále zlepšují různé

aspekty vlády, přičemž úředníci uznávají nutnost stanovení konkrétních pravidel pro to, jak budou data použita. Dosavadní zkušenosti jednotlivých subjektů ve veřejné správě, zejména občanů a dalších zainteresovaných subjektů mají vliv při dalších etapách digitalizace veřejné správy s ohledem na respektování požadavků na ochranu soukromí jednotlivých uživatelů – občanů.

Vládní agentury používají technologii k získávání dat ve snaze co nejlépe sloužit svým občanům. Od otázek bydlení a dopravy až po možné příčiny vysokého výskytu chorob v konkrétních oblastech jsou nyní vládní agentury schopny konsolidovat obrovské množství dat a pomocí sofistikované analýzy se dozvědět více o všem. Veřejné programy jsou nyní mnohem účinnější při plnění potřeb a přání občanů. Zapojení na platformách sociálních médií také poskytuje snadný a rychlý způsob shromažďování relevantních údajů a usnadňuje obousměrnou komunikaci s vládními subjekty, institucemi veřejné správy a jejich občany.

2.1.6 Elektronické vládní platformy

Podle průzkumu organizace OECD uvedlo více než 65 % vedoucích pracovníků veřejných služeb, že vytvoření personalizovaného a interaktivního obsahu pro klienta veřejné správy je prioritou. Používání elektronických vládních platforem pomáhá vedoucím zaměstnancům ve veřejné správě dosáhnout tohoto cíle. Občané na celém světě mají na dosah ruky více informací než kdykoli předtím, což jim umožňuje dosáhnout více za méně času. Například nyní můžeme domluvit návštěvu lékaře návštěvou webové stránky a výběrem dne a času, který je pro nás nejvhodnější. Můžeme si online prohlížet naše lékařské záznamy , podávat daňová přiznání,požádat o změnu osobních údajů. Zjednodušením těchto jednou zapojených procesů veřejné správy zlepšují zapojení a spokojenost občanů.

Přesun těchto programů a služeb online dává lidem nejen to, co chtějí, ale také uvolňuje státní pracovní sílu, aby se zaměřila na větší problémy. Od inteligentních měst po technologické výbory začaly místní, státní a federální vlády přijímat technologii.

3 Veřejná správa a její vymezení

V současnosti je veřejná správa často považována za součást určité odpovědnosti za určování politik a programů vlád, které také rozhodují o financování obcí či krajů ze státního rozpočtu daných zemí, tedy i v rámci ČR. Konkrétně se jedná o plánování, organizaci, řízení, koordinaci a kontrolu činností, které jsou prováděny v rámci systému veřejné správy. Veřejná správa je rysem v podstatě všech zemí, bez ohledu na jejich vládní systém. V rámci států se veřejná správa praktikuje na centrální, střední a místní úrovni. Vztahy mezi různými úrovněmi vlády v rámci dané země skutečně představují rostoucí problém veřejné správy.

Ve většině zemí světa existuje zřízení vysoce školených správních, výkonných nebo direktivních tříd, což učinilo z veřejné správy zvláštní profesi. Orgán veřejné správy se obvykle nazývá státní služba. Ve Spojených státech a několika dalších zemích byla konotace třídy elitářství tradičně spojená se státní službou, což vedlo k tomu, že profesní uznání přišlo pomalu a jen částečně, a to i v některých zemích také v rámci Evropské unie. Veřejná služba je tradičně v kontrastu s jinými orgány sloužícími státu na plný úvazek, jako je armáda, soudnictví a policie. Specializované služby, někdy označované jako vědecké nebo profesionální státní služby, poskytují spíše technickou než obecnou správní podporu.

Ve většině zemí se tradičně rozlišuje také mezi domácí státní službou a osobami zaměstnanými v zahraničí na základě diplomatických povinností. Státní úředník je proto jedním z konkrétních osob, které jsou přímo zaměstnány ve správě vnitřních záležitostí státu a jejichž role a postavení nejsou politické, ministerské, vojenské ani konstituční. Ve většině zemí státní služba nezahrnuje místní správu ani veřejné korporace, jako například ve Spojeném království National Coal Board. V některých zemích však, zejména v těch jednotných státech, ve kterých je provinční správa součástí ústřední vlády, jsou někteří provinční zaměstnanci státními zaměstnanci. Ve Spojených státech mají všechny úrovně vlády vlastní státní služby, federální, státní a místní, a státní služba je konkrétně ta část vládní služby, která vstoupila na zkoušku a nabídla trvalé funkční období.

Některé charakteristiky jsou společné pro všechny veřejné služby. Vyšší státní zaměstnanci jsou považováni za profesionální poradce těch, kteří formulují státní politiku. V některých zemích jsou vstupní požadavky na kariéru ve vyšších státních službách stresové kvalifikace v technických oborech, jako je účetnictví, ekonomie, lékařství a strojírenství. V jiných zemích se právní školení považuje za vhodné a v jiných není vyžadována žádná specifická technická nebo akademická disciplína mezi uchazeči o vedoucí funkce. Bez ohledu na jejich přesnou kvalifikaci jsou vyšší státní úředníci profesionální v tom smyslu, že se o jejich zkušenostech s veřejnými záležitostmi předpokládá, že jim poskytují informace o mezích, v nichž může být

státní politika účinná, a o pravděpodobných správních výsledcích různých kroků.

Očekává se, že státní úředníci budou v každé zemi radit, varovat a pomáhat těm, kdo jsou odpovědní za státní politiku, a pokud bude rozhodnuto, poskytnou organizaci její provádění. Odpovědnost za politická rozhodnutí nesou političtí členové výkonné moci (ti členové, kteří byli zvoleni nebo jmenováni, aby dali politické vedení vládě a obvykle kariérním úředníkům). Státní úředníci jsou obvykle chráněni před veřejnou vinou nebo cenzurou za jejich poradenství a doporučení související s výkonem jejich funkce. Činy jejich správy však mohou podléhat zvláštním soudním kontrolám, z nichž je žádný člen výkonné moci nemůže bránit.

Veřejné služby jsou organizovány na standardních hierarchických liniích, ve kterých struktura velení stoupá pyramidově, a to od nejnižších po nejvyšší. Tento příkaz předpokládá poslušnost zákonným příkazům nadřízeného a za účelem zachování tohoto systému je hierarchie úřadů vyznačena pevnými pozicemi, s jasně definovanými povinnostmi, specifickými pravomocemi, objektivními hodnotami platů a privilegií. V některých zemích může docházet k přímému jmenování osob, které nebyly dříve zaměstnány službou, ale i poté uznávaný systém interní propagace zdůrazňuje povahu hierarchické pyramidy.

3.1 Zásady veřejné správy

V průběhu 20. století bylo studium a praxe veřejné správy spíše pragmatické a normativní než teoretické a hodnotové. To může vysvětlit, proč se veřejná správa, na rozdíl od některých společenských věd, vyvíjí bez velkého znepokojení nad obsáhlou teorií. Teprve v polovině 20. století a při šíření německé sociologie Max Weberovy teorie byrokracie byl o teorii veřejné správy velký zájem. Nejnovější byrokratická teorie však byla adresována soukromému sektoru a bylo vynaloženo jen malé úsilí na propojení organizace s politickou teorií.

Významnou zásadou veřejné správy je ekonomika a efektivita, to znamená poskytování veřejných služeb za minimální náklady. To byl obvykle stanoven cíl správní reformy. Navzdory rostoucímu obavám o jiné druhy hodnot, jako je schopnost reagovat na potřeby veřejnosti, spravedlnost a rovné zacházení a zapojení občanů do vládních rozhodnutí, je účinnost i nadále hlavním cílem.

Veřejná správa se ve svém zájmu o efektivitu a zlepšování často zaměřovala na otázky formální organizace. Obecně se tvrdí, že administrativní nedostatky lze alespoň částečně napravit reorganizací. S armádou vzniklo mnoho organizačních principů, některé ze soukromého podnikání. Patří sem například:

- organizování útvarů, ministerstev a agentur na základě společných nebo úzce souvisejících účelů v rámci veřejné správy,

- seskupování podobných činností do jednotlivých jednotek v rámci veřejné správy,
- vyrovnání odpovědnosti s pravomocí ve veřejné správě,
- zajištění jednoty vedení útvarů ve veřejné správě na principu pouze jeden nadřízený pro každou skupinu zaměstnanců,
- omezení počtu podřízených ve vztahu k jedinému nadřízenému,
- rozlišování liniových (provozních nebo konečných) činností od zaměstnanců (poradenské, konzultační nebo podpůrné) činnosti použití,
- aplikace zásady řízení výjimečně (pouze vrchol neobvyklého problému nebo případu),
- mající jasně vymezenou řetězec příkazů směrem dolů a odpovědnost směrem vzhůru v rámci systému veřejné správy.

Někteří kritici tvrdili, že tyto a další principy veřejné správy jsou užitečné pouze jako hrubá kritéria pro dané organizační situace. Domnívají se, že organizační problémy se liší a že použitelnost pravidel na různé situace se také liší. Nicméně i přes mnohem sofistikovanější analýzy organizačního chování v posledních desetiletích platí, že zásady, které jsou vyjmenovány výše, stále platí.

Veřejná správa také kladla důraz na personální aspekty z hlediska své činnosti. Ve většině zemí zahrnuje správní reforma reformu státní správy. Historicky byl směr směřován k „meritokracii“, tedy k nejlepšímu jednotlivci pro každou práci, konkurenčním zkouškám pro vstup a výběru a postupu na základě zásluh. Pozornost se stále více věnuje jiným faktorům než intelektuálním přínosům, včetně osobních postojů, pobídek, osobnosti, osobních vztahů a kolektivního vyjednávání.

Kromě toho se rozpočet vyvinul jako hlavní nástroj při plánování budoucích programů, rozhodování o prioritách, řízení stávajících programů, propojení výkonných orgánů s legislativou a rozvíjení kontroly a odpovědnosti. Soutěž o kontrolu nad rozpočty, zejména v západním světě, začala před staletími a občas byl hlavním vztahem mezi panovníky a jejich podřízenými. Moderní systém výkonných rozpočtů, ve kterém exekutiva doporučuje, zákonodárci a výkonné orgány dohlíží na výdaje, vznikly v Británii 19. století. Ve Spojených státech se během 20. století stal rozpočet hlavním nástrojem legislativního dohledu nad správou, výkonnou kontrolou oddělení a resortní kontrolou podřízených programů. V mnoha rozvojových zemích světa převzala podobnou roli.

Klasický přístup k veřejné správě popsaný výše pravděpodobně dosáhl svého plného rozvoje ve Spojených státech během třicátých let 20. století, ačkoli od té doby se prostřednictvím vzdělávacích a školicích programů, technické pomoci a práce mezinárodních organizací stal také standardní doktrínou v mnoha země. Vládám s britskými nebo kontinentálně-právními perspektivami však některé její prvky odo-

lávaly, a dokonce i během třicátých let 20. století byla zpochybňována z několika čtvrtin. Od té doby se studium tohoto předmětu velmi rozvíjelo. Rovněž se stala poněkud zmatená v důsledku určitých nesrovnalostí v přístupu.

Ortodoxní doktrína spočívala na předpokladu, že správa byla jednoduše prováděním veřejných politik určených ostatními. Podle tohoto názoru by administrátoři měli usilovat o maximální efektivitu, ale měli by být jinak neutrální ohledně hodnot a cílů. Během Velké hospodářské krize třicátých let 20. století, a ještě více za druhé světové války, se však stále více ukázalo, že v administrativě vzniklo mnoho nových politik, že politické a hodnotové úsudky byly implicitní v nejvýznamnějších správních rozhodnutích, že mnoho správních úředníků pracovalo o ničem jiném než o politice, a že, pokud byly veřejné politiky kontroverzní, taková práce nevyhnutelně zahrnovala administrátory do politiky. Předpokládaná nezávislost správy od politiky a politiky byla považována za iluzorní. Od třicátých let 20. století tedy roste zájem o vytváření politiky a vývoj technik ke zlepšení politických rozhodnutí. Přestože koncept neutrální administrativy bez hodnoty je mnohými považován za již neudržitelný, nebyla nabídnuta žádná zcela uspokojivá náhrada. Jak zajistit, aby odpovědní a pohotová politická rozhodnutí činili správci kariéry a jak koordinovat svou práci s politikou politicky zvolených nebo jmenovaných úředníků, zůstává klíčovým zájmem, zejména v demokratických státech.

To bylo s vládním úsilím bojovat proti depresi, že nová informační zařízení byla představena, včetně národního příjmu účetnictví a kontrola hrubého národního produktu jako hlavní index ekonomického zdraví. Aplikovanými technikami fiskální a měnové politiky se staly zavedené specializace veřejné správy. Ekonomové zastávají klíčová místa ve správách většiny národů a mnoho dalších správců musí mít alespoň základní znalosti ekonomických důsledků vládních operací. Francie, Švédsko a další skandinávské národy, Velká Británie a Spojené státy patřily k lídrům ve vývoji technik ekonomického plánování. Takové plánování se stalo dominantním zájmem veřejné správy v mnoha rozvojových zemích.

Jak se ekonomická a sociální intervence ze strany vlád jednotlivých zemí zvýšila, omezení „inkrementalismu“ jako praxe veřejné správy se stále více prakticky projevují. Inkrementalismus je tendence vlády do určité míry manipulovat s politikami veřejné správy spíše než zpochybňovat hodnotu jejich pokračování. Byla zavedena řada technik pro racionálnější rozhodování ve veřejné správě. Jednou z široce používaných technik je analýza nákladů a přínosů, která se týká také oblasti veřejné správy. To zahrnuje identifikaci, kvantifikaci a porovnání nákladů a přínosů alternativních návrhů. Další, méně úspěšnou technikou bylo plánování, programování a rozpočtování ve veřejné správě, které bylo zavedeno na ministerstvu obrany USA v roce 1961 a rozšířen do dalších zemí. Srovnatelné programy v západní Evropě, jako například metoda „racionalizace výběru rozpočtu“ zavedená do Francie na konci 60.

let 20. století a tzv. analýza a přezkum programu ve Velké Británii v 70. letech 20. století byly také obecně neúspěšné.

Kvantitativní ekonomické měření ve veřejné správě je užitečné až do určitého bodu, ale hodnota lidského života, svobody od nemoci a bolesti, bezpečnosti na ulicích, čistého vzduchu a příležitosti k dosažení jsou v peněžních podmínkách jen těžko měřitelné. Veřejná správa se tak stále více zajímá o vývoj lepších sociálních ukazatelů, kvantitativních a kvalitativních, to znamená, lepších indexů účinků veřejných programů a nových technik sociální analýzy. Dalším vývojem byl rostoucí důraz na lidské vztahy, kdy elektronický podpis lze označit jako finální výstup jak usnadnit občanovi komunikaci s veřejnou správou. Toto vzniklo ve 30. letech 20. století, označované jako výzkum Hawthorne, zahrnující pracovníky a management průmyslového závodu v blízkosti Chicaga, přineslo význam pro produktivitu sociální nebo neformální organizace, dobré komunikace, chování jednotlivců a skupin a postoje jako přidané hodnoty a pozitivních přístupů ve veřejné správě.

Chování zaměstnanců veřejné správy ovlivnilo povědomí o důležitosti lidských vztahů. Bylo vyzváno mnoho administrativních administrativ (hierarchie, vedení směrnic, stanovené povinnosti, zacházení se zaměstnanci jako s neosobními „jednotkami“ výroby a peněžní pobídky). Koncem třicátých let 20. století se přístup k lidským vztahům vyvinul v koncept známý jako „rozvoj organizace“. Jeho primárním cílem bylo změnit postoje, hodnoty a struktury organizací tak, aby dokázaly vyhovět novým požadavkům. Uskutečnili se také vyškolení konzultanti a následně zaměstnanci, obvykle zvnějšku organizace, intenzivní pohovory s vedoucími a juniorskými pracovníky a školení o citlivosti a konfrontace. Na rozdíl od racionálního přístupu původní koncept řízení veřejné správy zdůrazňoval rozvoj organizace identifikaci osob s organizačními cíli, „seberealizaci“ pracovníků a manažerů, efektivní mezilidskou komunikaci a širokou účast na rozhodování. Jeho přímé použití ve vládních agenturách bylo omezené a nebylo vždy úspěšné, ale mělo na administrátory značný nepřímý vliv.

Dalším moderním hnutím ve veřejné správě byla větší účast občanů na vládě. Během 50. a 60. let 10. století to bylo povzbuzováno rostoucím pocitem, že vlády nereagovaly na potřeby svých občanů, zejména menšinových skupin a chudých. V 60. letech 20. století byla zahájena řada pokusů o zapojení občanů nebo jejich zástupců do přijímání vládních rozhodnutí. Jednalo se o delegování rozhodování z ústředních úřadů na místní úřady a na místní úrovni sdílení pravomocí se skupinami občanů.

Od počátku sedmdesátých let 20. století vedla rostoucí analýza vlivu vládních politik na veřejnost a vyústila v koncepci nazvanou „přístup veřejné politiky“ ke správě. Tím se zkoumá, do jaké míry každá fáze navrhování a provádění politiky ovlivňuje celkový tvar a dopad politiky. Podle konceptu způsob, jakým je problém koncipován, v první řadě ovlivňuje rozsah zvažovaných nápravných opatření. Po-

vaha rozhodovacího procesu může určit, zda je postup pouze přírůstkový nebo skutečně radikální. Ve skutečnosti se argumentovalo, že povaha rozhodovacího procesu utváří výsledek samotného rozhodnutí, zejména pokud tomuto procesu dominuje silná zájmová skupina. Výsledek ovlivňuje také ochota vlády hodnotit programy a v případě potřeby je upravovat. Mnoho příznivců přístupu veřejné politiky považuje tento koncept za důležitý nástroj pro vytvoření souboru znalostí, na nichž mohou být doporučení založena.

Až do druhé světové války mezi národy došlo k relativně malé výměně názorů o veřejné správě. Již v roce 1910 však byla zřízena profesní organizace, která se nakonec stala Mezinárodním institutem správních věd (IIAS). Zpočátku se její členství skládalo hlavně z učenců a praktiků správního práva v zemích kontinentální Evropy. Koncem 80. let měla IIAS členství z přibližně 70 zemí. Její tříleté kongresy pokryly všechny aspekty oboru. Od druhé světové války vzrostl mezinárodní zájem o správní systémy, což vyvolalo nutnost spolupráce během války, vytváření mezinárodních organizací, okupace dobývaných národů a správa programů hospodářské obnovy pro Evropu a Dálný východ, a prostřednictvím programů pomoci rozvojovým zemím. Jedním vedlejším produktem programů pomoci bylo nové uznání toho, jak zásadní je efektivní správa pro národní rozvoj. Ukázalo se také, že v jednotlivých zemích často zůstaly parochiální a kulturně vázané styly veřejné správy.

Dalším účinkem této mezinárodní komunikace a sdílení zkušeností bylo poznání, že rozvoj není exkluzivní pouze pro tzv. Nerozvinuté země. Všechny země se nadále vyvíjely a veřejná správa byla stále více vnímána jako správa plánované změny ve společnostech, které samy prošly rychlými změnami, ne všechny se plánovaly. Vláda již není pouze strážcem míru a poskytovatelem základních služeb: v postindustriální éře se vláda stala hlavním inovátorem, určujícím společenským a ekonomickým prioritám a podnikatelem ve velkém měřítku. V podstatě u každého významného problému nebo výzvy, od nezaměstnanosti po čistý vzduch, lidé hledali vládu s hledáním řešení nebo pomoci. Úkoly plánování, organizace, koordinace, řízení a hodnocení moderní vlády se rovněž staly úžasnými co do rozměrů i významu.

Evropské vysokoškolské systémy tradičně vytvořily pro své vlády administrativní právníky, ale samotné právní dovednosti jsou pro řešení současných problémů stěží dostačující. Americké univerzity začaly programy postgraduálního studia na počátku 20. století a koncem 80. let 20, století existovalo ve veřejné správě více než 300 univerzitních programů. Nicméně jen velmi málo vědců a dalších odborníků, kteří se stanou administrátory ve svých oborech, navštěvuje takové programy. Vzdělávací programy se rozvíjejí zejména od druhé světové války, mnohé z nich s pomocí vlády. Některé jsou připojeny k univerzitám. Při zřízení státní správy École Nationale jako jedné ze svých reforem státní služby v letech 1946–47 poskytla Francie rozsáhlý kurz pro rekruty vyšší státní správy. Teprve v roce 1969 Británie zřídila Vysokou

školu státní správy v rámci nového ministerstva státní správy. Ve Spojených státech vláda zavedla během 60. let 20. století řadu vzdělávacích a školicích programů. S ohledem na výše uvedené je nutné uvést, že principy a podoba veřejné správy do jisté míry čerpaly také ze zkušeností a východisek západoevropských zemí, ale také z dosavadních stavebních kamenů veřejné správy.

4 Technologie elektronického podpisu

4.1 Asymetrické algoritmy

Problém výměny klíčů mezi odesílatelem a příjemcem zprávy trápil kryptografy po několik století. Spočívá ve výměně tajné informace (šifrovacího klíče) tak, aby ji nikdo třetí nebyl schopen odposlechnout. Pro distribuci klíčů se využívaly služby kurýrů. Jejich použití je však na válečném poli problematické. Neřešitelnou situace začínala být v případě elektronické komunikace a elektronického obchodování. V 60. letech, kdy se v USA začala rozvíjet elektronická komunikace, narážel systém symetrického šifrování na obrovské logistické problémy. Každý den se na cestu vydávali kurýři s kufříky, ve kterých měli komunikační klíče pro daný den. Týkalo se to bank, státní institucí i armády. Situaci příliš neřešil ani systém Diffie-Hellman-Merkle. Zdálo se, že problém je neřešitelný.

V roce 1975 však načrtl Whitfield Diffie myšlenku asymetrické kryptografie. Jde o skupinu kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče. Základem jsou jednosměrné funkce, které umožní původní zprávu zašifrovat pomocí veřejného klíče, ale již nikoliv dešifrovat za pomocí téhož klíče. Pro dešifrování zpráv se použije klíč soukromý, který má uschovaný příjemce zprávy. Každý, kdo chce šifrovat zprávy s použitím asymetrických metod, si vytvoří pár klíčů (soukromý a veřejný). Veřejný klíč distribuuje po mezi všechny osoby, se kterými chce komunikovat a klíč soukromý si uchová u sebe v tajnosti. Dvě komunikující strany se pak vůbec nemusí setkat a přesto mají k dispozici nástroj pro bezpečnou komunikaci.

Systém generuje pár klíčů, jeden pro šifrování a druhý pro dešifrování. Jeden klíč si ponechá a uchová v tajnosti (soukromý klíč) a druhý (veřejný klíč publikuje na veřejném místě. Pro šifrování a dešifrování se používá tentýž algoritmus, odesílatel a příjemce zprávy musí mít dva nepárové klíče (svůj soukromý a partnerův veřejný klíč).

Pro zaručení bezpečnosti výměny zprávy:

- jeden z klíčů musí zůstat utajený,
- musí být nemožné nebo aspoň neproveditelné dešifrovat zprávu, jestliže není k disposici další informace,
- znalost algoritmu, jednoho z klíčů a vzorku šifry musí být nedostatečné informace k odhalení druhého klíče.

Další kategorie kryptosystémů s asymetrickou kryptografií (AK):

- digitální podpis,

- výměna klíčů: dvě strany spolupracují na výměně session key.

Generace asymetrických klíčů - matematicky obtížné problémy z oblasti teorie velkých čísel (faktorizace součinu dvou velkých čísel, diskrétní logaritmy, Eucliduv algoritmus) - modulární aritmetika.

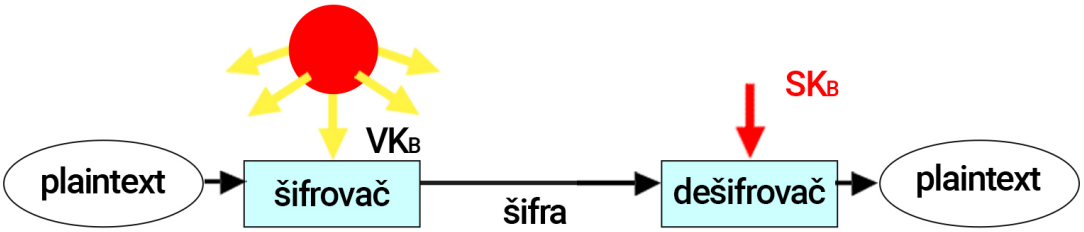
Nejpoužívanější algoritmy pro elektronické podepisování:

- **RSA** - autoři Rivest, Shamir, Adleman - generace klíčů velmi náročná (princip nesoudělnosti dvou velkých čísel), parametry algoritmu VK, SK a délka bloku, na který se šifrovaný text rozdělí [20],
- **DSA** - jedná se o algoritmus, jehož bezpečnost je závislá na problému výpočtu tzv. diskrétního logaritmu. Jedná se o algoritmus, který slouží k podpisu a zajištění důvěryhodnosti přenášených zpráv. Princip činnosti DSA je od základu jiný, než v případě reverzibilní šifry jako je RSA [21],
- **ECDSA** - algoritmus založený na principu eliptických křivek, varianta DSA protokolu. Použití pro šifrování i výměny tajného klíče - výpočetně méně obtížná metoda s podstatně kratším klíčem (5 - 10 x). [21].

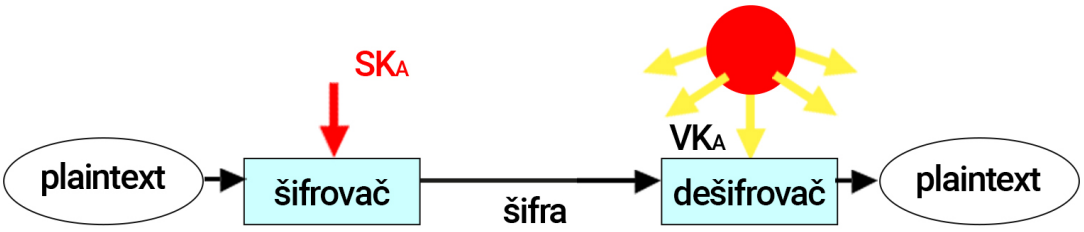
Další nejrozšířenější AK algoritmy:

- **ElGamal** - založen na obtížnosti výpočtu diskrétních algoritmů:
  - zvolí se velké prvočíslo p (min. 200 cifer)
  - zvolí se čísla g, $x > p$
  - x je soukromý klíč
  - vypočte se $y = g^{**}x \ mod \ p$
  - veřejný klíč je y, g, p
- **Diffie - Hellman** - algoritmus pro výměnu tajného klíče TK (session key) - založen na obtížnosti výpočtu diskrétních logaritmů. Princip: každá strana si na základě globálních veřejných parametrů vypočítá svou dvojici veřejný – soukromý klíč, svůj veřejný klíč předá partnerovi a z veřejného klíče partnera si vypočítá tajný klíč (tajný klíč se tedy nepředává nezabezpečeným komunikačním kanálem).

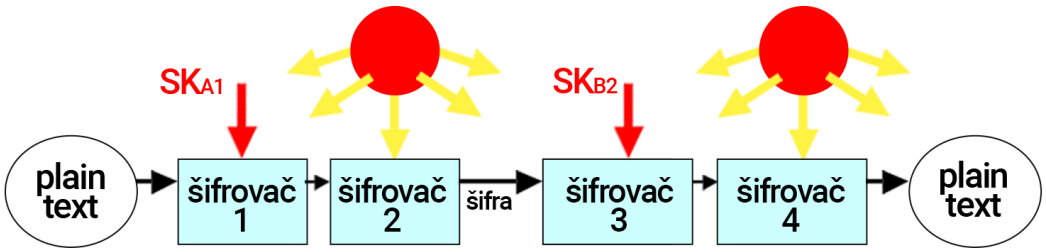
Uplatnění asymetrické kryptografie v různých typech kryptografických systémů viz.obr. 4.1.



Kryptografický systém pro zabezpečení důvěrnosti zprávy



Kryptografický systém pro zabezpečení autentičnosti zprávy



Kryptografický systém pro zabezpečení autentičnosti a důvěrnosti zprávy

Obr. 4.1: Uplatnění asymetrické kryptografie v různých typech kryptografických systémů

4.2 Hashovací funkce

Jedná se o jednosměrné funkce, které musí splňovat přesně definované podmínky. Základní hashovací funkce mapují řetězec libovolné délky (zpráva, datový soubor) na řetězec konstantní délky a vytvářejí tak otisk vstupního řetězce. Výsledný otisk se označuje jako výtah, hash, fingerprint nebo miniatura a je závislý na všech bitech vstupního řetězce. Tyto funkce slouží ke kontrole integrity dat, k porovnání dvojice zpráv, k vyhledávání, indexování a využívají se pro tvorbu digitálních podpisů [17].

Mezi nejznámější hashovací funkce patří MD4, MD5, SHA-1 a SHA-2. Tyto algoritmy jsou založeny na podobných principech jako blokové šifry, např. AES. Každá hashovací funkce v principu není injektivní (čili prostá), existují tedy různé zprávy poskytující stejný hash. To samo o sobě není problém, pokud hashovací funkce splňuje následující požadavky:

- je to jednosměrná funkce (tj. je snadné spočítat hash zprávy, ale nesmírně obtížné nalézt k danému hashi zprávu),
- není možné najít dva vstupy, které mají stejný výsledný hash (tj. kolize),
- je obtížné tyto kolize hledat systematicky,
- neexistuje korelace vstupních a výstupních bitů,
- jakékoliv množství vstupních dat poskytuje stejně dlouhý výstup [17].

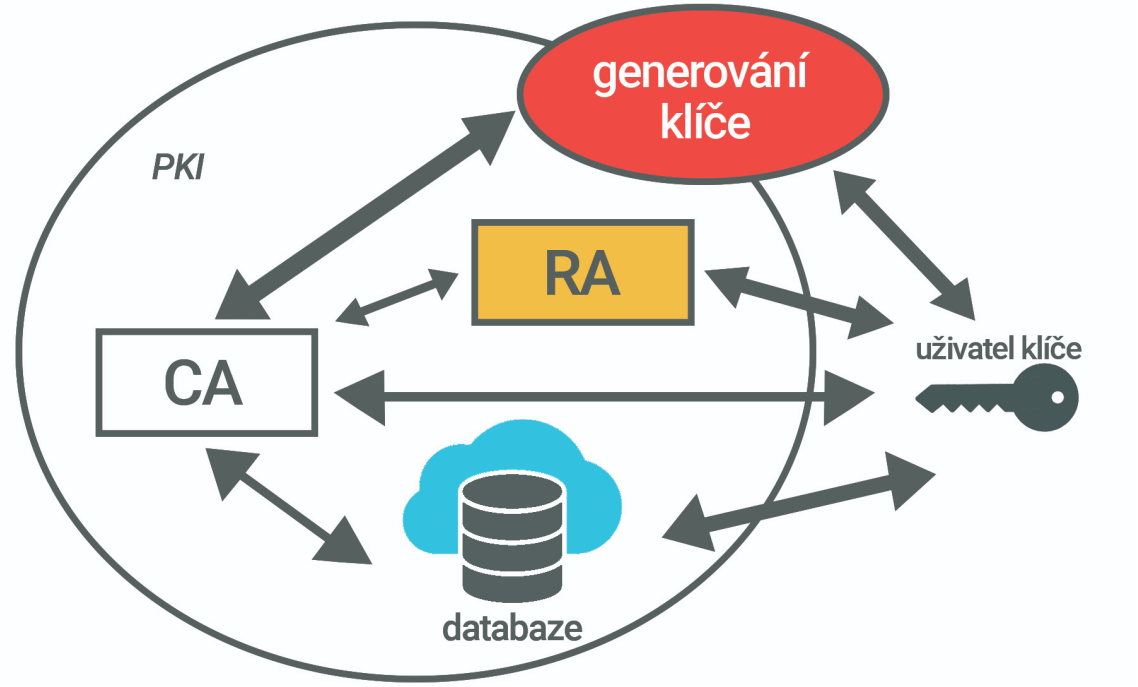
Formálně jde o funkci h, která převádí vstupní posloupnost bitů na posloupnost pevné délky n bitů: $h: D \rightarrow R$, *kde* $|D| \gg |R|$.

Přímo z této definice vyplývá, že existují kolize, to znamená existenci vstupních dat (x,y) takových, že $h(x) = h(y)$, tj. dvojice různých vstupních dat může mít stejný hash. Lze jen snižovat pravděpodobnost, že nastane kolize pro podobná data, například při náhodné změně v části vstupní posloupnosti. Cílem je tedy dosáhnout co nejvyšší pravděpodobnosti, že dvě zprávy se stejným hashem jsou stejné [17].

Hashovací funkce se nejčastěji využívají v hashovacích tabulkách, k rychlému nalezení dat pomocí vyhledávacího klíče (search key). Hashovací funkce se použijí k mapování vyhledávacího klíče do indexu pozice v hashovací tabulce, kde jsou pravděpodobně hledaná data uložena. Obecně, může hashovací funkce mapovat několik rozdílných klíčů na stejnou hashovací hodnotu. Hashovací funkce pouze ukazuje na místo, kde by se mělo začít hledat. Proto každá pozice hashovací tabulky obsahuje soubor záznamů a ne pouze jeden záznam. Z tohoto důvodu je pozice v hashovací tabulce často nazývána oblast (bucket) a hashovací hodnoty nazývány ukazatele na oblast (bucket indicies) [17].

4.3 Mechanismus podepisování elektronickým podpisem

Na níže uvedeném obrázku je podrobně znázorněna celá struktura CA (viz obr. 4.2).



Obr. 4.2: CA - struktura.

Základní komponety implementace PKI jsou:

- CA - funkční entita vydávající certifikáty,
- repozitář klíčů, certifikátů a CRL - je obvykle provozován na základě adresářové služby podle standardu LDAP (Light-weight Directory Access Protocol),
- správní funkce - zpravidla implementované prostřednictvím řídící konsole,
- další rozšiřující služby - obnova platnosti klíče a RA (automatizovaná nebo manuální).

Certifikační proces probíhá v následujících krocích:

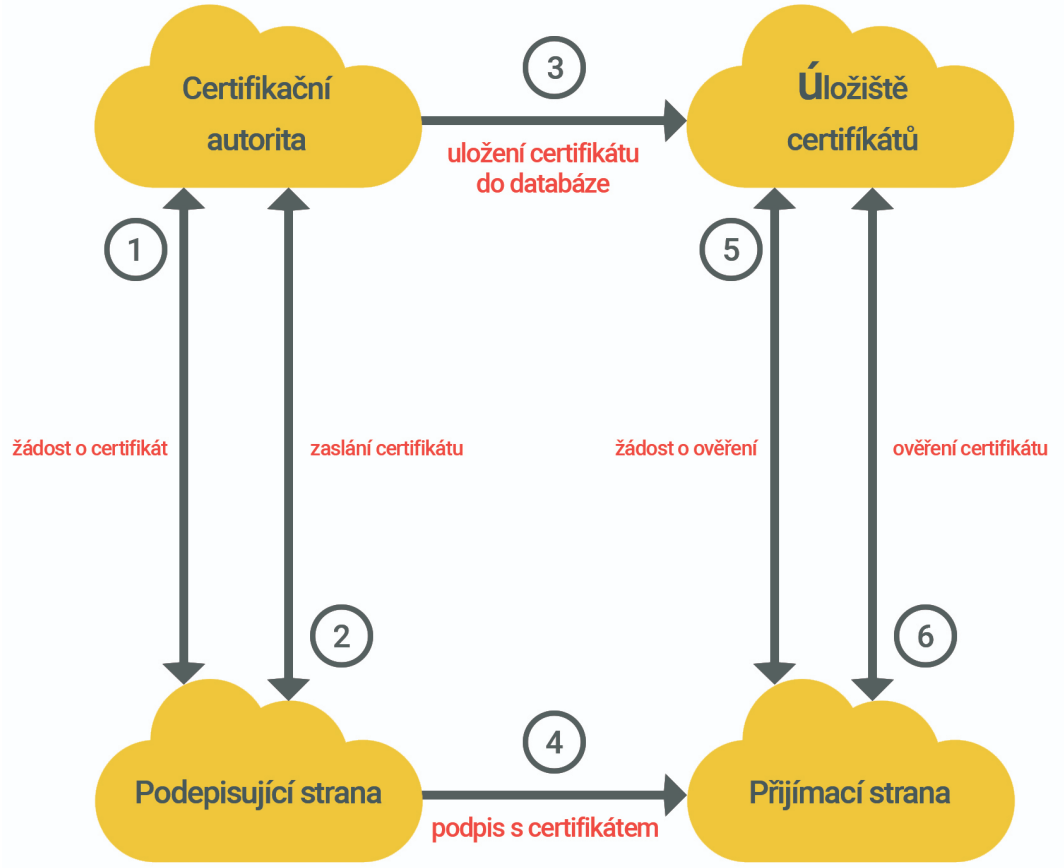
- odesílatel podepisovaného dokumentu žádá CA o elektronický certifikát pro svůj veřejný klíč
- CA ověřuje identitu žadatele a certifikát vydává,
- CA ukládá certifikát do veřejně přístupného on-line repozitáře,
- odesílatel podepisuje dokument svým privátním klíče a odesílá jej s připojeným certifikátem,

- příjemce ověřuje elektronický podpis veřejným klíčem odesílatele a požaduje ověření elektronickýho certifikátu v repozitáři příslušné CA,
- repozitář vrací zprávu o stavu odesílatelova certifikátu [22].

Typy certifikátů:

- podle subjektu - vlastníka veřejného klíče (fyzická nebo právnická osoba),
- zařízení (server, směrovač),
- aplikace,
- podle účelu použití - obecné použití, jednoúčelové použití, e-government,
- podle úrovně důvěryhodnosti - třídy důvěryhodnosti - definováno v Certifikační politice nebo v prováděcích směrnicích CPS (CPS - Certification Practice Statement) [22].

Následující obrázek ukazuje postup certifikačního procesu (viz obr. 4.3.)



Obr. 4.3: Postup certifikačního procesu.

5 Elektronický podpis v České republice

Za elektronický podpis je považován určitý proces, který vyplývá z rozhodnutí osoby, která daný dokument podepisuje a který stvrzuje identitu této osoby. Pokud hovoříme o elektronickém podpisu, máme na mysli výsledek, který je nezávislý na zvláštnostech situace, osob či technologie.

S elektronickým podpisem jsou spojeny údaje vytvořené zvláštním postupem s využitím kryptografie. Tento podpis poskytuje především následující funkce:

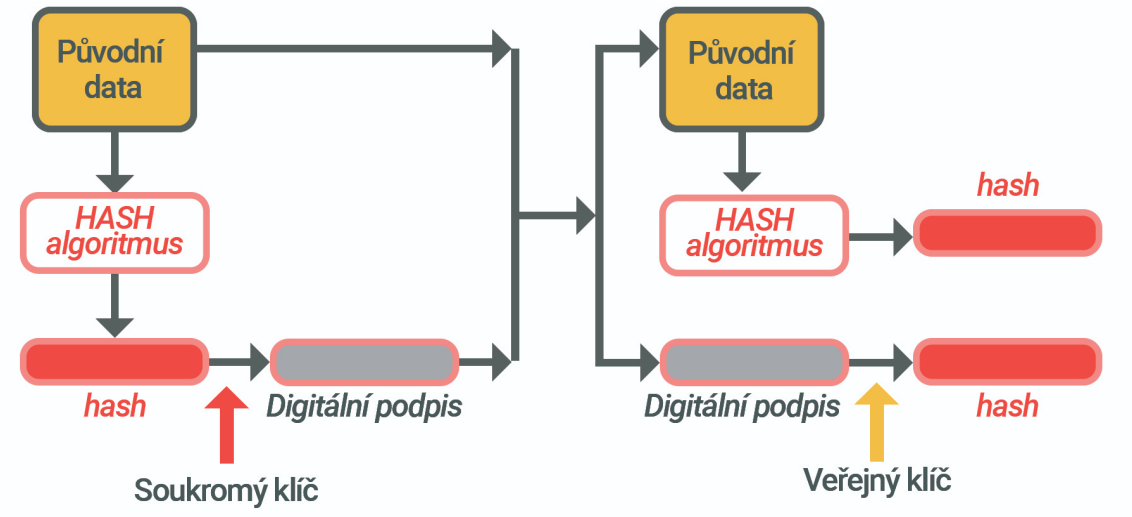
- podává identifikace původce podpisu,
- zaručuje integritu dané zprávy,
- zaručuje nepopiratelnost dokumentu,
- je tvořen prostřednictvím prostředků, které má pod svou výhradní kontrolou podepisující osoba.

Pro uživatele elektronického podpisu není bezpodmínečně nutné rozumět tomu, jak podpis funguje, ale je důležité především to, umět si zajistit prostředky pro jeho vytvoření a vše potřebné za něj udělá počítač. Postup je totiž poměrně složitý. Jako první se vezme tzv. otisk dokumentu představující datový řetězec, který má konkrétní délku a který označuje charakteristiku obsah daného dokumentu. Takto pořízený otisk se pomocí soukromého klíče podepisujícího podepíše. Tímto způsobem vznikne elektronický podpis, který společně s původním obsahem dokumentu tvoří dokument podepsaný elektronicky. Ověření pravosti podpisu pak provádí příjemce dokumentu. Příjemce dokumentu pak ověří pravost podpisu tak, že vytvořený otisk porovná s otiskem získaným v procesu ověřování elektronického podpisu veřejným klíčem podepisujícího. Co se týká platnosti veřejného klíče podepisujícího, ten je potvrzen certifikátem, který je vydáván a podepsán tzv. certifikační autoritou. Díky této kontrole si příjemce může být jist, že dokument opravdu přišel od toho, od koho měl a také to, že jeho obsah se nezměnil [23].

Počítač dovede prostřednictvím porovnání shody dokumentu a otisku potvrdit, že v daném dokumentu nebyla od jeho podepsání provedena žádná změna a také jednoznačně a nezpochybnitelně určit, pomocí jakého certifikátu byl podpis ověřen. Příjemce takto elektronicky podepsaného dokumentu může být díky shodě podpisu ubezpečen o dvou následujících skutečnostech:

- v zaslaném dokumentu nebyla provedena změna,
- dokument by podepsán elektronicky a díky tomu byl zabezpečen vlastníkem konkrétního certifikátu. Dokument je tedy možné spojit s tím, kdo jej podepsal [23].

Elektronický podpis je vytvořen prostřednictvím asymetrických kryptografických schémat, které se mění společně s vývojem nových verzí takovým způsobem, aby v budoucnu nemělo dojít k tomu, aby se někdo pokusil dokument změnit či zfalšovat viz obr. 5.1.



Obr. 5.1: Princip elektronickýho podpisu.

Elektronický podpis nezjišťuje důvěrnost podepsaného dokumentu. Případně vyžádaná důvěrnost musí být zajištěna dodatečně, např. zašifrováním podepsaného dokumentu veřejným klíčem příjemce. Efektivní využití elektronickýho podpisu je podmíněno nutností zajistit jednoznačné spojení podepisujícího subjektu s veřejným klíčem, o kterém prohlašuje, že je jeho vlastníkem. Automatizovanou správou veřejných klíčů zajišťuje PKI (Public Key Infrastructure), představující důvěryhodnou třetí stranu v procesech ověřování pravosti veřejného klíče v podpisových transakcích. Opírá se o řadu standardů a doporučení sjednocujících přístupy různých poskytovatelů těchto služeb.

Elektronický podpis je využíván např.:

- v elektronickém poštovním styku,
- v elektronické komerci (e-commerce, e-payment, EDI - "Electronic Data Interchange, SET - "Secure Electronic Transaction"),
- v elektronických bankovních transakcích (e-banking),
- při podávání elektronických dokladů útvarům státní správy (e-government),
- v notářských procedurách (ověření dokumentu apod.), atd.[22].

5.1 Typy elektronického podpisu

Dne 19.9.2016 nabyl účinnosti zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, který spolu se změnovým zákonem č. 298/2016 Sb. zrušil původní zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Český zákonodárce tak reagoval na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23.7.2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, účinné zčásti ode dne 17.9.2014 a zčásti ode dne 1.7.2016 [24].

Zákon v návaznosti na nařízení eIDAS upravuje zejména požadavky na podepisování dokumentů v závislosti na podepisující osobě a osobě, vůči níž je právně jednáno, vymezuje postupy kvalifikovaných poskytovatelů služeb vytvářejících důvěru, které vydávají certifikáty ověřující identitu podepisujících osob, a dále také vymezuje působnost Ministerstva vnitra v této oblasti, jakož i sankce, které může tento orgán v rámci svého dohledu uložit [24].

Elektronickým podpisem se rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání (srov. čl. 3 bod 10 nařízení eIDAS).

Obecně lze říci, že fyzické osoby, resp. soukromoprávní subjekty opatřují své dokumenty elektronickými podpisy (ať již prostým či uznávaným), zatímco u orgánů veřejné moci hovoříme o kvalifikovaném podpisu, pokud Zákon vyžaduje tuto formu, a pokud tuto formu nevyžaduje, je namístě použít kvalifikovanou elektronickou pečeť spolu s časovým razítkem (jehož předchůdcem byla elektronická značka).

Nejvyšší formou elektronického podpisu je **kvalifikovaný elektronický podpis** (§ 5 Zákona). Tuto formu musí používat orgány veřejné moci a jiné fyzické či právnické osoby při výkonu působnosti v oblasti veřejné správy, podepisují-li elektronický dokument, kterým právně jednají [24].

Uznávaný elektronický podpis (§ 6) používá soukromoprávní osoba, pokud právně jedná vůči veřejnoprávnímu podepisujícímu. Zákon stanoví, že takovým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu, vydaném tzv. kvalifikovaným poskytovatelem služeb vytvářejících důvěru, nejedná se o podpis kvalifikovaný.

Prostý elektronický podpis se používá k podepisování elektronického dokumentu a právně se jedná mezi osobami soukromého práva. Pokud by jednající soukromoprávní osoba chtěla postavit najisto splnění funkce ověření totožnosti podepisující osoby, může rovněž využít kvalifikovaného elektronického podpisu.

Kvalifikované elektronické pečeti, značky a časová razítka. Nestanoví-li právní předpis, že veřejnoprávní podepisující musí opatřit své právní jednání kva-

lifikovaným elektronickým podpisem, postačí kvalifikovaná elektronická pečeť (§ 8 Zákona). V praxi půjde zpravidla o strojově vyhotovené dokumenty jako např. výpisy z obchodního rejstříku či jiného veřejného rejstříku. Dále by podepisující osoba měla tento dokument opatřit kvalifikovaným elektronickým časovým razítkem [24].

5.2 Kvalifikovaný certifikát pro elektronický podpis

Kvalifikované certifikáty jsou určeny pro komunikaci občanů s orgány veřejné moci, současně se využívají také pro komerční účely. Kvalifikovaný certifikát pro elektronický podpis je možné využít k vytváření elektronického podpisu a jeho ověřování. Jiné využití, jako je například šifrování zpráv, je omezeno legislativou.

Kvalifikovaný certifikát vydávaný I.CA splňuje veškeré požadavky dané zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce a nařízením č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS). Ve spojení s čipovou kartou řady Starcos a uživatelskou aplikací I.CA SecureStore, které jsou certifikovány jako kvalifikovaný prostředek pro vytváření elektronických podpisů (QESCD), jej lze používat pro vytváření tzv. kvalifikovaného elektronického podpisu dle eIDAS [25].

I.CA vydává následující typy kvalifikovaných certifikátů:

- kvalifikovaný certifikát pro elektronický podpis – osobní, pro fyzické osoby, do certifikátu lze naplnit osobní údaje žadatele, vydáván na Registrační autoritě I.CA,
- kvalifikovaný certifikát pro elektronický podpis – zaměstnanecký/OSVČ, určen pro fyzické osoby zaměstnance nebo OSVČ, do certifikátu lze naplnit k údajům žadatele také identifikaci zaměstnavatele, živnosti, vydáván na Registrační autoritě I.CA,
- kvalifikovaný certifikát pro elektronický podpis – pseudonym, určen pro fyzické osoby, do certifikátu lze naplnit libovolný údaj. vydáván na Registrační autoritě I.CA [25].

5.3 Certifikační autorita

První certifikační autorita, a.s. (I.CA) byla založena v roce 2001 jako dceřiná společnost PVT, a.s. Převzala od mateřské společnosti veškeré činnosti související s poskytováním služeb certifikační autority, která byla v rámci PVT, a.s. provozována již od roku 1996.

I.CA, jako první v České republice, získala v roce 2001 osvědčení pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. V roce 2006 získala akreditaci také pro vydávání kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek a rovněž akreditaci pro vydávání kvalifikovaných certifikátů a pro poskytování služby časové autority na Slovensku [26].

Účinností nařízení EU č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) se I.CA stala kvalifikovaným poskytovatelem služeb vytvářejících důvěru v rámci EU.

I.CA je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice a na Slovensku. Hlavní náplní společnosti je zajišťování činností bezprostředně souvisejících s poskytováním služeb certifikační autority a časové autority [26].

V současnosti je I.CA vlastněna několika významnými společnostmi, kterými jsou:

- Česká spořitelna, a.s.,
- Československá obchodní banka, a. s.,
- O2 Czech Republic a.s.,
- Asseco Central Europe, a.s.,
- STÁTNÍ TISKÁRNA CENIN, státní podnik [26].

Vydávání kvalifikovaných certifikátů je upraveno nařízením EU č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) a zákonem č.297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. K jejich vydávání je oprávněn pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, kterým je První certifikační autorita, a.s. (I.CA) pro tyto služby od roku 2002 pro ČR a od roku 2006 také pro Slovensko [26].

5.4 Datová schránka

Datová schránka je elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci, a dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Datové schránky zřizuje a spravuje ministerstvo vnitra [27].

Základní druhy datových schránek:

- datová schránka orgánů veřejné moci,
- datová schránka pro právnické osoby,

- datová schránka pro fyzické osoby podnikající,
- datová schránka pro fyzické osoby [23].

Integrovaný systém datových schránek doručuje informace ze schránky odesílatele do schránky příjemce ve formě datových zpráv. Odesílatelem i příjemcem může být fyzická osoba, podnikající fyzická osoba, právnická osoba a orgán veřejné moci.

Datovou schránku tak lze přirovnat ke schránce elektronické pošty. Každá datová schránka představuje datové uložiště, které je určeno k doručování datových zpráv, potřebných jako podklady k úkonům orgánům veřejné moci [23].

Datové schránky zřizuje a spravuje Ministerstvo vnitra. Každá datová schránka je určená svou adresou, která je unikátní a schránkou v celém systému ISDS jednoznačně identifikuje.

Datová zpráva se skládá ze dvou částí:

- z obálky – obsahuje údaje o odesílateli a příjemci, informace potřebné k popisu datové zprávy,
- příloha – vlastní datová zpráva, skládá se z jednoho nebo více souborů [23].

Použití datových schránek může být buď:

- povinně
  - obousměrná komunikace orgánů veřejné moci mezi sebou,
  - komunikace orgánů veřejné moci vůči některým právnickým osobám,
  - komunikace orgánů veřejné moci vůči právnickým nebo fyzickým osobám, které si datovou schránku zřídily dobrovolně, nebo jim byla zřízena na základě zákona,
- nepovinně
  - komunikace fyzických osob vůči orgánům veřejné moci,
  - komunikace podnikajících osob mezi sebou za jistých okolností,
  - předmětem úvah je širší využití datových schránek pro neomezenou komunikaci mezi fyzickými a právnickými osobami [27].

Veškerá komunikace v oblasti veřejné správy by měla probíhat elektronicky, v případě orgánů veřejné moci je za účelem snížení ekonomických nákladů stanoveno povinné použití elektronické formy komunikace.

Pokud má fyzická či právnická osoba zřízenu datovou schránku, musí orgán veřejné moci doručovat v elektronické formě právě do datové schránky dané osoby. K přístupu do jedné datové schránky může mít oprávnění více osob [27].

Do datové schránky mají přístup pouze držitelé datové schránky (oprávněné osoby), popřípadě jimi Pověřená osoba či Administrátor. Správce ani Provozovatel Informačního systému datových schránek nejsou oprávněni k přístupu do datových

schránek jiných subjektů. Obsah datových zpráv je přístupný výhradně jejich odesílateli a příjemci.

Informační systém datových schránek je uzavřeným systémem, který obsahuje datové schránky, metadata o uživatelích a jejich oprávněních a o datových zprávách, které jsou prostřednictvím tohoto systému „zasílány“ (fyzicky k žádnému faktickému zasílání nedochází, zpráva je uložena na serveru v datové schránce, dokud ji z této schránky adresát nevybere). V principu se jedná o informační systém postavený nad databází, se kterým je možné komunikovat prostřednictvím grafického uživatelského rozhraní, a rozhraní poskytující webové služby jiným informačním systémům. Nejde tedy o klasický e-mailový systém, kde jsou zprávy posílány z jednoho serveru na druhý. Systém umožňuje také přeposlání zprávy na e-mail (jako přílohu), např. na adresu elektronické podatelny [27].

K bezpečnému používání datové schránky stanoví zákon pro uživatele dva základní postupy:

- obezřetné zacházení s přístupovými údaji (§ 9 zákona),
- zneplatnění přístupových údajů v mimořádném případě na základě oznámení (§ 12 zákona).

Informace o komunikaci s datovou schránkou, obsah přenášených zpráv i zacházení s přístupovými údaji, i když se jedná o datovou schránku právnické osoby, jsou přiřaditelné ke konkrétní oprávněné fyzické osobě a již z tohoto důvodu je třeba dodržovat povinnosti požadované zákonem č. 101/2000 Sb., o ochraně osobních údajů [27].

6 Elektronický podpis v Rusku

V roce 2002 začal startovat program nesoucí název „Elektronické Rusko 2002–2010“, který si kladl za cíl následující:

- rozpracování a vytváření elektronického obchodování,
- rozvoj telekomunikační infrastruktury,
- rozvoj systému přípravy odborníků v oblasti komunikační a informační technologie a také kvalifikovaných uživatelů [28].

První federální zákon č. 1 - FZ „o elektronickém podpisu“ začal v Rusku platit v roce 2002 a jeho vznik jeho významu byl přirovnáván k zavedení občanských průkazů. Vznik tohoto zákona se datuje na začátek 90. let. Vedle tohoto zákona řeší tuto problematiku také zákon o informaci, informačním rozvoji a chránění informace, zákona o komunikace a podle jiných právních předpisů Ruské federace. Hlavním cílem první části zákona bylo poskytnout právní rámec upravující používání elektronického podpisu při podepisování elektronických dokumentů a postavení tohoto podpisu na úroveň podpisu vlastnoručního [29]. Druhá část zákona se zabývá podmínkami pro použití podpisu, která se zabývá zejména otázkami právní relevantnosti elektronického podpisu a také prostředků pro jeho vytváření. Součástí zákona je dále stanovení minimálního požadavku na informace, které musí být součástí certifikátu. Konkrétně se jedná o následující informace:

- ty, které certifikát identifikují,
- ty, které umožňují identifikovat poskytovatele certifikátu,
- ty, které umožňují identifikovat držitele certifikátu [29].

Se získáním potřebného certifikátu je také spojen pojem certifikační autorita, kterou zákon definuje jako obchodní společnost, vlastníka licence. Co se týká podmínek, které musí být pro získání licence splněny, ty nejsou v zákoně konkrétně uvedeny, ale je v něm uveden odkaz na právní předpis, který je stanoví. Zákon také nezapomíná na používání elektronického podpisu v oblasti státní správy a samosprávy. Za vládní orgány a za orgány samosprávy se elektronickým podpisem musí podepisovat pouze fyzická osoba, která je k takovým transakcím zmocněna. V neposlední řadě jsou obecně stanovené zásady, které jsou nezbytné pro to, aby byly uznány zahraniční certifikáty a elektronické podpisy [29].

Elektronický podpis byl v Rusku používán i před zavedením zákona a podle občanského kodexu byl srovnatelný s vlastnoručním podpisem, který se však mohl používat pouze po dohodě zainteresovaných stran. Pokud došlo k nějaké konfliktní situaci, dokumenty podepsané elektronickým podpisem nebyly akceptovány. V Rusku pak může elektronický podpis získat pouze fyzická osoba a elektronické podpisy

zahraničních firem, které jsou vydané v cizině, v Rusku neplatí. Pokud chce elektronický podpis využívat zahraniční právnická osoba, musí si vybrat nějakého představitele, kterým je fyzická osoba a která tak může tento podpis získat od ruského autorizačního centra. Zrovnoprávnění elektronického podpisu s podpisem vlastnoručním je pak splněno podle zákona v následujících bodech:

- v okamžiku kontroly nebo v době podepisování elektronického dokumentu je certifikát klíče podpisu spojený s elektronickým podpisem stále platný,
- pravost elektronického podpisu v elektronickém dokumentu je potvrzena,
- elektronický podpis se používá podle informace, která je uvedena v certifikátu klíče podpisu.

Ruský zákon o elektronickém podpisu stanovuje následující dva typy informačního systému:

- informační systém obecného používání = jedná se o systém, jež mohou využívat nejen právnické, ale také fyzické osoby, přičemž jim toto užívání nemůže být zakázáno,
- korporativní informační systém = jedná se o systém, jež používá pouze omezená skupina uživatel, které určuje společně s pravidly užívání majitel korporativního informačního systému.

V Rusku si však zákon o elektronickém podpisu nezískal příliš velikou popularitu. Za tímto faktem stojí zejména následující důvody:

- nízká rychlost internetu,
- málo kvalitních počítačů,
- strach z něčeho nového,
- vysoká úroveň byrokracie.

V souvislosti s právními předpisy země, je možné se setkat s možností komunikovat s úřady přes internet. Ve většině případu je však na internetových stránkách těchto úřadů udělána pouze úvodní strana společně se základními informacemi, podle kterých je možno nechat stížnost, připomínky atd. Využití elektronického podpisu patří spíše do vzájemné komunikace s bankou a právnickými osobami. V dubnu roku 2010 přestavilo Rusko program s názvem Elektronická společnost, prostřednictvím kterého se budou občané moci objednat k lékaři, nebo zaplatit pokutu. Úpravou časového razítka se zabývá zákon o elektronickém podpisu, ale v případě, že by byla potřeba jej využít, tato možnost je nabízena akreditovaným poskytovatelem certifikačních služeb [28].

Pravdou však je, že v ruském právním řádu je možné se setkat s určitými ustanoveními, kterých se týkala e-Commerce. Příkladem takového ustanovení, je například

paragraf 106 ruského občanského zákoníku stanovující, že vlastnoruční podpis lze nahradit podpisem elektronickým, ale jen v případě, že tuto náhradu umožňuje jiný existující zvláštní zákon, nebo v případě, že se obě strany dohodnou. Jednalo se o ustanovení, které neupravovalo komunikaci se státní správou. Ruský občanský zákoník také obsahoval další významné ustanovení, které stanovuje možnost uzavírání smluv elektronickou cestou. Toto ustanovení upravuje přijímání elektronické dokumenty v oblasti plateb a bankovnictví, a to na základě nařízení, které vydala Ruská centrální banka. Možnost užívání elektronických dokumentů se objevovala také v oblasti penzijních fondů [29].

Role elektronického podpisu byla pak v Rusku uznána až zákonem z roku 2011, kdy byl přijat zákon číslo 63-FZ O elektronickém podpisu. Podle zákona se jedná o zvláštní typy informací v elektronické podobě. Tyto informace jsou připojeny k druhé za účelem určení totožnosti původce. Předkládaný normativní akt je tedy určen k regulaci vztahů v oblasti užívání elektronických podpisů pro právní konsolidaci občanských a právních transakcí, obecních nebo státních služeb apod.

Elektronické podpisy jsou vyjádřeny formou zvláštních certifikátů, které obsahují klíče. Takové certifikáty vydávají příslušné orgány pro jejich další použití. Majitelé takových certifikátů jsou tedy osoby, které potřebují právní registraci určitých dokumentů. Začíná to s vlastnostmi jednoduchého podpisu. Jsou to všechny druhy kódů, hesel a další prostředky. Potvrzují to podpis elektronické úrovně. Jednoduchý je obvykle používán při uzavření "lehkých"transakcí, stejně jako u dohod, které nejsou považovány za velké. V tomto případě je právo na výběr podpisu dáno účastníkům procesu předání dokumentu [29].

Komplexní podpis nekvalifikovaného typu je určen pro následující operace:

- kryptografická transformace informací;
- určení osoby, která obdrží elektronický dokument;
- zjišťování skutečnosti o změně elektronického dokumentu [29].

Potvrzení dokumentu ve formě malby kvalifikovaného komplexního typu podle FZ-63 "Elektronický podpis"je nezbytné pro následující akce:

- ověření malby v certifikátech kvalifikované povahy;
- formování a ověřování obrazů v jednotlivých dokumentech, jejichž seznam je uveden ve zmiňovaném federálním právu.

Cílem zákona 63-Fz je poskytnout právní rámec pro používání elektronického podpisu v elektronických dokumentech a elektronický podpis postavit na roveň podpisu vlastnoručnímu. Paragraf 3 zákona definuje elektronický dokument jako typ dokumentu, kde jsou informace prezentovány elektronickou formou. Druhá část zákona nazvaná podmínky pro použití elektronického podpisu upravuje především otázky

právní relevantnosti elektronického podpisu a prostředků pro jeho vytváření. Jako stěžejní se jeví paragraf 4, druhé části, který stanovuje, že elektronický elektronický podpis použitý v elektronickém dokumentu bude ekvivalentní podpisu vlastnoručnímu za předpokladu, že budou splněny dané podmínky:

- certifikát vztahující se k elektronickému podpisu je platný,
- podepisující se osoba byla ověřena (private-public key proccess),
- elektronický podpis byl použit v souladu s podmínkami stanovenými v certifikátu [29].

V zákoně je stanoven minimální požadavek na informace, které musí certifikát obsahovat. Jedná se o informace, které umožňují identifikovat certifikát samotný, které umožňují identifikovat poskytovatele certifikátu a informace a které umožňují identifikovat držitele certifikátu. Certifikační autorita je v zákoně definována jako obchodní společnost a tedy patrně není možné, aby certifikáty vydávala fyzická osoba nebo správní orgán. Aby certifikačni autorita mohla vykonávat svoji činnost, musí získat licenci. Podmínky získáváni licence ale nejsou v zákoně samotném stanoveny (v zákoně je pouze odkaz na zvláštní právní předpis). Za vládní orgány stejně tak jako za orgány samosprávy se elektronicky bude podepisovat speciálně k tomuto právnímu úkonu zmocněná fyzická osoba. Tento zákonen také stanovuje obecné zásady, které slouží i pro uznáni zahraničních certifikátů a elektronických podpisů [29].

6.1 Druh elektronického podpisu

Ruská legislativa stanoví 3 hlavní typy elektronického podpisu:

- **jednoduchý elektronický podpis** - elektronický podpis, který pomocí kódů, hesel nebo jiných prostředků potvrzuje skutečnost, že elektronický podpis je generován konkrétní osobou;
- **vylepšený nekvalifikovaný elektronický podpis** (nekvalifikovaný elektronický podpis) - elektronický podpis, který je získán v důsledku kryptografické konverze informací pomocí klíče elektronického podpisu, a umožňuje vám identifikovat osobu, která elektronický dokument podepsala, a zjistit, zda po dokumentu došlo k jeho změnám, jakož i vytvořené pomocí nástrojů pro elektronický podpis;
- **rozšířený kvalifikovaný elektronický podpis** (kvalifikovaný elektronický podpis) - elektronický podpis, který je získán v důsledku kryptografické konverze informací pomocí klíče elektronického podpisu, umožňuje identifikovat osobu, která elektronický dokument podepsala, a zjistit, že dokument byl po podpisu změněn a je také vytvořen pomocí elektronického podpisu. Současně

je klíč k ověření elektronických podpisů uveden v kvalifikovaném certifikátu a prostředky elektronického podpisu se používají k vytváření / ověřování elektronických podpisů, které obdržely potvrzení o splnění požadavků stanovených v souladu s právními předpisy Ruské federace v této oblasti.Byly zavedeny tyto typy regulace: jednoduchý elektronický podpis a vylepšený elektronický podpis. Kromě toho může být vylepšený elektronický podpis kvalifikovaný a nekvalifikovaný [30].

Elektronický podpis v Ruské federaci používají fyzické a právnické osoby a je analogem vlastnoručního podpisu oprávněné osoby na papíře a zapečetěných, pouze pokud jde o udělení právní moci elektronickému dokumentu.

Hlavní cíle používání elektronického podpisu jsou:

- společnost pro správu elektronických dokumentů,
- účast na elektronickém obchodování na platformách elektronického obchodování,
- podávání zpráv vládním orgánům,
- výhody použití elektronického podpisu pro organizaci jsou následující,
- zkrácení doby výměny dokumentů a transakcí,
- snížení nákladů na vytvoření, doručení, uložení dokumentů,
- záruky spolehlivosti a důvěrnosti přenášených informací,
- efektivní systém výměny dokumentů pro zaměstnance společnosti,
- odstranění problému přítomnosti / nepřítomnosti oprávnění podepisovat určité dokumenty [30].

Díky elektronické správě dokumentů pomocí elektronického podpisu je tedy možné vyhnout se množství problémů se správou papírových dokumentů, významně zkrátit čas na výměnu informací a zvýšit efektivitu organizace jako celku. Všechna zařízení, a to včetně čipů nebo USB klíče, které se v Rusko používají při elektronickém podpisu, musí odpovídat ruské normě GOST. K vytváření a ověřování elektronických podpisů (hashů) lze použít pouze ruské algoritmy a použití cizího kryptografického softwaru je zakázáno. Výjimky se týkají pouze prodejců, kteří byli dobrovolně certifikováni FSB. Certifikace zahrnuje přenos zdrojových kódů obsahujících algoritmy k ověření softwaru pro elektronický podpis. Tyto podpisy se používají například v oblasti bankovnictví, a to například u platebních příkazů, hotovostních příkazů, žádostí o platbu a podobných finančních dokumentů, musí být vytvořen podle ruského GOST. Přestože se GOST liší od globálních standardů algoritmů, používají analoga. Například GOST 28147-89 je matematická základna kryptografického algoritmu DES .

Automatizované bankovní systémy a služby vzdáleného bankovnictví však pou-

žívají kryptografii uznávané mezinárodní standardy. Asymetrické algoritmy, Diffie-Hellman, El Gamal nebo RSA, se používají k vytvoření bezpečné komunikační relace a výměny klíčů mezi klientským zařízením a veřejným serverem banky. Přenos dat z jedné banky do druhé probíhá prostřednictvím zabezpečeného kanálu VPN kódovaného protokolem IPsec nebo Russian GOST, který může být zapouzdřen, tj. tzv. Dvojitým šifrováním „tunel v tunelu“. Ruský standard ESS je přístupný veřejnosti a je popsán v GOST R 34.10-2012 . Zahraniční vývojáři k němu mají snadný přístup, když je třeba přizpůsobit svůj software tomu, co vyžaduje ruské právo. Kromě dat ESS se GOST R 34.10-2012 používá v zabezpečených protokolech, jako jsou TSL, HTTPS , XML Encryption a DNSSEC.

6.2 Komparace právní úpravy elektronického podpisu v ČR a Rusku

V rámci zákona zabývající se elektronickým podpisem se lze setkat se základním rozdělení zákona, které je následující:

- obecná ustanovení = součástí Českého i Ruského zákona je popis cíle, vymezení oblastí používání elektronického podpisu, regulace právních vztahu při použití elektronického podpisu a také vymezení základních pojmů,
- regulace podmínek použití elektronického podpisu = jak v Rusku, tak v České republice se jedná o podmínky, za jakých je možno zrovnoprávnit elektronický a vlastnoruční podpis. Součástí této části je také popis jeho používání a oblast týkající se certifikátu podpisového klíče,
- poskytovatele certifikačních služeb = co se týká poskytovatelů, je v obou zákonech součástí této části popis vztahů, které panují mezi poskytovatelem certifikačních služeb a organem veřejné moci. Dále povinnosti tohoto poskytovatele, ale také jeho majitele. Lze zde nalézt také problematiku anulování a přerušení platnosti certifikátu či jeho zánik,
- zvláštní podmínky upravující používání elektronického podpisu = tato část zákona pojednává o používání elektronického podpisu v oblasti veřejné moci, v rámci podnikového informačního systému a také uznávání zahraničního certifikátu. To je v Rusku a České republice stejné,
- závěrečná ustanovení = v této části zákona lze pozorovat první rozdíl mezi ruským a českým zákonem. V ruském zákonu nelze najít pojmy jako elektronická značka, časové razítko a elektronická podatelna. Ruský zákon obsahuje v oblasti odpovědnosti certifikační autority pouze obecně blíže nespecifikované ustanovení to, že tato autorita musí disponovat potřebnými finančními prostředky v případě, že bude potřeba pokrýt způsobené škody. Dalším rozdílem

je to, že z pohledu mezinárodního uznávání certifikátů je ruský zákon příliš obecný, jelikož se zabývá pouze možností, že lze zahraniční certifikát uznat, ale již nestanovuje minimální podmínky a ani kritéria pro takové uznání [31].

Vymezením pojmu elektronického podpisu se zákon České republiky a Ruska také liší. Český zákon jej vymezuje jako údaje v elektronické podobě připojující se k datové zprávě, nebo jako údaje logicky s nimi spojené sloužící jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. Ruský zákon pak definuje elektronický podpis jako tzv. „rekvizit elektronického dokumentu určený k ochraně tohoto dokumentu proti padělání“. Jedná se o podpis, který je výsledkem kryptografické transformace prostřednictvím soukromého klíče elektronickýho podpisu a který umožňuje identifikaci vlastníka certifikátu klíče podpisu, a také zjistit absenc narušení informací v elektronickém dokumentu. Ruský zákon vymezuje elektronický podpis a také jasně určuje způsob jeho vytváření, které se tvoří pomocí technologie publickey-cryptografy. Hlavním rozdílem mezi českým a ruský zákonem je v tom, že ruský zákon nezná tzv. technologickou neutralitu, která spočívá v tom, že technický pokrok se velmi rychle vyvíjí, a proto je potřeba vytvořit rámcovou normu, která se nebude muset díky tomuto pokroku neustále měnit. V Ruském zákonu se pak používá název elektronický dokument, zatímco v českém se používá pojem elektronické údaje [31].

Český zákon si klade za cíl kontrolovat povinnosti, které jsou stanoveny českým zákonem o elektronickém podpisu a při jejich porušení udělovat příslušné sankce. Ruský zákon považuje za cíl poskytovat právní podmínky, které jsou důležité pro použití elektronických podpisů v elektronických dokumentech. Pokud jsou tyto podmínky splněny, je tento podpis přiznán ekvivalentně k vlastnoručnímu podpisu v listinných podobách dokumentu. Jak ruský, tak český zákon upravuje právní rámec a technické aspekty jeho používání a český zákon navíc stanoví jako další cíl kontrolu těchto povinností.

7 Elektronický podpis ve státech Pobaltí

7.1 Litva

V Litvě je za elektronickou komunikaci odpovědný regulační úřad pro komunikaci Litevské republiky. Co se týká legislativy, v Litvě existuje Zákon o elektronické identifikaci a důvěryhodných službách pro elektronické transakce. Tento zákon upřesňuje postup pro udělování statusu kvalifikovaných poskytovatelů důvěryhodného seznamu a poskytování zpráv o činnosti kvalifikovaných poskytovatelů důvěryhodných služeb schválených příkazem č.1V-588 ředitelem Komunikačního regulačního úřadu ze dne 21. června 2018.

Příkazem číslo 1V-1055 ze dne 26. října 2018, schváleným ředitelem Komunikačního regulačního úřadu, jsou upravovány specifikace pro identifikaci osobní identity a dalších specifických atributů pro vydávání kvalifikovaných certifikátů pro elektronické podpisy, elektronické pečeti a autentizace webových stránek.

Článek 147 ze Zákona o elektronické identifikaci a důvěryhodných službách pro elektronické transakce pak určuje sankce, které jsou udělovány poskytovatelům důvěryhodných služeb v případě, že by byly jejich požadavky porušeny. Elektronický podpis je pak povinný pro veřejné subjekty a doporučován pro podniky a občany.

7.1.1 Vnitrostátní právní předpisy a zákonnost elektronického podpisu

I do litevské úpravy problematiky elektronického podpisu je částečně implementováno nařízení eIDAS, které je dále doplněno zákonem o elektronické identifikaci a důvěryhodných službách pro elektronické transakce. Právní účinek elektronického podpisu, který nesplňuje požadavky na kvalifikovaný elektronický podpis podle nařízení (EU) č. 910/2014, je rovnocenný právnímu účinku písemného podpisu, pokud se uživatelé tohoto elektronického podpisu dohodnou písemně předem a je možné dohodu uložit na trvalé médium. O používání nekvalifikovaného elektronického podpisu se pak neshromažďují žádné informace.

7.1.2 Použitelnost elektronického podpisu a certifikátů

V Litvě existuje jedno jediné kontaktní místo vnitrostátního systému elektronické veřejné správy, které umožňuje použití elektronických podpisů. Jedná se o `https://www.epaslaugos.lt/portal/en`. Komunikační regulační úřad Litvy má pak na starosti shromažďování informací, které se týkají používání elektronických podpisů od některých institucí veřejné správy a obchodních organizací a každoročně zadává

průzkum o používání elektronického podpisu. Tyto informace se používají k přípravě každoročního přezkumu, který je zveřejněn na vyhrazených webových stránkách. Podle uvedených statistik z roku 2018 se elektronický podpis používá hlavně pro veřejné služby a elektronické bankovnictví. Veřejnost je informována o elektronickém podpisu prostřednictvím vyhrazené webové stránky `www.elektroninisparasas.lt` , školení a konzultací, reklamy poskytovatelů služeb Trust, jakož i platforem elektronického podpisu a prostřednictvím jiných mediálních kanálů.

7.1.3 Distribuce podpisových certifikátů

V Litvě je možno se setkat s následujícími poskytovateli kvalifikovaných certifikátů pro elektronický podpis. Konkrétně se jedná o:

- centrum personalizace dokladů totožnosti pod Ministerstvem vnitra Litevské republiky sloužící pro veřejný prostor,
- státní podnikové centrum registrů.

Certifikáty elektronických podpisů distribuují poskytovatele služeb Trust a jejich partneři, kterými jsou například provozovatele mobilních sítí. Pro použití elektronického podpisu dokumentu je možno použít osobní průkaz totožnosti. V současné době je možno získat kvalifikovaný certifikát pouze osobním předložením Trusted Service Provider nebo na registračním úřadu [25].

Nejoblíbenějším formátem elektronických dokumentů ve veřejném sektoru je ADOC, která je založena na XML Advanced Electronic Signatures (XAdES). Specifikace elektronického dokumentu podepsaného elektronicky ADOC byla přijata v září roku 2009 a obsahuje zejména specifikaci elektronického podpisu. Tato specifikace definuje státní a obecní instituce, instituce a podniky, další subjekty oprávněné k výkonu funkcí veřejné správy připravované státem pověřenými osobami a přijímané od nevládních organizací, soukromých právnických a fyzických osob. Požadavky na úředně podepsané elektronické dokumenty (skupiny GeDOC a GGeDOC) a software pro jejich životní cyklus. Požadavky uvedené pro nevládní organizace, soukromé právnické a fyzické osoby jsou pouze informativní a to v případě, že připravované elektronické dokumenty nejsou určeny k předkládání institucí nebo vyžadované právnickými osobami.

Formáty elektronického podpisu jsou upravovány podle specifikace, která je v souladu s Popisem požadavků na elektronickou podpisovou specifikaci elektronického dokumentu, schváleným generálním ředitelem oddělení litevského archivu pod vládou Litevské republiky v červnu 2008. 9. října Objednací číslo V-119 (Úřední věstník, 2008, č. 118-4488). Tato specifikace také stanovuje požadavky na elektronické dokumenty podepsané pomocí konkrétních elektronických podpisů a vycházející z

norem a pokynů pro otevřený formát a elektronické podpisy. Vzájemná spolupráce druhů elektronických podpisů umožňuje, aby byl elektronický dokument vytvořený v jednom systému přenášen do jakéhokoli jiného systému, přičemž elektronický dokument může být ověřen na autentičnost a dlouhodobé uložení, pokud software těchto systémů splňuje požadavky na vytváření a ověřování elektronických dokumentů [32].

Tak, jako v jiných evropských státech, i Litva uznává tři typy elektronických podpisů:

- kvalifikovaný elektronický podpis – v algoritmu SHA-1 s RSA,
- jednoduchý elektronický podpis – v algoritmu RSA,
- pokročilý elektronický podpis – v algoritmu DSA.

7.2 Estonsko

Problematikou elektronického podpisu se v Estonsku zabývá Úřad pro estonský informační systém, a to od ledna roku 2019. Co se týká legislativy, řídí se tato problematika vnitrostátním právem nařízení eIDAS a v Estonsku zákonem o elektronické identifikaci a důvěryhodných službách elektronických transakcí. Používání elektronického podpisu je v Estonsku povinné pro veřejné subjekty a pro podniky a občany je pouze doporučeno. Elektronické podpisy se nejčastěji používají při komunikaci se státem. Konkrétně se pak jedná pouze o kvalifikované elektronické podpisy, které používá také většina soukromých společností, jako jsou banky, telekomunikace, energetické společnosti atd.

7.2.1 Použitelnost elektronického podpisu

Estonský národní portál `https://www.eesti.ee` podporuje dokumenty podepsané pomocí elektronických podpisů nebo e-pečetí. Estonsko také nabízí e-rezidenční karty pro lidi z celého světa, které se neliší od národního průkazu totožnosti. V současnosti je v Estonsku vytvořeno 644 933 799 elektronických podpisů, 98% Estonců má aktivní průkaz totožnosti a 67% je používá aktivně elektronicky. Co se týká služeb obecně, ty využívají elektronické služby až v 99%. Mezi ty nejvíce využívané služby v elektronické podobě patří podávání daňového přiznání od veřejného sektoru a bankovní převody ze soukromého sektoru. V Estonsku existuje aplikace DigiDoc4, prostřednictvím které jsou podepisovány především smlouvy a přijímány a ověřovány podpisy PDF pocházející zpravidla ze zahraničí.

7.2.2 Distribuce podpisových certifikátů

Za hlavního poskytovatele podpisových certifikátů je v Estonsku považována soukromá společnost SK ID Solutions AS, která má smlouvu s veřejným sektorem. Tato společnost je součástí evropského seznamu důvěryhodných poskytovatelů důvěryhodných služeb a splňuje požadavky nařízení eIDAS pro kvalifikované certifikáty pro elektronické podpisy. Činnosti SK ID Solutions AS jsou pravidelně kontrolovány po celou dobu životnosti služeb elektronického podpisu. Podpisové certifikáty jsou poskytovány jako součást národního systému eID. Totožnost žadatele o osvědčení je ověřena fyzickými nebo právně závislými stranami, které se rozhodnou vydat identifikační doklady. Estonské schéma eID je založeno na použití Public Key Infrastructure (PKI) s kryptografií podle osvědčených postupů a použití čipových karet SSCD / QSCD [33].

7.2.3 Místní technologické standardy

Formáty elektronického podpisu by měly být jednotné v celé Evropě, a proto i v Estonsku jsou používané formáty, které jsou použitelné v celé Evropě. Mezi standardy Evropské komise patří ASiC a podpisové standardy XAdES. Co se týká místního standardu formátu elektronického podpisu, v tom případě mluvíme o BDOC jako o novém formátu elektronickýho podpisu, který v současnosti nahrazuje v minulosti hojně používaný místní standard DDOC, který byl založen na standardu ETSI TS 101 903 a který se nazývá pokročilé elektronické podpisy [33].

7.2.4 Podpisové technologie

Co se týká podpisové technologie, v Estonsku existují dvě základní schémata, mezi které patří řešení založené na čipové kartě a řešení založené na SIM kartě. Co se týká podpisové technologie založené na SIM kartě, ten je znám pod názvem mobilní ID. Pořízení elektronický ID karty e-Residency, která představuje elektronickou osobní identifikaci, slouží k bezpečné identifikaci prostřednictvím internetu. Prostřednictvím této karty je možno vstoupit na webové portály, využívat e-služby, provádět transakce a platby či poskytovat elektronický podpisy [34]. Co se týká osvědčení o elektronickém podpisu a době jejich platnosti, ty jsou stanoveny následujícími požadavky:

- na kvalifikovaný certifikát pro elektronický podpis jsou stanoveny v článku 28 nařízení Evropského parlamentu a Rady (EU) č. 910/2014, *„ke zvýšení důvěry zejména malých a středních podniků a spotřebitelů ve vnitřní trh a na podporu používání služeb vytvářejících důvěru a produktů by měly být zavedeny pojmy „kvalifikované služby vytvářející důvěru“ a „kvalifikovaný poskytovatel služeb*

vytvářejících důvěru“ za účelem stanovení požadavků a povinností, které zajistí vysokou úroveň bezpečnosti všech používaných nebo poskytovaných kvalifikovaných služeb vytvářejících důvěru a produktů“,

- na kvalifikovaný certifikát pro elektronickou známku jsou stanoveny v článku 38 nařízení Evropského parlamentu a Rady (EU) č. 910/2014, *„oznamování narušení bezpečnosti a posuzování bezpečnostních rizik je nezbytné, aby mohly být dotčeným stranám v případě narušení bezpečnosti nebo ztráty integrity poskytnuty náležité informace“* [35].

Estonsko používá tyto druhy elektronických podpisů:

- kvalifikovaný elektronický podpis – s algoritmy SHA-1 s RSA,
- jednoduchý elektronický podpis,
- pokročilý elektronický podpis.

8 Elektronický podpis v Bělorusku

V říjnu roku 2018 schválila horní komora běloruského parlamentu změny zákona, týkající se elektronických dokumentů a podpisů. Podle běloruského ministra pro komunikaci a informatizace se očekává, že budou elektronický podpisy více používány. Tato změna by měla zjednodušit používání elektronických podpisů a tím by se mělo výrazně rozšířit jeho přijetí. V současnosti se používá přibližně 480 000 elektronických podpisů a každý měsíc probíhá asi 500 000 elektronických operací. V roce 2019 se chystá nový systém, který bude využíván k nakládání s důvěrnými dokumenty, a poté by se již neměly žádné dokumenty zpracovávat v tištěné podobě. Běloruské právní předpisy týkající se elektronických podpisů, se stále aktualizují. Nový zákon by tedy měl vyřešit především problém ověření pravosti elektronických dokumentů, které byly vytvořeny zahraničními partnery pomocí různých řešení ochrany dokumentů a to tak, že budou uznávány certifikáty zahraničních otevřených klíčů.

Aktuálním běloruským zákonem, zabývajícím se touto problematikou, je zákon číslo 113-Z o elektronickém dokumentu a elektronickým podpisu, který byl přijat v roce 2009. Tento zákon se zaměřuje na vytvoření právního základu pro používání elektronických dokumentů, určení hlavních požadavků kladených na elektronické dokumenty a rovněž na právní podmínky používání elektronického podpisu v elektronických dokumentech v případě, kdy budou dodržena pravidla elektronického podpisu v elektronickém dokumentu stejně, jako by to bylo v případě normálního papírového podání (tedy ne elektronicky) [36].

Právní předpisy týkající se elektronických dokumentů a elektronickýho podpisu, vycházejí z ústavy Běloruské republiky a skládají se z tohoto zákona a jiných právních aktů Běloruské republiky. Stanoví-li mezinárodní smlouva Běloruské republiky odlišná pravidla, než která jsou obsažena v tomto aktu, použijí se pravidla mezinárodní smlouvy. Vládní nařízení týkající se vztahů elektronických dokumentů a elektronických podpisů mají na starosti vládní orgány, jednotlivci a jiné organizace. Státní regulaci této problematiky pak provádí konkrétně předseda Běloruské republiky, Rada ministrů Běloruské republiky, národní banka Běloruska, Operační a analytické středisko za prezidenta Běloruské republiky, orgánů a institucí státní archivní služby Běloruské republiky, jiných státních orgánů a jiných státních organizací v rámci jejich pravomoci a v podle tohoto aktu a jiných právních předpisů Běloruské republiky.

Problematiku elektronickýho podpisu popisuje zákon č. 113-7 v kapitole 4. V této kapitole se říká, že elektronický podpis je určen především pro informace o totožnosti, které jsou běžnou součástí elektronického dokumentu a pro potvrzení integrity a pravosti elektronického dokumentu. Identita informací, která je běžnou součástí elektronického dokumentu, se provádí pomocí certifikovaných elektronic-

kých nástrojů elektronických podpisů, které používají osobní klíče osob podepisující elektronický dokument. Integrita a pravost elektronického dokumentu je potvrzena použitím certifikovaných elektronických nástrojů elektronických podpisů, které používají veřejné klíče signatářů elektronického dokumentu. Elektronický elektronický podpis je analogický s vlastnoručním podpisem a také může být používán místo otisku razítka [36].

Co se týká technologie elektronického elektronickýho podpisu, jedná se o kombinaci postupů, metod, softwaru a technických prostředků vztahujících se k praktickému používání elektronického elektronickýho podpisu. Součástí elektronického podpisu je soukromí klíč, jehož vlastníkem je organizace nebo osoba, která vydala osobní klíč pomocí certifikovaného nástroje elektronického elektronickýho podpisu. Majitel osobního klíče je povinen uchovat osobní klíč v tajnosti.

Veřejný klíč je generován na základě soukromého klíče pomocí certifikovaného nástroje elektronického elektronickýho podpisu. Vlastníkem veřejného klíče může být jak soukromá, tak i právnická osoba, která vlastní osobní klíč, na kterém byl veřejný klíč vyvinut.

Pořadí provozování státního systému otevřené správy klíčů je určeno ustanovením, které je schváleno společným usnesením Rady ministrů Běloruské republiky a národní banky Běloruské republiky, pokud není stanoveno jinak prezidentem Běloruské republiky. Národní banka Běloruska akreditující poskytovatele služeb ve státním otevřeném systému správy klíčů a monitoruje dodržování akreditačních podmínek. Podmínky akreditace poskytovatelů služeb ve státním otevřeném systému správy klíčů, postup akreditace a sledování dodržování jeho podmínek stanoví národní banka Běloruska. Národní banka Běloruska zajišťuje interakci státního systému otevřené správy klíčů se zahraničními poskytovateli služeb. Co se týká osvědčování otevřeného klíče splňující požadavky právních předpisů cizí země, ve které je osvědčení vydáno, je uznáno na území Běloruské republiky v případech a v pořadí určeném mezinárodní smlouvou Běloruska, která stanovuje vzájemné uznávání osvědčení o otevřených klíčích nebo jiný způsob poskytování právní síly cizím elektronickým dokumentům. Na území Běloruské republiky je uznávaným osvědčením o otevřeném klíči vydaným zahraničním poskytovatelem akreditovaným ve státě otevřeném systému správy klíčů [36].

I v Bělorusku se používají následující typy podpisů, podobně jako v ostatních sledovaných zemích:

- kvalifikovaný elektronický podpis – Schmorův podpisový algoritmus STB,
- jednoduchý elektronický podpis,
- pokročilý elektronický podpis.

9 Zhodnocení a budoucí trendy elektronického podpisu ve veřejné správě

Veřejná správa v oblasti aplikace elektronického podpisu začala postupně vyhodnocovat, že jejich pracovní postupy související s podpisy budou plně elektronický pomocí zabezpečených elektronických podpisů. Přijetím potvrzení právní platnosti díky nařízení eIDAS stále více subjektů přijímá řešení pro elektronické podpisy ve své práci a veřejné správě je tato oblast významná. S ohledem na hodnotu elektronických podpisů to nepřekvapuje: Evropská komise prostřednictvím institutu eSignature (CEF) společnosti Europe udržuje vzorový software v souladu s nařízením eIDAS. DSS (Digital Signature Services) je knihovna s otevřeným zdrojovým kódem, kterou lze integrovat do podpisového řešení veřejných i soukromých subjektů v rámci zemí EU. Podporuje vytváření a ověřování pokročilých a kvalifikovaných elektronických podpisů.

Zavádění řešení založených na DSS usnadňuje vzájemné uznávání a přeshraniční interoperabilitu elektronických podpisů mezi členskými státy EU. To znamená, že veřejné správy a podniky mohou důvěřovat a používat elektronické podpisy, které jsou platné a strukturované ve formátech interoperabilních EU. Specialisté v oblasti IT mohou také zkontrolovat soulad svého stávajícího řešení elektronického podepisování s formáty ETSI uvedenými v prováděcím rozhodnutí Komise (EU) 2015/150617. Veřejná správa je vyzvána, aby minimalizovala náklady, nabízela kvalitní služby a neustále udržovala dodržování platných právních předpisů i interních předpisů institucí veřejné správy. Kromě toho se od nich očekává, že budou v popředí příkladem v éře elektronickýho nastavení. Instituce a subjekty CEF pomáhají vládním orgánům řešit tyto jedinečné potřeby a výzvy související s administrativou v písemné podobě. Díky tomu se veřejné správy mohou stát efektivnějšími a nakonec uvolnit zdroje, aby nabídly větší množství a kvalitu služeb poskytovaných ve veřejné správě.

Technologie a informační technologie a jejich možnosti představují způsob, jak rozvíjet efektivitu veřejné správy v dnešním elektronickým světě. Ať už instituce používají technologii k lepší spolupráci na pracovišti nebo k pomoci pracovnímu týmu pro rozvoj činností veřejné správy při vytváření, péči a komunikace s klienty institucí veřejné správy a inteligentní integrace technologie do rutinních činností veřejné správy je dnes do určité míry standardizováno. Instituce ve veřejné správě musí také strategicky investovat do technologických řešení, která zlepšují služby institucí veřejné správy pro jednotlivé klienty a pro vlastní zaměstnance dané instituce veřejné správy. U elektronických podpisů je vhodné souhrnně uvést, jak využití řešení pro elektronický podpis lze vnímat jako podstatnou změnu pro instituce ve veřejné správě.

Přidaná hodnota bezpečnost dokumentů. Také ve veřejné správě je bezpečnost prioritou pro všechny klienty, zejména pokud se pracuje s osobními daty klientů. Pokud je řešení bohaté na funkce, ale chybí v oddělení zabezpečení a dodržování právních předpisů. Jako preferované řešení pro elektronický podpis je takové, které je samostatným prvkem. Nemusíme si dělat starosti s problémy s ověřováním nebo s krátkými časy, pokud jde o specifické právní předpisy týkající se elektronických podpisů. Vylepšená účinnost díky možnosti přístupu a podepisování kdekoli je také pozitivní. Vhodné jsou také mobilní technologie, které by v budoucnu mohly být také využity. Inovace v oblasti technologií a informačních technologií je kritická součást procesu elektronický transformace a efektivity činností ve veřejné správě. Zaměstnanci a klienti musí být schopni podepisovat dokumenty na různých zařízeních a v různých aplikacích; se softwarovými řešeními pro elektronický podpis. Toto řešení musí být snadné a transparentní. Zjednodušený musí být také pracovní postup.

Pracovní postupy a jejich efektivita. Využití elektronických podpisů umožňuje rychleji komunikovat a i realizovat úkony ve vztahu k institucím veřejné správy. Místo nutnosti roztříštěné komunikace a čekání na stahování, skenování nebo faxy jsou dokumenty místo toho automaticky odesílány s elektronickým podpisem v pracovním postupu. Tato jednoduchá funkce má jen jednoduchý dopad. Umožňuje to více času na péči o klienty a efektivní využití disponibilních zdrojů. Navíc elektronické podpisy jdou významné, pokud jde o přínos z celkového pracovního toku, protože je možné efektivně sledovat dokumenty klienta a vždy vědět, kde jsou v procesu a jaké budou další kroky.

Lepší zkušenosti a komunikace s klienty. Přijetí elektronických podpisů může zlepšit klientský pozitivní zážitek s poskytováním služeb v rámci instituce veřejné správy. Technologie mají přidávající hodnotu a využití softwaru pro elektronický podpis zefektivňuje podepisování důležitých dokumentů a proces pro klienta je mobilní / uživatelsky přívětivý, bezpečný a rychlý.

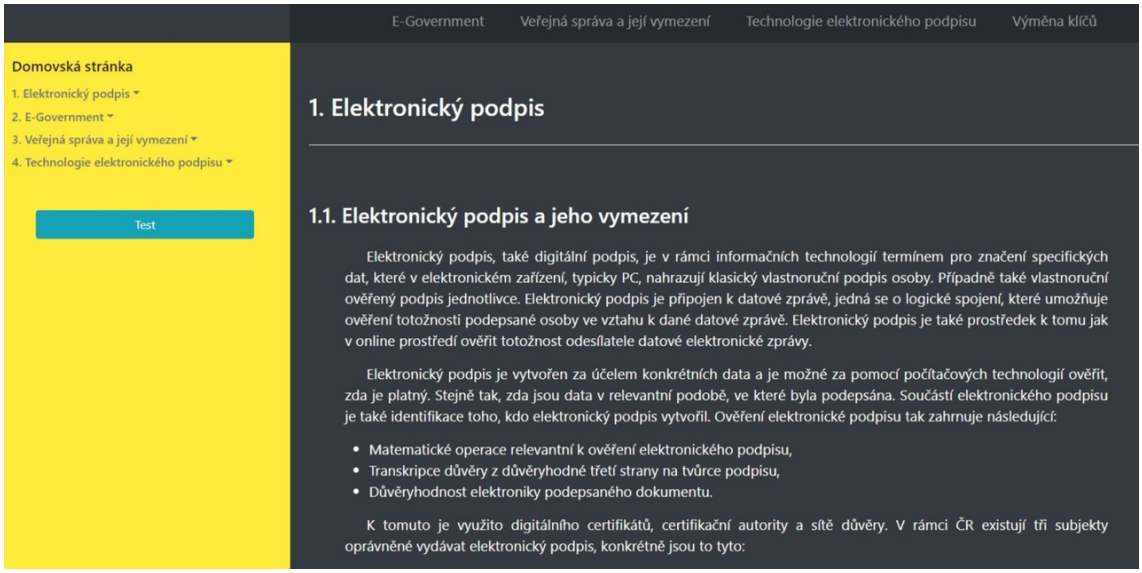
Integrace softwaru pro elektronický podpis je ve veřejné správě významným prvkem efektivity činností zaměstnanců i služeb pro klienty a jejich kvality. Elektronický podpis usnadnil interní procesy, pomohl komunikovat rychleji a s menšími problémy, zefektivnil přístup k informacím pro zaměstnance instituce veřejné správy a vytvořil dobrou zkušenost pro naše klienty, která minimalizuje problémy a zrychluje komunikaci zaměstnanců instituce veřejné správy. Globální trh s elektronickým podpisem v posledních letech neustále roste a očekává se, že poroste ještě dále.

Schopnost podepisovat dokumenty elektronicky již není považována za neobvyklou. Celosvětové používání elektronických podpisů rostlo intenzivně v minulých letech. Rostoucí využívání elektronických podpisů a zařízení pro sběr podpisů k eliminaci podvodů, podpoře technologických inovací a lepší integritě dat, škálovatel-

nosti a spolehlivosti jsou zásadním předpokladem růstu trhů v evropských zemích i globálně. Jedním z nich by měla být schopnost elektronicky podepisovat dokumenty také v mobilním zařízení a dokonce i v režimu offline. Tím, že uživatelům bude umožněn elektronický podpis prakticky odkudkoli, získají uživatelé své dokumenty, které podepsali velmi rychle a efektivně. Jedná se o řešení optimalizující čas a náklady v rámci institucí veřejné správy.

10 Popis výukové aplikace

V rámci bakalářské práci byla vytvořena webová aplikace, dostupná na stránce: `http://ep.fxdev.ru/`, jejíž printscreenovou podobu uvádí obrázek 10.1 . Zdrojový kód vytvořené stránky je součástí přílohy 1.



Obr. 10.1: Vytvoření vlastní webové stránky.

Kostra webové stránky byla vytvořena v aplikaci HTML5.

HTML znamená obecně značkovací jazyk, kterým se píšou webové stránky, HTML 5 je jeho konkrétní specifikace. HTML5 je poslední standard, podle něhož prohlížeče zobrazují a zpracovávají webové stránky. mysl HTML5 spočívá v první řadě v tom, usnadnit prostřednictvím dohodnutých standardů práci vývojářům a tvůrcům webových prohlížečů. Je také navrženo s cílem poskytnout lepší, rychlejší a ucelenější uživatelský zážitek na PC i mobilních zařízeních.

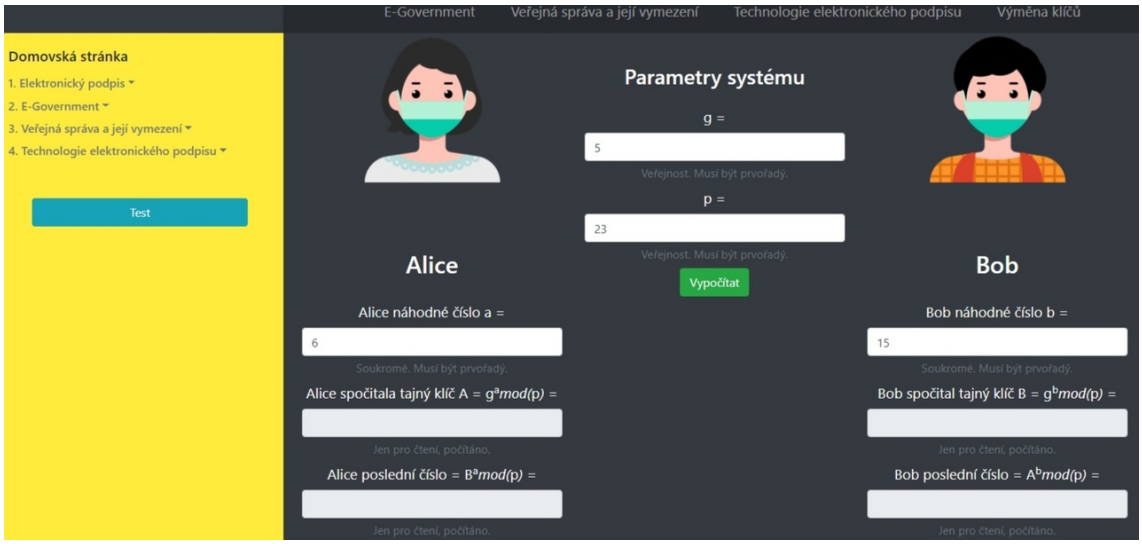
Pro vytvoření softu byl použit Visual Studio Code a sftp plugin. Jako server - shared hosting, což popisuje hostující server a jeho cestu, a apache 2.4.10, který ukazuje na otevřený server.

Pro design webové stránky byl použit bootstrap 4.3.1 a Custom CSS. Custom CSS používá jednoduchou a volně stažitelnou sadu nástrojů pro tvorbu webu a webových aplikací. Pomocí editoru Custom CSS se může přizpůsobit vzhled libovolného webu. Custom CSS umožňuje přidat jakékoliv vlastní CSS styly do webu.

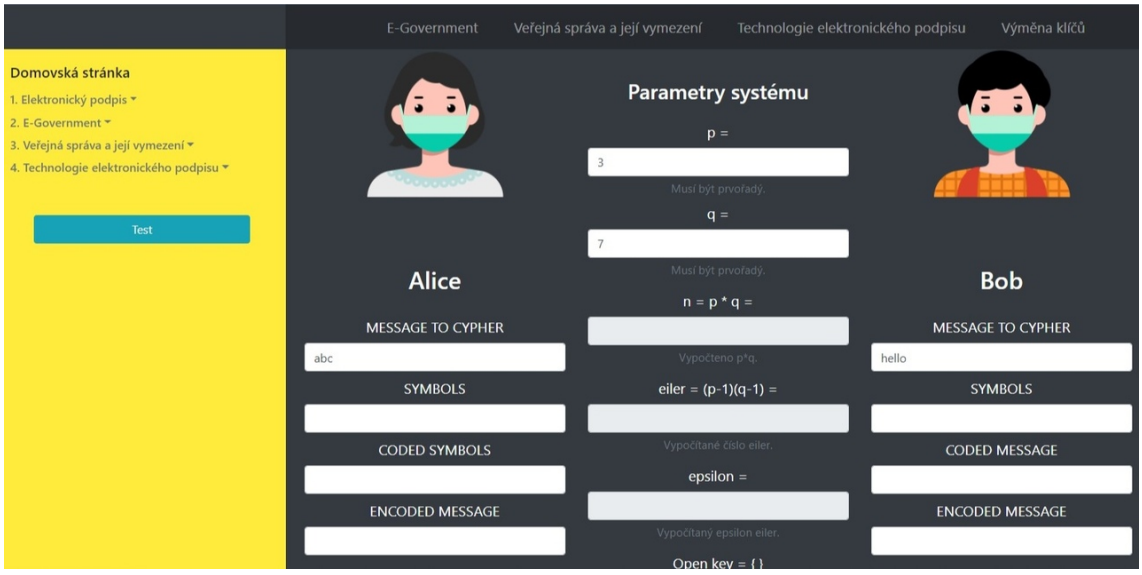
Aplikační logika a animace - byl použit jazyk Java script a knihovna jquery 3.3.1. Jquery 3.3.1. je rychlá, malá a bohatá knihovna JavaScript. Díky snadno použitelnému rozhraní API, které funguje v celé řadě prohlížečů, je mnohem jednodušší

procházení dokumentů a manipulace s nimi, manipulace s událostmi, animace a Ajax. Díky kombinaci všestrannosti a rozšiřitelnosti, jQuery změnil způsob, jakým miliony lidí píšou JavaScript.

Bootstrap identifikuje design celé webové stránky a vlastní JS kód je kód, doplňující stránku o nové vlastnosti.

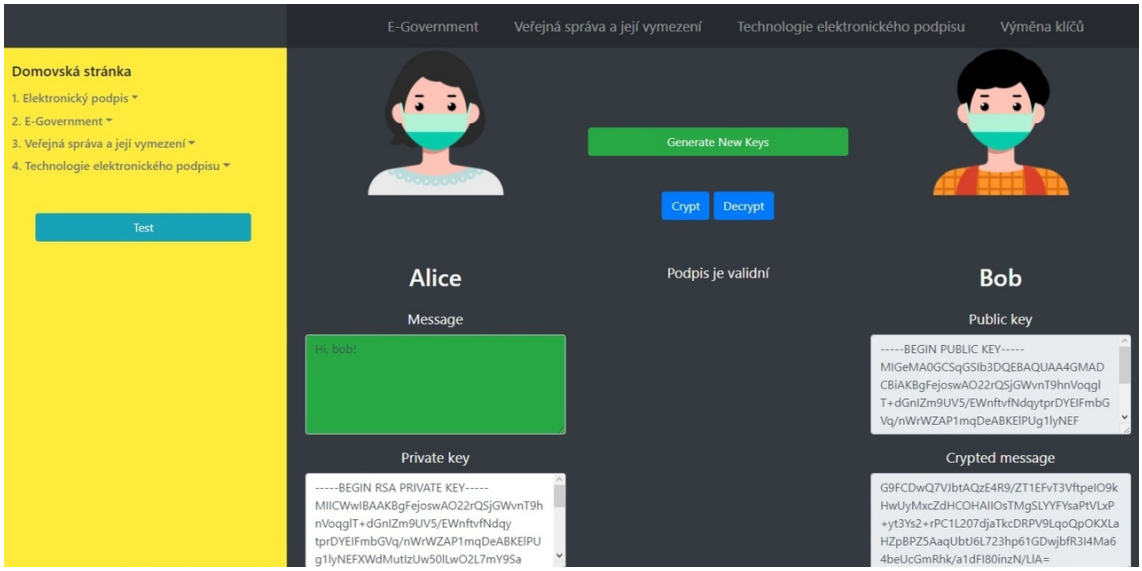


Obr. 10.2: Diffieho–Hellmanova výměna klíčů.



Obr. 10.3: Výměna klíčů pomoci RSA.

Na záložce „Výměna klíčů“ je vysvětlen postup pro vypočítání klíče. Pro kalkulačky Diffie–Hellman (viz obr. 10.2), Step by step RSA (viz obr. 10.3), a RSA-podepisováni (viz obr. 10.4) opět byla použita rychlá a bohatá knihovna JavaScript – jquery a vlastní JS kód.

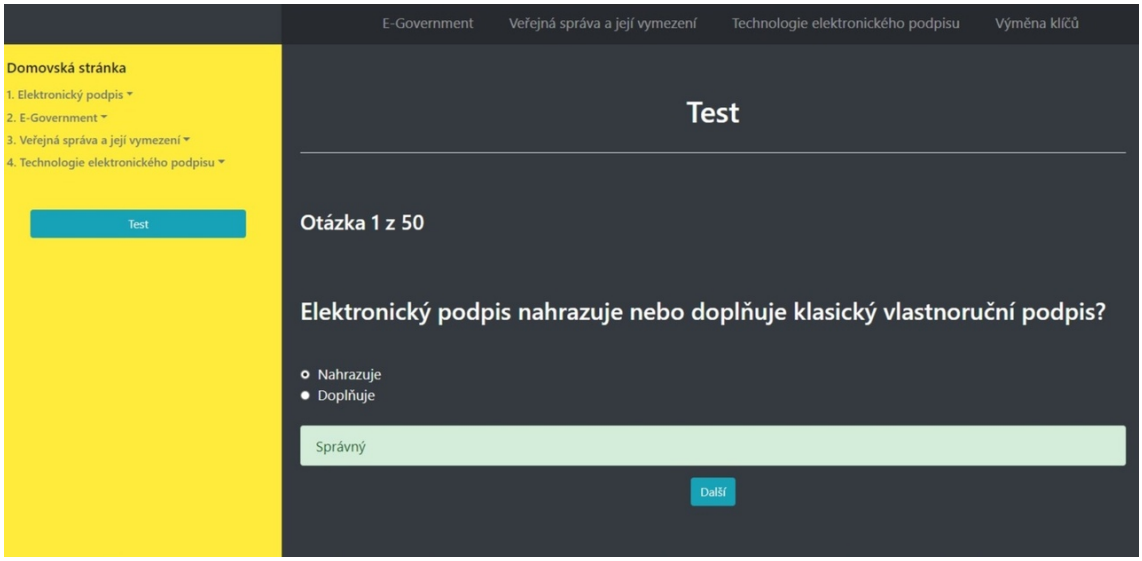


Obr. 10.4: Podepisování pomoci RSA (real RSA)

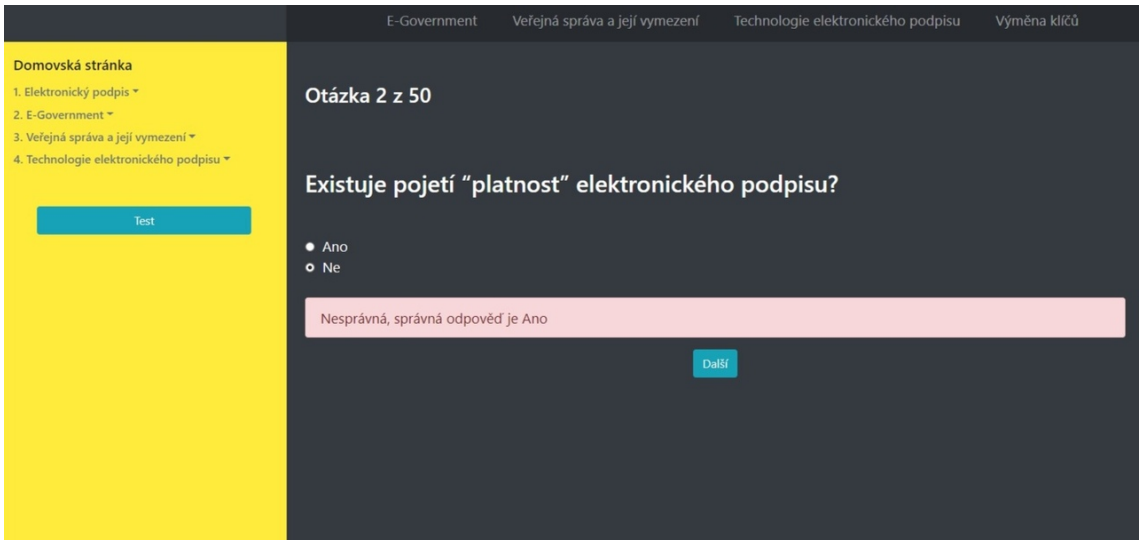
V levé části hlavní stránky je políčko „Test“. Po rozkliknutí se objeví uživateli test s 50 otázkami, na které má na výběr odpovědi.

V případě správné odpovědi se objeví zelený pruh a slovíčko "správně"(viz obr. 10.5), při špatné odpovědi se objeví červený pruh a slovíčko "špatně"(viz obr. 10.6) a uživateli napoví správnou odpověď.

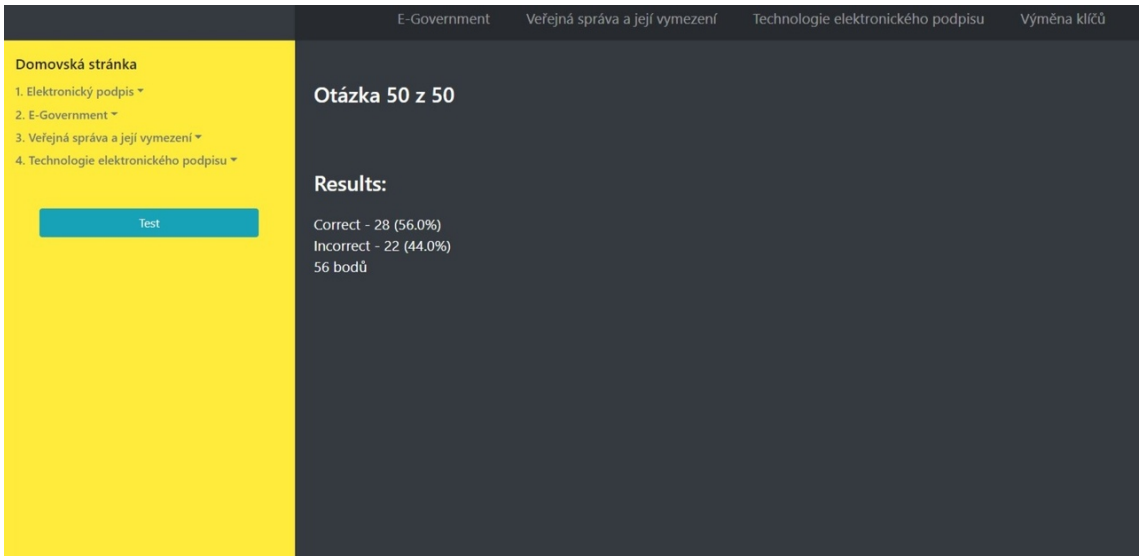
Na konci testu se uživateli objeví tabulka, jak si v testu vedl a ukáže mu, kolik měl správných a špatných odpovědí. Pro ukázku byl test náhodně vyplněn třetí osobou (viz obr. 10.7).



Obr. 10.5: Test – Ukázka správné odpovědi.



Obr. 10.6: Test – Ukázka nesprávné odpovědi.



Obr. 10.7: Test – Výsledky testu.

Závěr

Hlavním cílem této bakalářské práce bylo zhodnocení elektronického podpisu a jeho vymezení v teoretické rovině a následně z hlediska komparace u vybraných států, především Ruska, statů Pobaltí a Běloruska.

Elektronický podpis neboli „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání“, jak jej definuje unijní právo, je stále předmětem řady nejasností a zmatků.

Elektronický podpis je hojně využívaný především v komunikaci se státní správou, se soudy, advokáty a dalšími institucemi, kdy je možné tento elektronický podpis využít při zasílání úředních dokumentů bez nutnosti nechávat si ověřovat podpis na úřadech a následně jej zaslat doporučeně. Vzhledem k tomu, že Česká republika je členem Evropské unie, platí pro ni i nařízení týkající se elektronického podpisu tak, aby byly tyto podmínky sladěny v rámci celé Unie.

Při porovnávání legislativy ČR a EU s využíváním elektronických podpisů v rámci vybraných států Ruska, Litvy, Estonska a Běloruska bylo v rámci práce zjištěno, že zde existují podobná nařízení a směrnice jako v ostatních členských zemí, i když Rusko a Bělorusko nejsou členy EU. I v těchto zkoumaných státech existují tři druhy elektronického podpisu, stejně tak jako v členských zemích. Rozdíly jsou pouze v tom, za jakých podmínek se digitální podpis používá, kdo za něho v dané zemi odpovídá (úřad, ministerstvo) a v jakém algoritmu jsou podpisy využívány.

Problematika elektronického podpisu, která ještě před deseti lety zajímala jen hrstku specialistů, se stále více dostává do popředí zájmu širší veřejnosti. Není divu, vždyť například sliby o možnosti posílat daňová přiznání po internetu a opatřená elektronickým podpisem jsou lákavé a srozumitelné snad každému. Elektronický podpis, častěji se mu ale říká digitální, si našel cestu a využití v mnoha oblastech.

Pro znázornění pochopení celé problematiky byla vytvořena webová stránka, která popisuje „Elektronický podpis“, „E-govermment“, „Veřejnou zprávu a její vymezení“ a „Technologii elektronického podpisu“. Součástí této stránky je i hlavička v nadpise „Výměna klíčů“, která popisuje proces tvorby klíčů mezi dvěma subjekty a to pomocí výměny klíčů. Náhledy jednotlivých stránek jsou součástí kapitoly 10. „Popis výukové aplikace“.

Na závěr výukového programu je pro uživatele připraven test z otázek o elektronickém podpisu, který má 50 otázek. Na konci testu se uživatel dozví, kolik měl správných a kolik měl špatných odpovědí a zda výukovým programem prošel.

Do budoucna stojí jistě za zvážení vytvoření druhu elektronického podpisu, který by měl účinky úředně ověřeného podpisu, i když jsou zde jisté obavy s tímto spojené, což může být důvodem, proč k tomuto kroku zatím nedošlo. Elektronický podpis

bude ze své povahy vždy jen souborem elektronických dat přemisťujícím se nejčastěji prostředím internetu. Ať už by byl elektronický podpis vytvořen sebebezpečněji a podepisující by byli při jeho používání nanejvýš obezřetní, vždy existuje riziko, že někdo tento soubor elektronických dat na dálku v síti zachytí, zkopíruje a zneužije.

Osobní návštěva podepisujícího, ať už třeba na poště, u notáře nebo jinde (např. u advokáta, srov. prohlášení o pravosti podpisu), a následné klasické „fyzické“ ověření podpisu jinou osobou, představuje stále nejvyšší formu záruky, že právní jednání činí skutečně podepisující osoba a ze své vlastní vůle.

Literatura

[1] BUDIŠ, P., ŠTĚDROŇ, B. *Elektronické komunikace*. 1. vyd. Slovakia: Magnet Press, 2008, s. 5-8 [cit. 2019-10-10].

[2] BUDIŠ, P., ŠTĚDROŇ, B. *Elektronické komunikace*. 1. vyd. Slovakia: Magnet Press, 2008, s. 8-10 [cit. 2019-10-10].

[3] Ministerstvo vnitra České republiky. *Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb* [online]. 2020 [cit. 2020-04-20]. Dostupné z `https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu\-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx`.

[4] ADAMS, C. LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations.* Second Edition, Addison-Wesley Professional, 2003, ISBN 978-0-672-32391-1, s. 11-12 [cit.2019-10-22].

[5] ADAMS, C. LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations.* Second Edition, Addison-Wesley Professional, 2003, ISBN 978-0-672-32391-1, s. 20-23 [cit.2019-10-23].

[6] Schellekens, M. (2004). *Electronic signatures: Authentication technology from a létal perspective* (Information technology law series; 5). The Hague: Cambridge: T.M.C. Asser Press; Cambridge University Press.[cit.2019-11-01].

[7] MASON, S. *Electronic signatures in practice* [online]. British Institute of International and Comparative Law, 2006, 58-61 [cit. 2019-10-19].

[8] CASTRO, D. *Electronic Identification: Explaining International Leadership: Elektronice Identification Systems* [online]. In: Washington D. C.: The Information Technology and Innovation Foundation (ITIF), 2011 [cit. 2019-10-21].

[9] DOSTÁLEK, L., VOHNOUTOVÁ, M. *Velký průvodce infrastrukturou PKI.* Computer Press, Albatros Media, 2017. ISBN 9788025145135 [cit. 2019-10-21].

[10] BOSÁKOVÁ, D., KUČEROVÁ, A., Peca, Jaroslav; Vondruška, Pavel. *Elektronický podpis přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* Nakladatelství ANAG, 2002. 106 s. ISBN 80-7263-125-X [cit. 2019-12-01].

[11] Ministerstvo vnitra České republiky. *eIDAS, vytvářející důvěru a elektronická identifikace* [online]. 2019 [cit.

2020-03-08]. Dostupné z https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx

[12] České vysoké učení technické *Certifikáty a elektronické podpisy* [online]. CVUT: CVUT, 2020 [cit. 2020-04-20]. Dostupné z:https://ist.cvut.cz/bezpecne-it/certifikaty-elektronicke-podpisy/

[13] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi.* Olomouc: ANAG, 2008. Právo (ANAG). ISBN 9788072634651 [cit. 2020-03-01].

[14] ŠTĚDROŇ, Bohumír. *Úvod do eGovernmentu: právní a technický průvodce.* Praha: Úřad vlády české republiky, 2007, ISBN 978-80-87041-25-3 [cit. 2020-02-20].

[15] LIDINSKÝ, Vít. *EGovernment bezpečně.* Praha: Grada, 2008. ISBN 9788024724621 [cit. 2019-12-01].

[16] KOVAŘÍKOVÁ, Karolína. *Nařízení eIDAS – elektronický podpis a jeho aplikace ve veřejné správě.* Brno, 2019. Bakalářská práce. Mendelova univerzita [cit. 2019-12-03].

[17] *Hashovací funkce.* [cit. 2020-04-20]. Dustupné z:https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7029

[18] JONÁŠ, M. *Bezpečnost elektronického obchodu.* Brno, 2007. Bakalářská práce. Vysoké učení technické v Brně. [cit. 2019-11-24].

[19] VELEBIL, J. *Diskrétní matematika a logika.* Praha, 2006. Text k přednášce. České vysoké učení technické. [cit. 2019-11-24].

[20] Algoritmus RSA.Dostupné z https://www.algoritmy.net/article/4033/RSA [cit. 2019-11-26].

[21] SVOBODA, P. *Systémy elektronických podpisů.* Brno, 2006. Diplomová práce. Masarykova univerita v Brně. [cit. 2020-02-20].

[22] *Bezpečnost IS/IT. Elektronický podpis.* Dostupné z : https://akela.mendelu.cz/~lidak/bis/9pki.htm [cit. 2020-03-17].

[23] LAPÁČEK, Jiří. *Jak na datovou schránku a elektronickou.* Computer Press, Albatros Media, 2017. ISBN 9788025147696 [cit. 2020-03-22].

[24] Rada and Partner, advokátní kancelář, *K nové právní úpravě elektronického podpisu.* Rada and Partner, advokátní kancelář, 2017. Dostupné z: https://www.epravo.cz/top/clanky/

k-nove-pravni-uprave-elektronickeho-podpisu-106077.html [cit. 2020-03-25].

[25] *Kvalifikovaný certifikát pro elektronický podpis.* Dostupné z: https://www.ica.cz/kvalifikovany-certifikat-pro-ePodpis [cit. 2020-03-27].

[26] I.CA. *O společnosti I.CA.* Dostupné z: https://www.ica.cz/o-nas [cit. 2020-03-25].

[27] ŠTĚDROŇ, B., PROKEŠ, J. *Datové schránky, elektronický podpis a autorizovaná konverze dokumentů.* Praha, Bulletin Advokacie, 10/2011, s. 30-32. ISSN 1805-8280 [cit. 2020-04-02].

[28] DUBININA, Natalia.; *Minkomsvjazi zapustit „Elektronek obščestvo".* Dostupný z: http://www.bfm.ru/articles/2010/04/17/minkomsjazi-zapustit-elektronnoe-obshhestvo.html [cit. 2020-04-07].

[29] ŠTĚDROŇ, B. *Právní úprava elektronického podpisu v Rusku,* 2003. Dostupné z https://itpravo.cz/index.shtml?x=122460 [cit. 2020-04-07].

[30] *Požadavky EDS. Druhy elektronických podpisů v Rusku a požadavky na ep. Podstata elektronického podpisu.* Dostupné z: https://studiorespect.ru/cs/trebovaniya-k-ecp-vidy-elektronnyh-podpisei-v-rossii-i-trebovaniya-k.html [cit. 2020-04-09].

[31] PETROV, Andrey. *Elektronický podpis.* Praha, 2010. Bakalářská práce. Vysoká škola regionálního rozvoje a Bankovní institut [cit. 2020-04-10].

[32] *eSignature DSS Community,* 2017, Lithuania, dostupné z https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=75664488 [cit. 2020-04-15].

[33] *eSignature DSS Community,* 2017, Estonia, dostupné z https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=75664488 [cit. 2020-04-17].

[34] *What is Mobiil-ID?* Dostupné z https://www.id.ee/index.php?id=36882 [cit. 2020-05-02].

[35] *Zákon o důvěryhodných službách pro elektronickou identifikaci a elektronickou transakci,* 2019, dostupné z https://www.riigiteataja.ee/akt/112122018030 [cit. 2020-05-14].

[36] *Zákon č. 113–Z o elektronickém dokumentu a elektronickém elektronickým podpisem,* 2009 dostupné z `http://cis-legislation.com/document.fwx?rgn=30109` [cit. 2020-05-20].

Seznam symbolů, veličin a zkratek

AES	Advanced Encryption Standard
AI	Umělá inteligence
AK	Asymetrická kryptografie
API	Application Programming Interface
CA	Certifikační autorita
CEF	Connecting Europe Facility
CPS	Certification Practice Statement
ČR	Česká Republika
CRL	Certificate Revocation List
CSS	Cascading Style Sheets
DES	Data Encryption Standard
DNSSEC	Domain Name System Security Extensions
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EDI	Electronic data interchange
eIDAS	Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu
ES	Směrnice Evropského parlamentu a Rady
ESS	Enhanced scatter search scheme
ETSI	European Telecommunications Standards Institute
EU	Evropská unie
FSB	Federální služba bezpečnosti
FZ	Federativný zákon
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
I.CA	První certifikační autorita
IIAS	Mezinárodní institut správních věd
IoT	Internet věcí (Internet of Things)
ISDS	Informační systém datových schránek
IT	Informační Technologie
LDAP	Lightweight Directory Access Protocol
MD4	Message Digest 4
MD5	Message Digest 5
OECD	Organizace pro hospodářskou spolupráci a rozvoj
OSVČ	Osoba samostatně výdělečně činná
PC	Osobní počítač

PKI	Public Key Infrastructure
RA	Registrační autorita
RSA	Iniciály autorů Rivest, Shamir, Adleman
Sb.	Sbírka zákonů
SET	Secure Electronic Transaction
SFTP	SSH File Transfer Protocol
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2
SK	Soukromý klíč
TK	Tajný klíč
TSL	Transport Layer Security
USA	United States of America
USB	Universal Serial Bus
VK	Veřejný klíč
XML	EXtensible Markup Language

Seznam příloh

1. Obsah přiloženého CD

- `index.html` — Hlavní stránka, obsahuje první kapitolu
- `1` — Složka s kapitolou: Elektronický podpis
  - `index.html` — Soubor s kapitolou: Elektronický podpis
- `2` — Složka s kapitolou: E-Government
  - `index.html` — Soubor s kapitolou: E-Government
- `3` — Složka s kapitolou: Veřejná správa a její vymezení
  - `index.html` — Soubor s kapitolou: Veřejná správa a její vymezení
- `4` — Složka s kapitolou: Technologie elektronického podpisu
  - `index.html` — Soubor s kapitolou: Technologie elektronického
- `calculator` — Složka kalkulačky: Výměna klíčů
  - `index.html` — Soubor s kalkulačkou: Výměna klíčů
- `dist` — Složka s technickými soubory
  - `archive` — Složka s technickými soubory projektu
    - `css` — Složka stylů projektu
      - `archive.css` — Vlastní styly CSS pro tento projekt
    - `img` — Projektové obrázky
      - `alice.png` — Obrázek Alice v sekci kalkulačky
      - `animation1.gif` — Animace Uplatnění asymetrické kryptografie v různých typech kryptografických systémů
      - `animation3.gif` — Animace Princip elektronickýho podpisu
      - `animation4.gif` — Animace Postup certifikačního procesu
      - `animation6.gif` — Animace Podpis a ověření elektronického podpisu
      - `animation8.gif` — Animace Zaručený elektronický podpis
      - `animationex.jpg` — Obrázek CA - struktura
      - `bob.png` — Obrázek Bob v sekci kalkulačky
    - `js` — Složka s zdrojovym kode Javascript
      - `js.js` — Soubor s jednotlivými projektovými skripty (logika kalkulaček)
  - `bootstrap` — Bootstrap css a javascript knihovna pro rychlý vývoj stránek
    - `css` — Složka Bootstrap CSS
      - `bootstrap.min.css` — Bootstrap CSS knihovna
    - `js` — Složka knihovny Bootstrap JS
      - `bootstrap.min.js` — Bootstrap JS knihovna
  - `jquery` — Knihovna javascript pro vývoj kalkulaček
    - `js` — Složka Jquery JS
      - `jquery-3.3.1.slim.min.js` — Soubor knihovny JQuery JS
- `test` — Složka testovací sekce
  - `index.html` — Soubor s testem