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 V PRAXI
ELECTRONIC SIGNATURE IN PRACTICE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Klára Blahušová

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. Václav Zeman, Ph.D.

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Klára Blahušová ***ID:*** 211781

Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Elektronický podpis v praxi

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 a vytvořte 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: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

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

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

Anotace

Bakalářská práce se zabývá problematikou elektronického podpisu, se zvláštním zřetelem na členské státy Evropské unie, ale v závěru se dotkne i zemí Evropského sdružení volného obchodu (Island, Lichtenštejnsko, Norsko a Švýcarsko) a několika dalších států mimo Evropskou unii, jako jsou Spojené království, Spojené státy americké a Čína. Práce se věnuje právním aspektům elektronického podpisu, jeho úpravě a případným změnám v jednotlivých státech. Součástí každé kapitoly, která pojednává o daném státu, je i výpis kvalifikovaných certifikačních autorit (u evropských států) a certifikačních autorit (u ostatních států).

První část bakalářské práce je věnována pojmu elektronický podpis a teorii s ním spojené, druhá část textu se věnuje samotným státům. Souhrn informací získaných pro bakalářskou práci se nachází ve webové aplikaci.

Klíčová slova

Certifikační autorita, eIDAS, elektronický podpis, kvalifikovaná certifikační autorita, kvalifikovaný elektronický podpis.

Abstract

The topic of this work is electronic signatures and their use in the European Union, while consideration is also given to nations in the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland) and others, such as Great Britain, USA and China. Description is given of legislation governing electronic signatures, the form this takes and differences between the aforementioned countries. Each section contains a list of relevant certificate authorities for the territories discussed therein.

The first part defines what an electronic signature is and the theory behind it, whereas the other is devoted to application in said territories. A summary of the information provided herein is available online via a dedicated web app.

Keywords

Certificate authority, eIDAS, electronic signature, qualified certificate authority, qualified electronic signature.

Bibliografická citace

BLAHUŠOVÁ, Klára. *Elektronický podpis v praxi*. Brno, 2021. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/133522. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce doc. Ing. Václav Zeman, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	Klára Blahušová
VUT ID studenta:	211781
Typ práce:	Bakalářská práce
Akademický rok:	2020/21
Téma závěrečné práce:	Elektronický podpis v praxi

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucího závěrečné 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 autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brně dne 31. května 2021 ----------

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D. za ochotu, odbornou pomoc a cenné rady při zpracování mé bakalářské práce.

V Brně dne 31. května 2021 ----------

podpis autora

Obsah

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

Úvod

Svět se neustále modernizuje, stále více styků v právní a obchodní oblasti se převádí do elektronické podoby. Možnost využití elektronické pošty a bezpečného elektronického bankovnictví nutně vyžaduje i určitou formu elektronického podpisu.

Elektronický podpis by měl mít stejný účel a vlastnosti jako podpis ruční. Měl by tedy nejen ověřovat identitu dané osoby (znak autenticity), ale měl by být také vyjádřením její vůle, být nefalšovatelný (znak nepopiratelnosti) a nepřenosný. Podepsaný dokument by dále nemělo být možné měnit (znak integrity). Autenticita, nepopiratelnost a integrita jsou vlastnosti elektronického podpisu, které jsou vynucené zákonem až u zaručeného elektronického podpisu a kvalifikovaného podpisu.

V běžné emailové komunikaci stačí na konec naší zprávy napsat naše jméno; jedná se většinou o elektronickou komunikaci mezi známými, nebo ve vztahu učitel a žák, případně pokud se obě strany na tomto typu komunikace domluví. Tento typ elektronického podpisu prostého se však již nedá aplikovat na některé obchodní styky, a hlavně se ve většině státech nedá aplikovat na právní styky a komunikaci se zahraničím. Proč tomu tak je? Elektronická podoba elektronického prostého podpisu nijak nezaručuje Alici, že se opravdu podepsal Bob, jeho jméno si mohla přivlastnit Eva. Proto vznikly další typy elektronického podpisu, které se již méně podobají tomu ručně psanému, avšak jsou mnohem spolehlivější pro elektronickou komunikaci. Jedná se o elektronický podpis zaručený a kvalifikovaný elektronický podpis. Zaručený elektronický podpis musí být vytvořen určitým způsobem, který zaručí neměnnost dokumentu a nepopiratelnost. U kvalifikovaného elektronického podpisu existuje třetí strana, která prokáže Alici, že Bob je opravdu tím, za koho se vydává. Až tyto dva typy podpisu splňují základní podmínky ručně psaného podpisu a jsou jeho elektronickým ekvivalentem. Tyto dva typy jsou užívané v České republice, ale jakým způsobem to funguje v ostatních státech?

1. ELEKTRONICKÝ PODPIS

Právní úprava elektronického podpisu je vymezena v 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 (neboli „eIDAS“) [1]:

- *„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.*
- *Elektronickou identifikací se rozumí postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu.“*

Nařízení eIDAS má za účel zajistit správné fungování vnitřního trhu a současně usilovat o bezpečnost prostředků pro elektronickou identifikaci a pro služby vytvářející důvěru. Stanovuje podmínky uznání elektronické identifikace, pravidla pro služby vytvářející důvěru a právní rámec pro elektronické podpisy.

Jedním z cílů tohoto nařízení je také odstranění překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají k autentizaci, a to alespoň pro účely veřejných služeb.

1.1 Pojmy

Podkapitola se věnuje pojmům, které se přímo vztahují k elektronickému podpisu, nebo je potřeba je od elektronického podpisu odlišit.

1.1.1 Digitální podpis

Rozdíl mezi elektronickým a digitálním podpisem:

- **Elektronický podpis** je právní termín (nařízení eIDAS). Je to potencionálně jakýkoliv údaj v elektronické podobě, jenž je připojen k datové zprávě a slouží jako metoda k ověření identity podepsané osoby. Dělí se na elektronický podpis prostý (podepsání konce dokumentu naším jménem a příjmením), zaručený elektronický podpis (může obsahovat jakákoliv data, hlavně aby byla logicky spojena s daty, které podepisují) anebo kvalifikovaný elektronický podpis (kvalifikovaný certifikát).
- **Digitální podpis** je termín užívaný v kryptografii. Jedná se o podpis vytvořený kryptografickými prostředky (privátní a veřejní klíč, hašování). Dělí se na přímé digitální podpisy (přímá komunikace dvou subjektů) nebo verifikované digitální podpisy (využívá při komunikaci třetí důvěryhodnou stranu).

Obecně bychom mohli říci, že kombinací digitálního podpisu a elektronického podpisu dostaneme zaručený elektronický podpis [2]. Zaručený podpis totiž nemusí být ověřen třetí stranou, ale musí zajišťovat základní ochranu před změnou nebo jiným zásahem do podepsaných dat.

V angličtině se pod digitálním podpisem většinou myslí podpis vytvořený pod certifikační autoritou.

1.1.2 Elektronická pečeť

Elektronická pečeť, podobně jako elektronický podpis slouží k identifikaci a zaručení integrity dokumentu. Neidentifikuje fyzickou osobu (konkrétního jedince), ale váže se k právnickým osobám. Jejich vložení do dokumentu probíhá automatizovaně prostřednictvím software.

1.1.3 Časové razítko

Časové razítko poskytuje údaj o konkrétním čase, kdy bylo k dokumentu připojeno. Kvalifikovaný elektronický podpis v sobě také nese údaj o čase, ale tento čas je systémový, sám o sobě není spolehlivý, proto se užívá časového razítka.

1.1.4 Certifikační autorita

Certifikační autorita je obecně třetí strana, většinou soukromý subjekt, který vydává certifikáty. Kvalifikovanou certifikační autoritu určuje kontrolní orgán daného státu a následně ji oznámí Evropské komisi. Certifikační autority vedou seznamy všech vydaných certifikátů, i těch, kterým vypršela platnost (odvolaný nebo zrušený certifikát uchovává autorita po dobu stanovenou státem). Na stránkách První certifikační autority jsou to Seznamy veřejných certifikátů a Seznamy zneplatněných certifikátů.

1.2 Typy elektronického podpisu

Definice níže uvedených typů elektronických podpisů vyplývají z nařízení eIDAS (zejména Oddíl 4 Elektronický podpis) [1].

1.2.1 Elektronický podpis prostý

Je to nejjednodušší a nejčastěji užívaný elektronický podpis. Jedná se o podpis v podobě:

- napsání jména a příjmení například na konci e-mailu, v dokumentu odesílaném učiteli, nebo v SMS zprávě posílané druhé osobě;
- odkliknutí políčka „souhlasím“ při vstupu na webovou stránku;
- naskenovaný vlastnoruční podpis apod.

K prostému elektronickému podpisu se neváže třetí strana, respektive není zde žádný prostředník, který ověří, že podepsanou osobou jsme opravdu my, a ne jiná osoba, která se za nás vydává.

V eIDAS, článku 25 o právních účincích elektronických podpisů je uvedeno: *„Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“* Dokument podepsaný elektronickým podpisem prostým se tak může použít jako důkaz v trestně právním jednání nebo se může použít pro uzavření obchodní smlouvy, pokud se tak obě strany dohodnou.

1.2.2 Zaručený elektronický podpis

Zaručený elektronický podpis se liší od prostého svými požadavky:

- Data musí být jednoznačně spojena s podepisující osobou a musí danou osobu identifikovat.
- Zaručený elektronický podpis musí být vytvořen pomocí dat, jež může použít jen podepisující osoba.
- Musí být poznat případná změna dat po podepsání.

Ani k zaručenému elektronickému podpisu se však neváže nutnost užití třetí strany k potvrzení skutečné identity (útočník si může vytvořit na cizí jméno elektronický podpis sám). Nezaručuje tedy identitu podepsané osoby, zaručuje pouze neměnnost a integritu podepsaného dokumentu.

1.2.3 Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis by měl být vytvořen kvalifikovanou autoritou pro vytváření elektronických podpisů. Kvalifikovaný podpis má rovnocenný právní účinek jako podpis vlastnoruční, stejně jako zaručený a prostý elektronický podpis. Právní účinky by měly být vymezeny vnitrostátním právem, ale neměly by být v rozporu s požadavky stanovenými v eIDAS. Tento typ podpisu je nejbezpečnější a podle nařízení eIDAS musí být takto vytvořený podpis uznán ve všech členských státech EU.

Srovnání typů elektronického podpisu se nachází v tabulce 1.

Tabulka 1: Shrnutí typů elektronického podpisu.

	Elektronický podpis prostý	*Zaručený elektronický podpis*	*Kvalifikovaný elektronický podpis*
Jednoduchost použití (software)	Ano	Ano	Ne
Zabezpečení	Ne	Ano	Ano
Užití v jednání se státem (ČR)	Ne	Ne	Ano
Užití v jednání mezistátně (EU)	Ne	Ne	Ano
Hardware (token)	Ne	Ne	Ano

2. TECHNICKÉ PROSTŘEDKY

2.1 Tvorba elektronického podpisu

Elektronický podpis prostý, jak bylo zmíněno výše, je například podepsání se na konci emailu v podobě uvedení svého jména a příjmení nebo přiložení elektronické podoby ručního podpisu. Elektronický podpis prostý je jednoduché vytvořit, avšak neposkytuje žádnou ochranu datům, která podepisuje.

Existují aplikace (převážně zdarma) pro mobilní telefony, kde se uživatel podepíše na obrazovku, podpis se převede do vektoru a uživatel si jej může poslat, některé aplikace nabízí synchronizaci s počítačem. Většinu podpisů lze následně upravovat (barva podpisu, velikost atd.) a uložit v obrázkovém formátu (jpeg, png atd.). Mobilní aplikace často pochází od soukromých subjektů: Office od Microsoft Corporation, Digital Signature or TechinGif, Adobe Fill & Sign od Adobe, JetSign Signature App od JetSign atd.

Počítačovou variantou pro elektronický podpis prostý je například užití Adobe Acrobat Reader a jeho funkce Adobe Fill & Sign. Po otevření dokumentu v Adobe programu se zvolí funkce sign. Funkce sign nabízí přidání podpisu anebo přidání iniciál. Podpis může být napsán na klávesnici a následně mu může být změněn styl fontu, nebo může být nakreslen (například myší, nebo přes grafický tablet). Vytvořený podpis je možné uložit, takže při podepisování dalšího dokumentu se celý proces ulehčí a podpis bude konzistentní v následujících dokumentech. Další variantou je vyfocení ručně napsaného podpisu, převedení fotky do počítače a vektorizování v grafickém programu (vektorizace většinou neproběhne přesně, budou nutné menší úpravy), nebo odstranění pozadí, pokud je fotka dostatečně kvalitní a není třeba měnit velikost.

Poslední variantou jsou online softwary. Pro použití se většinou musí uživatel na stránce zaregistrovat, nahraje dokument, který chce podepsat a následné upravování je stejné jako u Adobe Acrobat Reader. Uživatel má možnosti napsat svůj podpis a upravit font, nakreslit vlastní nebo nahrát obrázek svého podpisu. Po uložení stačí dokument stáhnout a pro další podepsání je podpis uživatele uložen. Do této kategorie spadá například www.pandadoc.com, www.signnow.com, www.smallpdf.com atd.

Zaručený elektronický podpis jsou data, která jsou zabezpečena privátním klíčem a měla by zajišťovat integritu a nepopiratelnost původu podepsaných dat. Avšak takový elektronický podpis si může signatář vytvořit i sám doma a nepotřebuje k tomu třetí stranu, která prokáže jeho identitu.

2.1.1 Certifikát

Pro získání kvalifikovaného elektronického podpisu je nutností certifikát. U kvalifikovaného elektronického podpisu třetí strana ověří uživatele, jestli je to opravdu on a bude uchovávat údaje pro ověření identity uživatele. Níže popsaný postup

certifikace je převzatý ze stránky První certifikační autority, jedná se o postup k získání kvalifikovaného certifikátu od kvalifikované certifikační autority [3].

Postup certifikace:

1) **Výběr certifikátu** – jedná se o výběr mezi osobními certifikáty určenými pro fyzické osoby, nebo pro fyzické osoby, jež požadují uvedení identifikace zaměstnavatele, či výběr mezi certifikáty pro právnické osoby.
2) **Elektronická žádost a potřebné dokumenty** – žadatel o kvalifikovaný elektronický podpis předkládá identifikační dokumenty podle vybraného certifikátu. Obecně se vždy jedná o občanský průkaz, nebo pas a další doklady totožnosti, pokud se má certifikát vázat k firmě, musí být předložen doklad existence společnosti (ne starší než šest měsíců) a potvrzení o zaměstnaneckém poměru.
3) **Návštěva certifikační autority** – nutností je navštívit registrační autoritu, kde žadatel předloží elektronickou žádost a požadované osobní doklady. Následně je žadateli vydán certifikát.
4) **Instalace certifikátu do počítače** – vydaný certifikát je třeba nainstalovat do počítače, případně do čipové karty.
5) **Obnova platnosti certifikátu** – uživatel je vždy informován před vypršením platnosti a má možnost požádat o vydání dalšího (následného) certifikátu. Pokud tak učiní s doposud platným certifikátem, stačí podat žádost, zaplatit a certifikát bude zaslán elektronickou cestou.

Kvalifikovaný certifikát můžeme přirovnat k občanskému průkazu či pasu (Tabulka 2). Podstatným rozdílem je, že průkazy totožnosti jsou v tištěné podobě. V některých evropských zemích se dokonce vydávají občanské průkazy ve tvaru čipové karty, na které jsou certifikáty držitele karty [2].

Obsah certifikátu má identifikovat danou osobu, a tudíž v něm můžeme najít podobnost s občanským průkazem, který taktéž identifikuje jedince. Takové srovnání se nachází v tabulce 2.

Tabulka 2: Srovnání certifikátu a občanského průkazu [2].

Certifikát	**Občanský průkaz**
Verze	Verze formátu občanského průkazu
Pořadové číslo	Číslo občanského průkazu
Algoritmus podpisu	Způsob podpisu úředníka, typy ochranných prvků
Vydavatel	Vydal
Platnost	Platnost
Předmět: jméno, adresa atd.	Jméno a adresa
Rozšíření certifikátu	Nepovinné údaje
Veřejný klíč	-
-	Fotografie

Ukázka certifikátu se nachází v příloze A. Jedná se o standard X.509, což je standard pro podepisování přes veřejný klíč. Obsah je následující:

- **Version** = verze certifikátu (X.509 v3).
- **Serial Number** = sériové číslo podpisu.
- **Signature algorithm** = ID algoritmu použitého pro zašifrování klíče (sha256WithRSAEncryption).
- Položka **Subject** (v tabulce 2 nazvaná předmětem) charakterizuje žadatele a položka **Issuer** (v tabulce 2 nazvaná vydavatelem) používají stejný formát pro zpracování dat, tzv. jedinečné jméno. Součástí jedinečného jména jsou zkratky:
    - C = stát, resp. jeho mezinárodní poznávací značka (CZ);
    - CN = název, u fyzické osoby jméno a příjmení, u právnické osoby název subjektu (MUDr. Marie Novotná, I.CA Qualified 2 CA/RSA 02/2016);
    - O = název firmy (První certifikační autorita, a.s.);
    - ST = kraj (Zlínský);
    - L = místo (Zlín, tř. Tomáše Bati 21, 76001);

- GN = jméno (Marie);
- SN = příjmení (Novotná);
- SP = provincie;
- OU = oddělení nebo organizační jednotka;
- T = pozice v zaměstnání;
- P = pseudonym;
- E = adresa elektronické pošty [2].

- **Validity** = platnost certifikátu.
- **Subject Key Algorithm** = informace o veřejném klíči (modulus, exponent).
- **X.509v3 extension** = dodatky. U první certifikační autority se jedná o specifikace vybraného typu elektronického podpisu, v ukázce to je specificky Twin ID. Dále je blíže specifikován standard X.509v3.
- **Signature algorithm** = digitální podpis vytvořený pomocí algoritmu, který byl definován na začátku certifikátu.

Standard X.509 se může kódovat a převádět do formátu PEM (Privacy Enhanced Mail), což je formát Base64 ASCII a DER (Distinguished Encoding Rules), což je binární forma certifikátu.

První certifikační autorita působící v České republice nabízí několik typů kvalifikovaných certifikátů pro elektronický podpis s následujícími technickými náležitostmi:

- **(78) I.CA** – použitým hashem je SHA256, poskytnutá platnost od února 2016 do února 2026.

```
Issuer: SERIALNUMBER=NTRCZ-26439395, CN=I.CA Root CA/RSA, O="První certifikační autorita, a.s.", C=CZ
Subject: SERIALNUMBER=NTRCZ-26439395, O="První certifikační autorita, a.s.", CN=I.CA Qualified 2 CA/RSA 02/2016, C=CZ
```

- **(128) I.CA** – použitým hashem je SHA512, poskytnutá platnost od června 2019 do června 2029.

```
Issuer: CN=I.CA Root CA/ECC 12/2016, OID.2.5.4.97=NTRCZ-26439395, O="První certifikační autorita, a.s.", C=CZ
Subject: OID.2.5.4.97=NTRCZ-26439395, O="První certifikační autorita, a.s.", CN=I.CA Qualified 2 CA/ECC 06/2019, C=CZ
```

- **(195) I.CA** – použitým hashem je SHA256, poskytnutá platnost od července 2015 do července 2025.

```
Issuer: SERIALNUMBER=NTRCZ-26439395, CN=I.CA Root CA/RSA, O="První certifikační autorita, a.s.", C=CZ
Subject: SERIALNUMBER=NTRCZ-26439395, O="První certifikační autorita, a.s.", CN=I.CA Qualified CA/RSA 07/2015, C=CZ
```

Jednotlivé typy kvalifikovaných certifikátů pro elektronický podpis mají odlišné zpracování Subject, Issuer (v seznamu znázorněno v šedých boxech) a jsou zahrnuty odlišné X.509v3 extensions.

2.2 Standardy

Technické standardy poskytuje Evropský ústav pro telekomunikační normy, anglicky European Telecommunications Standards (ETSI). Dále také „ETSI“. ETSI aktualizuje staré standardy a vydává nové každý měsíc, následující standardy jsou základními pro technické parametry elektronického podpisu. Pod ETSI funguje technická komise Technical Committee Electronic Signatures and Infrastructures (ESI), která je přímo zaměřená na elektronické podpisy a infrastruktury.

Standardy, které ESI vytváří se zaměřují na podporu eIDAS a na podporu mezinárodních požadavků na zajištění důvěry v elektronickou komunikaci [4].

Mezi ESI standardy patří referenční formáty XAdES (XML Advanced Electronic Signatures), PAdES (PDF Advanced Electronic Signature), CAsES (CMS Advanced Electronic Signature) a ASiC (Associated Signature Container).

Všechny formáty poskytují dlouhodobou nepopiratelnost. PAdES umožňuje podepisovat a přikládat data v prostředí PDF softwarů, má schopnost připojit i XML data a podpis může být zobrazený ve formě ručně psaného podpisu. CAdES umožňuje podepisovat jakákoliv data a podpis je v binárním tvaru. XAdES poskytuje XML verzi, podle softwaru poskytuje i podpis ve formě ručně psaného podpisu [5].

2.2.1 Formáty elektronických podpisů

ESI: Electronic Signature Formats, jedná se o jeden z prvních standardů, jenž se vztahuje k formátu elektronického podpisu. Standard vznikl v prosinci v roce 2003 [6] a pojednává o bezpečnostních mechanismech pro ochranu důvěry v elektronickou komunikaci. Standard o formátech elektronických podpisů odkazuje na stávající standardy zabývající se problematikou:

- RFC standardy;
- Standard ITU-T X.509.

RFC standardy, jichž autorem je Internet Engineering Task Force (IETF), česky Komise pro technickou stránku internetu, pojednávají o Cryptographic Message Syntax (CMS) a Internet X.509 Public Key Infrastructure Certificate ve spojitosti s elektronickým podpisem. CMS používá kryptografie pro zabezpečení a zašifrování digitálních podpisů.

Standard ITU-T X.509, jehož autorem je ISO neboli International Organization for Standardization, česky Mezinárodní organizace pro normalizace, definuje rámec pro PKI, pro infrastrukturu správy a distribuce veřejných klíčů. Standard X.509 je blíže popsán v podkapitole Certifikát.

Electronic Signature Formats standard se dá aplikovat na jakoukoliv službu ať už se jedná o SIM karty, speciální programy pro elektronické podpisy, nebo smart cards atd.

2.3 Ověření elektronického podpisu

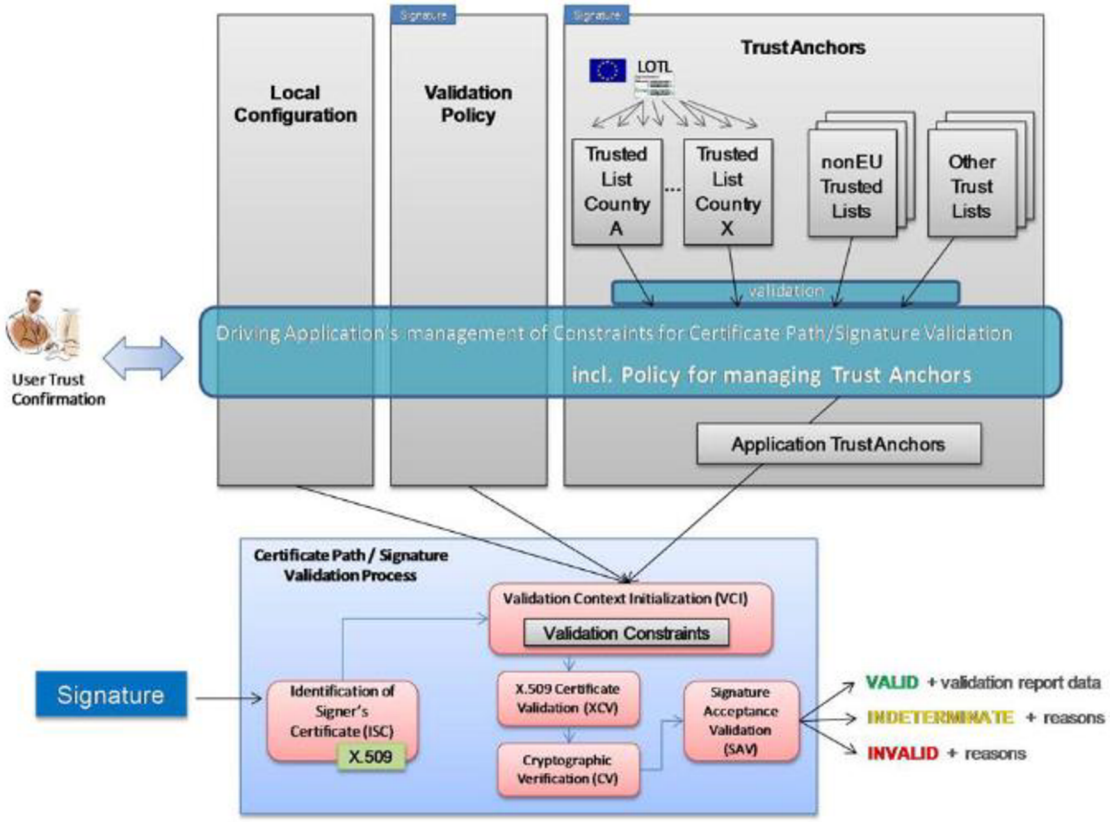
V publikaci Electronic Signatures and Infrastructures (ESI), Trusted Lists se v příloze o používání důvěryhodných seznamů nachází příklad využití důvěryhodného seznamu pro kontrolu validace kvalifikovaného elektronického podpisu [7].

Důvěryhodným seznamem se rozumí seznam všech kvalifikovaných poskytovatelů služeb vytvářejících důvěru a samotných poskytovaných kvalifikovaných služeb vytvářejících důvěru. Kontrolní orgány každého státu tyto seznamy poskytují Evropské komisi, důvěryhodné seznamy se musí pravidelně kontrolovat, zda nedošlo ke změnám, které by mohly zpochybnit důvěryhodnost.

Pojmem důvěryhodná kotva se rozumí certifikační autorita, která poskytuje jeden nebo více důvěryhodných certifikátů obsahující veřejné klíče. Tento pojem také může odkazovat na samotný certifikát takové certifikační autority [8]. Ověření platnosti elektronického podpisu je následující (znázornění procesu se nachází na obrázku 1, jenž je převzat od ETSI):

- Aplikační management pro omezení certifikační cesty, resp. potvrzení validace:
  - Lokální konfigurace.
  - Zásady ověřování.
  - Důvěryhodné kotvy: evropský prohlížeč důvěryhodných seznamů obsahuje seznamy všech evropských států, které případně porovná i s důvěryhodnými seznamy jiných zemí, aby mohlo dojít k aplikaci kotev.
- Validační cesta elektronického podpisu:
  - Kontrola identifikace uživatele certifikátu.
  - Validace kontextu – spojení dat z aplikačního managementu.
  - Kontrola validace certifikátu.
  - Kontrola kryptografických prostředků.
  - Přijetí podpisu: **platný**, **neurčitý** a **neplatný**.

Takovéto ověření nastává v případě, že se jedná o certifikát podle standardu X.509. Výše popsaný postup je znázorněn na obrázku 1.



Obrázek 1: Příklad použití důvěryhodného seznamu v kontextu potvrzení elektronického podpisu [7].

3. ELEKTRONICKÝ PODPIS VE STÁTECH EVROPSKÉ UNIE

V Evropě se jednotlivé státy musí řídit nařízením 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 [1], neboli eIDAS.

Obecně pro každý stát platí, že elektronický podpis je považován za platný, pokud byl použit v době své platnosti. To znamená, že pokud se na něj odvoláváme v právním styku ohledně skutečnosti, která nastala např. v minulém kalendářním roce, vše závisí na tom, zdali byl elektronický podpis platný v této konkrétní době, a není podstatné, zda je platný i v době, kdy se problém začne právně řešit.

Dále platí, že každý stát má kontrolní orgán, jenž musí uchovávat informace a aktualizovat stav elektronických podpisů, jejich prostředků a kvalifikovaných subjektů a tyto informace poskytovat Evropské komisi. Evropská komise uchovává informace k elektronickému podpisu i seznam kvalifikovaných certifikačních autorit poskytujících důvěru svých členských států na svých stránkách [9].

Jednotlivé státy si samostatně specifikují regulace, kdy je elektronický podpis legální, a které typy elektronického podpisu se mohou použít při určitých jednáních, popřípadě situacích. Tyto regulace však nesmí být v rozporu s nařízením EU.

3.1 Česká republika

3.1.1 Přehled českých zákonů týkajících se elektronického podpisu

V České republice se o elektronickém podpisu pojednává v zákoně č. 297/2016 Sb., Zákon o službách vytvářejících důvěru pro elektronické transakce.

Předmětem úprav tohoto zákona jsou zejména kvalifikovaní poskytovatelé služeb vytvářejících důvěru (postupy, požadavky a povinnosti) a působnost Ministerstva vnitra, což je kontrolní orgán pro Českou republiku v problematice elektronického podpisu.

V zákoně se vyskytuje i nový pojem, který je převzatý z původního, již neplatného zákona, a to *uznávaný elektronický podpis*. Uznávaným elektronickým podpisem se v České republice rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu, nebo kvalifikovaný elektronický podpis, záleží na znění dané části zákona. Uznávaný elektronický podpis však lze použít pouze v České republice. Pro komunikaci se zahraničím je potřeba použít kvalifikovaný elektronický podpis.

Dle § 6 tohoto zákona *„…lze použít pouze uznávaný elektronický podpis, podepisuje-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti.“* [10]. V § 5 je zmíněno, že kvalifikovaný elektronický podpis je vyžadován v jednání se státem,

územním samosprávným celkem či právnickou osobou zřízenou zákonem. Pro použití kvalifikovaného elektronického podpisu v jednání s ministerstvy musí být použití kvalifikovaného elektronického podpisu přímo zmíněno v zákoně. Je tomu tak například v katastrálním zákoně, kde je nutné použít kvalifikovaný elektronický podpis s časovým razítkem.

Kromě této zajímavosti se zákon o službách vytvářejících důvěru pro elektronické transakce příliš neliší od úprav ostatních evropských států. Kvalifikovaný poskytovatel služeb, nebo také kvalifikovaná certifikační autorita, uchovává po dobu 10 let dokumenty související s vydaným kvalifikovaným certifikátem pro elektronické podpisy. Po uplynutí této doby poskytovatel uchovává dalších 15 let údaje, na jejichž základě byla ověřena totožnost. Dále se v § 14 a § 15 specificky pojednává o poskytování služeb Správou základních registrů, poté jsou uvedeny přestupky, a přechodná ustanovení a zákony, jež se tímto zákonem ruší [10].

3.1.2 České kvalifikované certifikační autority

Česká republika má celkem šest kvalifikovaných certifikačních autorit:

- **První certifikační autorita, a. s.** se sídlem v Praze, působící od roku 2010, poskytuje kvalifikovaný certifikát pro elektronický podpis (většinou přes čipové karty, dva typy se váží na USB token), elektronickou pečeť, kvalifikovaný certifikát pro webovou autentizaci, časová razítka a další.
- **Česká pošta, s. p.** od roku 2016 také poskytuje služby vytvářející důvěru prostřednictvím USB tokenů a čipových karet, časová razítka i elektronickou pečeť.
- **Eldentity a. s.** působící od roku 2017, poskytuje kromě USB tokenů a čipových karet IDPrime zabudované v MicroSD kartě. Všechny výše vyjmenované se nachází i na stránkách Policie České republiky.
- Další certifikační autoritou pro Českou republiku je **Správa základních registrů (2019)**, která poskytuje pouze jeden typ čipové karty.
- Podle seznamu Evropské komise patří do kvalifikovaných certifikačních autorit i **SEFIRA spol. s. r. o** a **Software602 a. s.**

Seznam vydávaných kvalifikovaných prostředků pro vytváření elektronických podpisů a kvalifikovaných certifikačních autorit v České republice se nachází na stránce Ministerstva vnitra v oddělení eGovernment [11].

Informace jsou na stránkách Evropské komise aktualizovány k 18. 5. 2021 [9].

3.2 Slovenská republika

3.2.1 Přehled slovenských zákonů týkajících se elektronického podpisu

Ve Slovenské republice se jedná o zákon č. 272/2016 Sb., o důvěryhodných službách pro elektronické transakce na vnitřním trhu a o změně a doplnění některých zákonů (zákon o důvěryhodných službách), který vstoupil v účinnost 1. 8. 2019 [12].

Předmětem zákona jsou podmínky a povinnosti poskytování důvěryhodných služeb kvalifikovaných certifikačních autorit. Zákon také blíže popisuje působení Národního bezpečnostního úřadu, což je kontrolní orgán pro Slovenskou republiku.

Kvalifikovaný elektronický podpis ve styku s orgány veřejné moci může jako osobní atribut obsahovat rodné číslo, číslo pasu a číslo identifikační karty.

Novým pojmem je mandátní certifikát, což je ve slovenském právu kvalifikovaný certifikát pro elektronický podpis vydaný fyzické osobě, aby mohla jednat za jinou osobu či orgán veřejné moci. Jejich jménem může jednat, nebo vykonávat činnost a funkce, které spadají pod zastupující osobu či orgán. Mandátní certifikát obsahuje identifikační údaje o mandatářovi (ten, který vykonává činnost), následně informace o mandantovi (ten, za kterého je činnost vykonávaná). Zánik mandátního certifikátu nastává při úmrtí, zaniknutí či dokonání činnosti. O zrušení certifikátu je však nutné požádat.

Pozn.: Ministerstvo vnitra Slovenské republiky má na svých stránkách zpracované informace ohledně elektronického podpisu, včetně nejčastějších dotazů [13].

3.2.2 Slovenské kvalifikované certifikační autority

Slovenská republika má sedm aktivních kvalifikovaných certifikačních autorit, k nimž patří:

- **Prvá certifikačná autorita a. s.** poskytující kvalifikovaný certifikát pro elektronický podpis, pečeť a časové razítko.
- **Ministerstvo obrany Slovenskej republiky** poskytující kvalifikovaný certifikát jak pro elektronický podpis i pečeť, a kvalifikované časové razítko.
- **NASES** (Národná agentúra pre sieťové a elektronické služby) poskytující kvalifikovaný certifikát pro elektronický podpis, i pro pečeť.
- **Národný bepečnostný úrad**, který nabízí nejvíce služeb ohledně kvalifikovaného elektronického podpisu. Patří zde všechny kvalifikované certifikáty, a to certifikát pro elektronický podpis, pečeť, časové razítko.
- **Viasec, s.r.o.** poskytuje pouze časové razítko.
- **Disig** poskytuje podobné množství služeb jako Národný bezpečnostný úrad.
- **Brainit.sk, s.r.o.** poskytuje kvalifikovaný certifikát pro elektronický podpis a pečeť.

Informace jsou na stránkách Evropské komise aktualizovány k 19. 5. 2020 [9].

3.3 Spolková republika Německo

3.3.1 Přehled německých zákonů týkajících se elektronického podpisu

Zákon o regulaci elektronického podpisu je ve Vertrauensdienstegesetz (VDG), resp. zákonu o důvěryhodných službách [14], z roku 2017.

Kvalifikované certifikáty pro elektronické podpisy mohou obsahovat informace o oprávnění žadatele k zastupování třetí osobou (pokud lze prokázat souhlas třetí osoby), úřední a pracovní informace a další osobní informace. Paragraf 12 tedy umožňuje zastupování a dává možnost použití jakýchkoliv osobních informací jako součást kvalifikovaného certifikátu. Dále umožňuje zapsání pseudonymu do kvalifikovaného certifikátu (pokud bude součástí zastupování, třetí osoba musí o pseudonymu vědět a souhlasit).

Zrušení kvalifikovaného certifikátu nastává po zažádání, pokud byl certifikát vydán na základě nesprávných informací, při konci platnosti, či při padělání. Zrušit certifikát může i přímo poskytovatel důvěryhodných služeb. Tato praxe nastává u většiny evropských států.

Kontrolním orgánem je Bundensnetzagentur (Federální síťová agentura). Může určit soukromý objekt jako kvalifikovanou certifikační autoritu, pokud certifikační autorita splňuje podmínky v souladu s eIDAS. Může jej jmenovat s časovým omezením a jmenování může být spojeno s dalšími podmínkami (oddíl 17 [14]).

Pozn.: Používání elektronických podpisů a kvalifikovaných elektronických podpisů není v Německu běžné, protože pořízení takového podpisu je drahé [15].

3.3.2 Německé kvalifikované certifikační autority

Německo má celkem třináct aktivních kvalifikovaných certifikačních autorit.

Patří mezi ně například tyto:

- **Bank-Verlag GmbH** (GmbH v němčině znamená společnost s ručením omezením) se sídlem v Kolíně nad Rýnem, která poskytuje kvalifikovaný certifikát pro elektronický podpis a pečeť.
- **Deutsche Post AG**, jedná se o německou poštu na stejné úrovni jako Česká pošta. Poskytuje kvalifikovaný certifikát pro elektronický podpis.
- **Bundesagentur fuer Arbeit**, je v Německu vládní úřad pod ministerstvem práce a sociálních věcí. Poskytuje kvalifikovaný certifikát pro elektronický podpis a pro časové razítko.
- **D-Trust GmbH** poskytuje kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.
- **DGN Deutsches Gesundheitsnetz Service GmbH** poskytuje kvalifikovaný certifikát pro elektronický podpis a časové razítko.

Informace jsou na stránkách Evropské komise aktualizovány k 4. 5. 2021 [9].

3.4 Rakouská republika

3.4.1 Přehled rakouských zákonů týkajících se elektronického podpisu

Hlavní je federální zákon o elektronických podpisech a důvěryhodných službách pro elektronické transakce z roku 2016 (modifikován v roce 2018, aktualizován pravidelně) [16].

Kvalifikovaný elektronický podpis musí splňovat zákonný požadavek dle § 886 ABGB, což je rakouský občanský zákoník, podle kterého musí být podpis ověřen, lze nahradit soudním nebo notářským ověřením, replika podpisu je dostatečná pouze v některých obchodních jednáních, ostatní požadavky stanoví notář, či právník. Smluvní ujednání zůstávají nedotknuta a ponechána na kvalifikovaném subjektu. Závěť nelze napsat v elektronické podobě bez ověření notářem či právníkem. V obchodním styku vše závisí na domluvě stran (kvalifikovaný elektronický podpis není omezen). Kvalifikované subjekty se zavazují k úchově a ochraně dat. Přenos údajů je povolen jen oprávněným osobám. Sám uživatel musí požádat o zrušení certifikátu, pokud došlo ke ztrátě, nebo pokud existují náznaky, že byly ohroženy údaje. Zrušení ze strany služby nastává v případě, že orgán dozoru nařídí pozastavení, smrti podepsaného, či pokud byl certifikát založen na základě nesprávných informací. V rakouském právu se objevuje i pojem pozastavení kvalifikovaného certifikátu. Pozastavením se rozumí, že certifikát ztrácí platnost. Pokud tato doba přesáhne období dva týdny, je certifikát zcela zrušen.

Kontrolní orgán určuje ministr pro digitalizaci na základě dostatečného technického vybavení, zaměstnání personálu a dalších požadavků. Kontrolní orgán musí splňovat stejné požadavky jako v okolních státech (seznamy posílá Evropské komisi atd.).

3.4.2 Rakouské kvalifikované certifikační autority

Rakousko má pět aktivních kvalifikovaných certifikačních autorit a všechny jsou společnostmi s ručením omezeným:

- **Rundfunk und Telekom Regulierungs-GmbH,** společnost poskytuje jen certifikát pro elektronické pečetě (není kvalifikovaný).
- **PrimeSign GmbH** poskytuje kvalifikovaný certifikát pro elektronický podpis a elektronickou pečeť.
- **A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH** poskytuje kvalifikovaný i obyčejný certifikát pro elektronický podpis a elektronickou pečeť.
- **Swisscom IT Services Finance S.E.** taktéž poskytuje kvalifikovaný i obyčejný certifikát pro elektronický podpis a elektronickou pečeť.
- **e-commerce monitoring GmbH** poskytuje kvalifikovaný certifikát pro elektronický podpis a časové razítko, také obyčejný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.

Informace jsou na stránkách Evropské komise aktualizovány k 25. 3. 2021 [9].

3.5 Polská republika

3.5.1 Přehled polských zákonů týkajících se elektronického podpisu

Hlavním zákonem pro regulaci elektronických podpisů je Zákon o usługach zaufania oraz identyfikacji elektronicznej (zákon o důvěryhodných službách elektronické identifikace) [17].

Kvalifikovaný poskytovatel služeb musí získat od žadatele potvrzení o správnosti informací připojených k certifikátu a případně informovat o zneplatnění daného certifikátu (jedná se přímo o součást zákona). Všechny informace, které by mohly poškodit poskytovatele či příjemce, musí být důvěrné, mlčenlivost musí dodržovat všechny osoby jednající jako poskytovatel (vyžádat si je může soud, ministr pro digitalizaci), mlčenlivost trvá 10 let ode dne ukončení právního vztahu.

Polské právo se v postavení k elektronickému podpisu jeví podobně jako rakouské poměrně otevřeně – až na vztah poskytovatele s podepisujícím (mlčenlivost, zrušení, případně zneplatnění). Část zákona byla věnována i kvalifikovanému elektronickému podpisu při komunikaci se soudem nebo státním orgánem, kde bylo zdůrazněno, že dokument zaslaný s tímto podpisem je platný.

Kontrolním orgánem v Polsku je Narodowe Centrum Certyfikacji (Národní certifikační centrum). Kontrolní orgán splňuje stejné požadavky jako v okolních státech (aktualizuje informace pro Evropské komisi atd.).

3.5.2 Polské kvalifikované certifikační autority

Polsko má šest aktivních kvalifikovaných certifikačních autorit:

- **Asseco Data Systems S. A.** poskytuje kvalifikované certifikáty pro elektronický podpis, pečeť i časové razítko.
- **ENIGMA Systemy Ochrony Informacji Sp. Z o. o.** nabízí kvalifikované certifikáty pro elektronický podpis, pečeť i časové razítko.
- **Krajowa Izba Rozliczeniowa S. A.** poskytuje kvalifikované certifikáty pro elektronický podpis, pečeť i časové razítko.
- **EiroCerst Sp. z o. o.** nabízí kvalifikované certifikáty pro elektronický podpis, elektronickou pečeť i časové razítko.
- **Polish Security Printing Works** nabízí kvalifikované certifikáty pro elektronický podpis, pečeť i časové razítko.
- **Národní Polská Banka** poskytuje zaručený elektronický podpis platný a plně použitelný jen v Polsku.

Informace jsou na stránkách Evropské komise aktualizovány k 2. 4. 2021 [9].

3.6 Francouzská republika

3.6.1 Přehled francouzských zákonů týkajících se elektronického podpisu

Část francouzské právní úpravy se nachází v Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, vyhláška o elektronických podpisech [18].

Vyhláška slouží pro použití článku 1367 občanského zákoníku ve znění z článku 4 vyhlášky 2016-131, kterou se reformuje smluvní právo. V článku 1367 se v první paragrafu mluví o ručně psaném podpisu a ve druhém paragrafu jsou vypsané náležitosti pro elektronický podpis (spolehlivý proces identifikace, spolehlivost se předpokládá do prokázání opaku a měla by být zajištěna totožnost signatáře a integrita dokumentu) [19].

Avis n° 2017-0462 du 18 avril 2017 sur un projet de décret relatif au service de recommandé électronique [20], stanovisko k návrhu vyhlášky týkající se služby elektronické doporučené pošty, je jen návrh vyhlášky nacházející se na webové stránce Légifrance Le service public de la diffusion du droit (veřejná služba šíření zákona). Odkaz na potencionálně ustanovenou vyhlášku podle návrhu není součástí a právní úpravu, která aplikuje nařízení eIDAS, se nepodařilo nalézt. V návrhu se však mluví o aplikaci eIDAS do francouzského práva.

Kontrolním orgánem ve Francii je Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), neboli Národní agentura pro bezpečnost informačních systémů.

3.6.2 Francouzské kvalifikované certifikační autority

Francie má 25 kvalifikovaných certifikačních autorit. Patří zde soukromé subjekty, ale také ministerstva a subjekty spadající pod stát, například:

- **Gendarmerie Nationale**, Národní četnictvo, poskytuje kvalifikovaný certifikát pro elektronický podpis a elektronickou pečeť.
- **Docusign France**, americká společnost se sídlem v San Francisku, působí i na území Francie. Poskytuje kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.
- **Agence Nationale des Titres Sécurisés**, Národní agentura pro zabezpečené tituly, poskytuje pouze kvalifikovaný certifikát pro elektronický podpis.
- **CertEurope**, poskytuje kvalifikovaný certifikát pro elektronický podpis a elektronickou pečeť.
- **Cryptolog International** poskytuje kvalifikovaný certifikát pro elektronický podpis, pečeť a časové razítko.
- **Yousign**, francouzská firma, poskytuje kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.

Informace jsou na stránkách Evropské komise aktualizovány k 29. 4. 2021 [9].

3.7 Španělské království

3.7.1 Přehled španělských zákonů týkajících se elektronického podpisu

Zákonem, který implementuje eIDAS, je Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, zákon upravující některé aspekty elektronických důvěryhodných služeb [21].

Doba platnosti kvalifikovaných certifikátů nesmí přesáhnout 5 let, obecně doba platnosti závisí na charakteristikách a technologii generování podpisu. Implementace zrušení a pozastavení certifikátu se neliší od ostatních evropských států, nastává, pokud podepisující subjekt o ukončení zažádá, při nepravdivých informacích, dle kterých byl podpis vytvořen, v případě, kdy o ukončení rozhodne soud, smrtí signatáře apod. Informace o podpisu budou vydány na základě předložení dokladu totožnosti. Pro kvalifikovaný certifikát se žadatel musí dostavit osobně (během pandemie viru COVID-19 vyšlo královské nařízení, jež umožňovalo získat kvalifikovaný certifikát i dálkově), dále jsou specifikované požadavky, co vše se musí ověřit při určitých typech elektronických certifikátů, tedy pro elektronický podpis, i elektronickou pečeť.

Mezi povinnosti certifikačních autorit patří neuchovávat ani nekopírovat prostřednictvím třetích stran, musí použít spolehlivé systémy, jež zajistí bezpečnost. Musí mít veřejně přístupnou konzultační službu. Následně musí uchovávat po určitou dobu získané informace, stejně jako v našem státě je to 15 let.

Původní Ministerstvo hospodářství a podnikání bylo zrušeno v roce 2020 a jeho funkce převzalo nové ministerstvo. Kontrolním orgánem pro Španělsko je tedy Ministerio de Asuntos Económicos y Transformación Digital, Ministerstvo hospodářství a digitální transformace.

3.7.2 Španělské kvalifikované certifikační autority

Španělsko má 37 kvalifikovaných certifikačních autorit, patří zde i soukromé subjekty, k autoritám řadíme například:

- **Anf Autoridad de Certificación Asociación Anf AC**, která poskytuje kvalifikovaný certifikát pro elektronický podpis, pečeť a časové razítko.
- **Consejo General de la Abogacía Española**, Generální rada španělských právníků, poskytuje kvalifikovaný certifikát pro elektronický podpis a pečeť.
- **Ministerio de Empleo y Seguridad Social**, Ministerstvo zaměstnanosti a sociálního zabezpečení, poskytuje kvalifikovaný certifikát pro elektronický podpis a elektronickou pečeť.
- **Logalty Prueba por Interposición, S.L.**, poskytuje kvalifikovaný elektronický certifikát pro elektronický podpis, pečeť a časové razítko.
- **Uanataca, S.A**, poskytuje kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.

Informace jsou na stránkách Evropské komise aktualizovány k 5. 5. 2021 [9].

3.8 Italská republika

3.8.1 Přehled italských zákonů týkajících se elektronického podpisu

V Itálii mají Codice dell'amministrazione digitale Decreto Legislativo 7 marzo 2005, n. 82, což je Kodex digitální správy, jedná se o legislativní nařízení. V kodexu je několik článků, jež jsou dedikované elektronickému kvalifikovanému podpisu. Agentura pro digitální Itálii v dubnu 2021 uveřejnila článek, který je věnován kvalifikovanému elektronickému podpisu a právním úpravám [22]. Agentura pro digitální Itálii poskytuje průvodce pro připojování podpisů, upozorňuje na některé právní úpravy, i na zrušené.

O elektronickém podpisu blíže pojednává článek 35 o bezpečných postupech pro generování kvalifikovaného podpisu, článek 21 týkající se dokumentů, které jsou podepsány zaručeným, kvalifikovaným nebo digitálním podpisem a článek 25 o ověřeném podpisu, což je elektronický podpis ověřený notářem nebo jiným veřejným činitelem. Článek 24 pojednává o digitálním podpisu, což je jedinečný podpis Itálie, kdy se jedná o podpis, který je jednoznačně spojen s unikátním předmětem nebo dokumentem. Připojení digitálního podpisu nahrazuje pečeť, razítko a jiné známky jakéhokoliv druhu. Pro generování digitálního podpisu se musí použít kvalifikovaný certifikát.

Italským kontrolním orgánem je Agenzia per l'Italia Digitale, Agentura pro digitální Itálii. Statistické údaje o šíření kvalifikovaných důvěryhodných služeb se nachází na stránkách Agentury pro digitální Itálii [23].

3.8.2 Italské kvalifikované certifikační autority

V Itálii je 23 certifikačních autorit. Z toho některé jsou určeny státem, například Ministerstvo vnitra, které však na stránkách Evropské komise nemá vypsané typy služeb, jež poskytuje. Je pravděpodobné, že služby nabízené ministerstvem nesplňují nařízení eIDAS, ale fungují na národní úrovni. Z autorit, které mají vypsané typy služeb, které poskytují uvádíme:

- **Ministero della Difesa**, Ministerstvo obrany, nabízí kvalifikovaný certifikát pro elektronický podpis a časové razítko.
- **Namirial S.p.A.**, společnost nabízí kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.
- **Consiglio Nazionale del Notariato**, Národní rada notářů, poskytuje kvalifikovaný certifikát pro elektronický podpis a časové razítko.
- **Azienda Zero** nabízí kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.
- **InfoCamere S.C.p.A.** poskytuje kvalifikovaný certifikát pro elektronický podpis, elektronickou pečeť a časové razítko.

Informace jsou na stránkách Evropské komise aktualizovány k 14. 5. 2021 [9].

3.9 Finská republika

3.9.1 Přehled finských zákonů týkajících se elektronického podpisu

Ve Finsku se k elektronickému podpisu váže Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (zákon o silné elektronické identifikaci a elektronických důvěryhodných službách) [24] a Viestintä: Määräys sähköisistä tunnistus- ja luottamuspalveluista, Viestintävirasto 72 A/2018 M (nařízení o elektronické identifikaci a důvěryhodných službách) [25]. Oba dokumenty jsou přeloženy do angličtiny.

Zákon o silné elektronické identifikaci a elektronických důvěryhodných službách je platný od roku 2009 a v roce 2019 byl aktualizován kvůli evropským nařízením. Novým pojmem je silná elektronický identifikace, kterou se rozumí identifikace a ověření pravosti osoby, právnické osoby, nebo fyzické osoby zastupující právnickou osobu elektronickými prostředky, jež vyžadují zvýšenou úroveň zabezpečení. Zákon obsahuje klasické regulační prvky jako faktory ověření použité v metodě identifikace, požadavky a povinnosti poskytovatele, odpovědnost za škody, zásady identifikace apod. Zákon před nařízením eIDAS sloužil jako výchozí, po nařízení jsou části nahrazeny zmínkou, že se povinnosti a požadavky mají řídit podle evropského nařízení. Zajímavostí je, že aktualizace některých částí proběhla i 26. 3. 2021 (příklad jedné z úprav je uveden v následujícím odstavci).

Kontrolním a správním orgánem je Finnish Transport and Communications Agency (Traficom), přibližný překlad Ministerstvo dopravy a komunikace. Finské národní centrum pro kybernetickou bezpečnost v Traficomu sleduje a dohlíží na dodržování požadavků, vydává podrobnější předpisy a vede seznam poskytovatelů identifikačních služeb, kteří splňují požadavky [26]. Poslední aktualizace v zákoně o silné elektrotechnické identifikaci a elektronických důvěryhodných službách ze dne 26. 3. 2021 udává TRAFICOMu úkoly, jako povinnost sledovat dodržování zákona, každoročně zpracovat statistiky a dodržovat povinnosti vyplývající z nařízení eIDAS (plné znění viz zákon ve finštině [27]).

3.9.2 Finské kvalifikované certifikační autority

Finsko má jen jednu tuto autoritu:

- **Digital and Population Data Services Agency**, autorita poskytuje kvalifikovaný certifikát pro elektronický podpis a kvalifikovaný certifikát pro webovou autentizaci.

Informace jsou na stránkách Evropské komise aktualizovány k 1. 4. 2021 [9].

3.10Švédské království

3.10.1 Přehled švédských zákonů týkajících se elektronického podpisu

Na stránkách švédského parlamentu jediný zákon obsahující zmínku o eIDAS je Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning, nařízení 2018:1486 s pokyny pro agenturu pro digitální správu [28].

Kontrolním orgánem je Post and Telecom Authority (PTS).

3.10.2 Švédské kvalifikované certifikační autority

Certifikační autoritou ve Švédsku jsou:

- **TrustWeaver AB** poskytující kvalifikovaný certifikát pro kvalifikovaný elektronický podpis a kvalifikovanou pečeť.
- **ZealiD AB** poskytující certifikát pro kvalifikovaný elektronický podpis.

Informace jsou na stránkách Evropské komise aktualizovány k 22. 2. 2021 [9].

4. ELEKTRONICKÝ PODPIS A ESVO

Evropské sdružení volného obchodu neboli ESVO, anglicky European Free Trade Association (EFTA), dále také „ESVO“.

Do ESVO patří čtyři státy: Norsko, Island, Lichtenštejnsko a Švýcarsko. Tyto státy až na Švýcarsko vytvořily s Evropskou unií Evropský hospodářský prostor (EHP). Kromě rozšíření čtyř základních svobod (volný pohyb zboží, osob, služeb a kapitálu) se k EHP váže i povinnost zavedení určitých částí legislativy Evropské unie do legislativy jednotlivých zemí.

Co tato skutečnost znamená pro kvalifikovaný elektronický podpis a eIDAS? Norsko, Island a Lichtenštejnsko se musí řídit evropským nařízením eIDAS (od roku 2018) a aktualizují své aktivní kvalifikované certifikační autority Evropské komisi.

4.1 Norské království

4.1.1 Přehled norských zákonů týkajících se elektronického podpisu

Hlavní zákon zabývající se elektronickým podpisem je Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester), zákon o provádění nařízení EU o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu (zákon o elektronických důvěryhodných službách).

Zákon vstoupil v platnost v červnu 2018. Král má vyhrazenu většinu pravomocí, například určuje, který orgán má být kontrolním orgánem a spravovat list Evropské komisi, nebo který orgán má dohlížet na dodržování ustanovení v tomto zákoně, může udělit pokutu činnému orgánu při porušení nařízení a rozhoduje o vstupu v platnost. Některé pravomoci spadají pod Ministerstvo místní správy a modernizace [29].

Kontrolním a správním orgánem je Nkom, Norský komunikační úřad [30].

4.1.2 Norské kvalifikované certifikační autority

V Norsku je devět aktivních kvalifikovaných certifikačních autorit, ze zmiňovaných devíti poskytuje šest jen kvalifikovaný certifikát pro elektronický podpis (například uživatel je bez možnosti pořídit časové razítko nebo elektronickou pečeť):

- **Bankenes ID-tjeneste AS,**
- **Danske Bank,**
- **Nordea Bank Abp filial i Norge,**
- **SpareBank 1 Utvikling DA,**
- **Commfides Norge AS** a **Buypass AS** nabízí i certifikát pro elektronickou pečeť.

Informace jsou na stránkách Evropské komise aktualizovány k 15. 4. 2021 [9].

4.2 Island

Nepodařilo se získat bližší informace k právní úpravě elektronického podpisu na Islandu. Island by však měl, podobně jako Norsko uznávat nařízení eIDAS a aplikovat jej do své právní úpravy elektronického podpisu.

Island má pouze jednu aktivní kvalifikovanou certifikační autoritu, **Audkenni ehf.**, která poskytuje pouze certifikát pro kvalifikovaný elektronický podpis.

Informace jsou na stránkách Evropské komise aktualizovány k 18. 3. 2021 [9].

4.3 Lichtenštejnské knížectví

V červenci roku 2019 Lichtenštejnsko vydalo úpravu zákona o provedení eIDAS, zákon o elektronických podpisech a důvěryhodných službách pro elektronické transakce. Obsah zákona je převzat od Rakouska (viz kapitola Rakouská republika), Lichtenštejnský zákon se od rakouského liší minimálně [31].

Vláda volí kontrolní orgán, kritérii jsou splnění požadované spolehlivosti, spolehlivý personál s odbornými znalostmi a zkušenostmi, dostatečné technické vybavení, zajišťuje nezbytnou důvěrnost a nestrannost.

Kontrolním orgánem je Amt für Kommunikation, česky Úřad pro komunikaci.

Lichtenštejnsko má dvě kvalifikované certifikační autority:

- **FLZ-Anstalt** poskytující kvalifikovaný certifikát pro elektronický podpis.
- **Office for Communications**, která poskytuje jen certifikovanou pečeť.

Informace jsou na stránkách Evropské komise aktualizovány k 1. 3. 2021 [9].

4.4 Švýcarská konfederace

4.4.1 Přehled švýcarských zákonů týkajících se elektronického podpisu

Švýcarsko nespadá pod eIDAS, elektronický podpis je v právní úpravě řešen ve Federálním zákoně o certifikačních službách v oblasti elektronického podpisu a další aplikace digitálních certifikátů (ZertES) [32].

Typy elektronického podpisu:

- **Elektronický podpis** – 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. Jedná se o ekvivalent naší definice elektronického podpisu.
- **Fortgeschrittene elektronische Signatur** (pokročilý elektronický podpis) – jednoznačně spojen s majitelem, identifikuje majitele, je generován ze zdrojů, jež majitel má pod svou výhradní kontrolou a musí být možné rozpoznat manipulaci s podpisem. Jedná se o ekvivalent našeho zaručeného podpisu.

- **Geregelte elektronische Signatur** (regulovaný elektronický podpis) – zdokonalený elektronický podpis, který byl vytvořen pomocí zabezpečené služby pro vytváření elektronických podpisů a je založen na certifikátu vydaném fyzické osobě.
    - Lze jej fyzickým osobám nebo subjektům vlastnícím UID. Fyzické osoby se pro uznání musí dostavit osobně a subjekty vlastnící UID, jež nejsou fyzickými osobami, musí být zastoupeny osobně. Za určitých podmínek se žadatel nemusí dostavit osobně.
    - Musí obsahovat: sériové číslo, typ (regulovaný certifikát), jméno (případně pseudonym, nebo identifikační číslo), veřejný kryptografický klíč, dobu platnosti, informace o poskytovateli, další prvky jsou dobrovolné.
    - Federální rada určuje formát regulovaných certifikátů.
- **Qualifizierte elektronische Signatur** (kvalifikovaný elektronický podpis) – regulovaný elektronický podpis založený na kvalifikovaném certifikátu.
    - Lze vydat pouze fyzické osobě.
    - Součástí musí být označení, že je určen pouze pro elektronický podpis. Typ musí být zaznamenán jako kvalifikovaný certifikát.

Zneplatnění certifikátu nastává po podání žádosti, ukáže se nezákonné získání nebo špatně podané informace, propadnutí. Prohlášení neplatnosti musí být oznámeno vlastníkovi, certifikační služby také musí vézt seznamy a federální rada je může kdykoliv zkontrolovat (případně i již neplatné certifikáty). Certifikační služby mají stejné povinnosti jako v případě eIDAS. Součástí zákona jsou mezinárodní dohody, jež zákon uznává za účelem usnadnění mezinárodního používání elektronických podpisů [32].

Tradiční podpis je vyžadován při: pracovních smlouvách, dokumentech psaných rukou a dokumentech, jež musí mít notářské ověření, jako například manželské a dědické smlouvy, realitní transakce a zakládání právnických osob.

4.4.2 Švýcarské certifikační autority

Švýcarsko má čtyři certifikační autority:

- **Swisscom (Schweiz) AG** poskytuje kvalifikovaný certifikát pro elektronický podpis a elektronickou pečeť. Od února 2021 v souladu s eIDAS poskytuje i kvalifikovaný certifikát pro časové razítko.
- **QuoVadis Trustlink Schweiz AG.**
- **SwissSign AG** poskytuje také kvalifikovaný certifikát pro elektronický podpis, pečeť a časové razítko. Součástí jejich služeb jsou další zabezpečovací služby, například varianty SSL a email ID.
- **Federální úřad pro informační technologie, systémy a telekomunikace [33].**

5. ELEKTRONICKÝ PODPIS VE SVĚTĚ

5.1 Spojené království Velké Británie a Severního Irska

Spojené království 31. ledna 2020 opustilo Evropskou unii, proto se na něj nevztahují nařízení vydaná Evropskou unií. Spojené království bude i do budoucna uznávat elektronické podpisy vzniklé ve státech Evropské unie a také se bude do doby, než bude mít vlastní zákony upravující problematiku elektronického podpisu, řídit dle eIDAS.

5.1.1 Přehled anglických zákonů týkajících se elektronického podpisu

Zákon o vystoupení z Evropské unie 2018 obsahuje uznání evropských práv a nároků i po brexitu [34], znamená to, že eIDAS je stále součástí vnitrostátního práva, aby byla zajištěna právní jistota během přechodné doby.

Přechodná doba skončila 1. ledna 2021 a vyústila v tzv. pobrexitovou dohodu. V anglickém znění EU-UK Trade and Cooperation Agreement (TCA). V paragrafu 63 je zmíněno, že dohoda obsahuje jistou záruku, kdy Spojené království ani EU nebudou diskriminovat elektronické podpisy nebo elektronické dokumenty na základě jejich digitální podoby a také, že smlouvy lze uzavřít i nadále digitálně [35].

Úřad britského komisaře pro informace (ICO) poskytuje pokyny týkající se eIDAS, tedy že vláda začlenila pravidla eIDAS do právních předpisů Spojeného království. Poskytovatelé důvěryhodných služeb působící v Spojeném království budou muset dodržovat pravidla eIDAS podle britských předpisů eIDAS [36]. Respektive převzali eIDAS a upravili si jej, záznam úprav se nachází na stránkách legislation.gov.uk v 2019 No. 89 [37].

Vláda Spojeného království rovněž uvedla, že kvalifikované elektronické podpisy podporované poskytovatelem důvěryhodných služeb EU, budou i nadále uznávány v anglickém právu [38].

5.1.2 Anglické certifikační autority

Mezi certifikační autority patří například:

- **Barclays Bank Plc,**
- **British Relecommunications Plc,**
- **Digidentity BV,**
- **Entrust (Europe) Ltd,**
- **Health & Social Care Information Centre atd.**

Informace jsou na stránkách Evropské komise aktualizovány k 31. 12. 2020. Je otázkou, zda budou na stránkách aktualizovány i do budoucna (například Švýcarsko s Evropskou komisí informace ohledně svých certifikačních autorit nesdílí) [9].

5.2 Spojené státy americké

Elektronické podpisy se mohou použít při obchodování, mohou být předloženy u soudu a obecně mají stejná práva jako podpisy psané vlastní rukou. Elektronickým podpisem se v americkém právu rozumí elektronický zvuk, symbol nebo proces připojený k dokumentu, či jinému záznamu nebo s ním logicky spojený, a tento proces byl provedený osobou s úmyslem podepsat záznam.

5.2.1 Přehled amerických zákonů týkajících se elektronického podpisu

V Americe existují dvě stěžejní právní úpravy, jedná se o ESIGN neboli Electronic Signatures in Global and National Commerce Act, česky zákon o elektronických podpisech v globálním a národním obchodu z roku 2000 a UETA neboli The Uniform Electronic Transactions Act, česky potom zákon o elektronických podpisech v globálním a národním obchodě z roku 1999. Oba zákony se však výhradně vztahují na obchodní transakce. Specifikují také výjimky, kdy se elektronický podpis nemůže použít k podepsání dokumentu (například rozvod, závěť, adopce atd.). Všech padesát států USA přijalo ESIGN, některé státy ovšem nepřijaly UETA. Mezi tyto patří New York, který stále zákon nepřijal, Washington v roce 2020 zákon schválil a Illinois v roce 2021 přistupuje k uzákonění [39].

UETA obsahuje kromě právní úpravy také konkrétní příklady použití elektronických podpisů. Poskytuje státům rámec pro uzákonění státního práva týkajícího se vymahatelnosti elektronického podpisu [40].

ESIGN je federální zákon, platí tedy pro všechny státy USA. Zákon klade určité požadavky na elektronický podpis: obě strany musí souhlasit s elektronickým obchodováním, obě strany musí být uvědomeny, že se podepisují (například pokud na obchodních stránkách stačí odkliknout pole „souhlasím“, tak na udělující souhlas musí být upozorněno), záznam se musí uchovat v okamžiku přijetí a další [41].

V Americe existují dva typy elektronického podpisu:

- **Elektronický podpis** je obyčejný elektronický podpis, který však musí obsahovat zpětně důkaz o tom, že byl podepsán (ověřování přes e-mail, heslo, nebo pin).
- **Digitální podpis** používá digitální certifikát od poskytovatele důvěryhodných služeb, například certifikát od certifikační autority a musí být připojen k dokumentu kryptografickými metodami [42].

5.2.2 Americké certifikační autority

Následující certifikační autority jsou soukromými subjekty a na svých stránkách mají potvrzeno, že jejich podpis je v souladu s ESIGN a UETA: **PandaDoc, Signaturely, SignRequest, DocuSign, Docsketch atd.**

5.3 Čínská lidová republika

Elektronickým podpisem se rozumí údaje v elektronické podobě obsažené a připojené k datům, jež mají být použity k identifikaci podepisujícího.

5.3.1 Přehled čínských zákonů týkajících se elektronického podpisu

Čínský zákon zabývající se elektronickým podpisem je Electronic Signature Law of the People's Republic of China, zákon Čínské lidové republiky o elektronickém podpisu z roku 2004. Zákon je pro lepší srozumitelnost přeložen do angličtiny [43].

Pokud se strany dohodnou na použití elektronického podpisu, takovému dokumentu nemohou být upřena žádná práva. Elektronický podpis se nemůže použít v případech: osobních vztahů (manželství, dědictví), převodu práv, ukončení veřejných služeb a další okolnosti, pokud tak stanoví zákon.

Čínský zákon nepoužívá stejně jako eIDAS typy elektronického podpisu, mluví se pouze o elektronickém podpisu a o spolehlivém elektronickém podpisu, který má stejnou právní váhu jako ručně psaný podpis. Spolehlivý elektronický podpis musí splňovat tyto náležitosti:

- Data, která jsou použita pro vytvoření elektronického podpisu, jsou vlastněna pouze podpisovatelem.
- Data, která tvoří podpis, jsou kontrolována pouze podepisovatelem v době, kdy je podpis vytvářen.
- Jsou patrné jakékoliv změny obsahu provedené na elektronickém podpisu nebo v podepsaném dokumentu [44].

Při soudním jednání bude komplexně zkoumáno, zda elektronický podpis splňoval zmíněné náležitosti. Elektronický podpis opatřený certifikátem od certifikační autority se považuje za evidentní důkaz, že je elektronický podpis autentický a platný.

5.3.2 Čínské certifikační autority

Ministerstvo průmyslu a informačních technologií na webových stránkách vede seznam certifikačních autorit, jež splňují požadavky stanovené zákonem. V seznamu pro rok 2021 je zapsáno šest firem [45]:

- **Beijing Digital Certification** s platnou licencí od října 2020 do října 2025;
- **Hubei Province Digital Certification Management Center** má platnou licenci od listopad 2020 do listopadu 2025;
- **Yixin Technology** s platnou licencí od listopad 2020 do listopadu 2025;
- **China Railway Xinhongyuan (Peking) Software Technology** má platnou licenci od prosince 2020 do prosince 2025;
- **Zhejiang Digital Security Certificate Management** má platnou licenci od prosince 2020 do prosince 2025;
- **Fujian Digital Security Certificate Management** s licencí od ledna 2021 do ledna 2026.

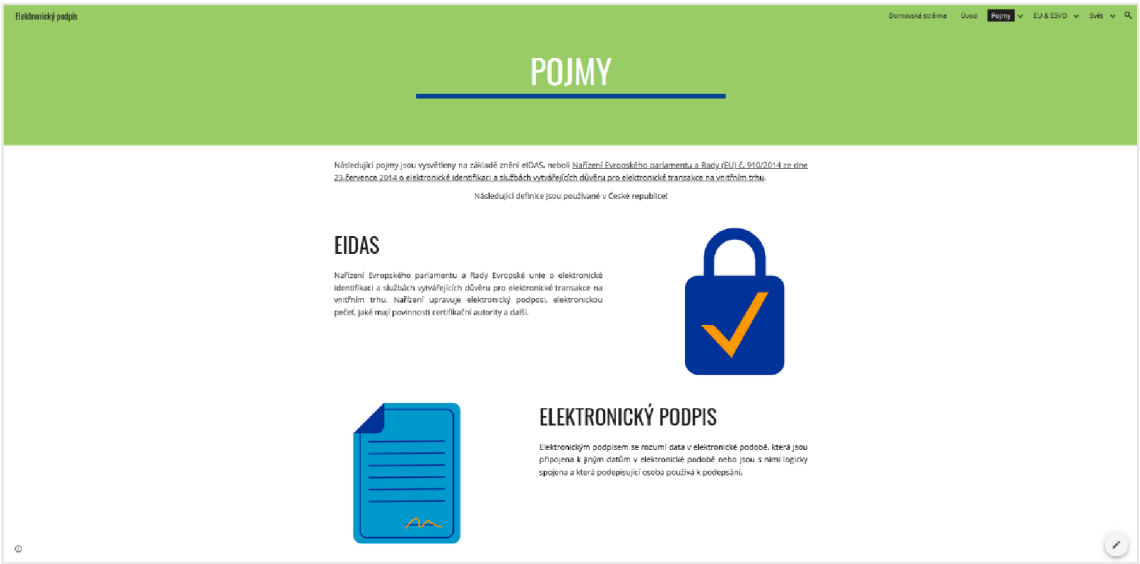
6. WEBOVÁ APLIKACE

Na základě získaných informací byla vytvořena výuková aplikace v podobě webové stránky za pomoci nástroje Google Sites. Webová stránka slouží k vysvětlení problematiky elektronického podpisu, k objasnění základních pojmů spojených s elektronickým podpisem a ke shrnutí informací získaných k vybraným státům.

Stránka má následující strukturu:

- **Domovská stránka** – obsahuje mapu EU a na ní vyznačené zpracované státy, následují odstavce odkazující na čtyři hlavní části webové stránky (úvod, pojmy, EU & ESVO a Svět) spolu s charakteristikou, co se na stránkách nachází.
- **Úvod** – seznámení s bakalářskou prací a webovou stránkou.
- **Pojmy** – stránka objasňuje základní pojmy, které se vážou k elektronickému podpisu. Součástí jsou tři podstránky, dvě blíže objasňující problematiku a jedna obsahuje krátký kvíz:
  - **Typy elektronického podpisu**,
  - **Technické standardy**,
  - **Kvíz** – vytvořený za pomoci nástroje Google Forms.
- **EU & ESVO –** nachází se zde seznamy zpracovaných států z EU a ESVO s odkazy na podstránky, které obsahují získané informace k vybraným státům.
- **Svět** – obsahuje seznam tří vybraných států s odkazy na podstránky, které obsahují získané informace k vybraným státům.

Odkaz na stránku: https://sites.google.com/view/elektronicky-podpis.



Obrázek 2: Ukázka z webové aplikace

ZÁVĚR

Cílem bakalářské práce bylo zmapovat současný stav využívání elektronického podpisu a elektronické komunikace ve veřejné správě států Evropské unie. Bohužel, nalezené studie a statistiky o využívání elektronického podpisu ve státech EU jsou staré přibližně deset let, v dnešní době jsou již zastaralé, a tudíž nejsou součástí bakalářské práce. Proto je zde pojednáváno o právní úpravě ve státech, které měly právo přeloženo do anglického jazyka, nebo jejichž jazyk byl dostatečně srozumitelný k získání informací. Překlady jednotlivých práv slouží k přiblížení situace, jakým způsobem s elektronickým podpisem daný stát nakládá, nejedná se tedy o oficiální překlad znění zákona. Informace získané pro vypracování bakalářské práce jsou shrnuty prostřednictvím webové stránky.

První a druhá kapitola blíže objasňuje pojem elektronický podpis, pojmy spojené s elektronickým podpisem, základní technické prostředky a další stěžejní informace související s řešenou problematikou.

Následující kapitoly práce se věnují jednotlivým státům v tomto pořadí:

- Třetí kapitola se věnuje elektronickému podpisu ve státech Evropské unie. Státy EU se řídí podle nařízení eIDAS a jednotlivé implementace tohoto nařízení se ve státech liší minimálně.
- Čtvrtá kapitola se zabývá elektronickým podpisem ve státech ESVO (Státy patřící do Evropského sdružení volného obchodu). Jedná se o: Norsko, Island, Lichtenštejnsko a Švýcarsko.
- Pátá kapitola obsahuje tři vybrané státy ze světa. Konkrétně byly vybrány pro porovnání Spojené království, USA a Čína.

Šestá kapitola se věnuje zpracování výukové webové stránky, která shrnuje získané informace o elektronickém podpisu a vybraných státech.

Příloha B obsahuje tabulku souhrnných informací o situaci v jednotlivých státech v souvislosti se zkoumaným problémem. Byly porovnávány informace, zda stát uznává a aplikuje eIDAS, který zákon v daném státě pojednává o elektronickém podpisu, kontrolní orgán (váže se jen ke státům aplikujícím eIDAS) a dále jsou uvedeny maximálně čtyři zástupné certifikační autority.

LITERATURA

[1] EVROPSKÝ PARLAMENT A RADA (EU). *Nařízení o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES* [online]. 2014 [cit. 2020-12-10]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910

[2] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009 [cit. 2020-12-10]. ISBN 978-80-251-2619-6.

[3] PRVNÍ CERTIFIKAČNÍ AUTORITA. *Získat elektronický podpis.* I.CA [online]. Podvinný mlýn 2178/6 190 00 Praha 9 [cit. 2020-12-11]. Dostupné z: https://www.ica.cz/certifikaty

[4] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Electronic Signatures and Infrastructures Activities* [online]. 2020 [cit. 2021-5-28]. Dostupné z: https://portal.etsi.org/TB-SiteMap/esi/esi-activities

[5] CEF DIGITAL. *ESignature standards* [online]. 2019 [cit. 2021-5-28]. Dostupné z: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+standards

[6] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Electronic Signature Formats* [online]. 2003 [cit. 2021-5-27]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.05.01_60/ts_101733v010501p.pdf

[7] ETSI TS 119 612 V2.1.1. *Electronic Signatures and Infrastructures (ESI);Trusted Lists* [online]. 2015 [cit. 2020-12-11]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.01.01_60/ts_119612v020101p.pdf

[8] BARKER, E, M SMID a D BRANSTAD. *A Profile for U.S Federal Cryptographic Key Management Systems* [online]. 2015 [cit. 2021-5-10]. ISBN NIST Special Publication 800-152. Dostupné z: http://dx.doi.org/10.6028/NIST.SP.800-152

[9] EVROPSKÁ KOMISE. *CEF Digital Connecting Europe: Trusted List Browser* [online]. Evropská unie, 1995 [cit. 2020-11-31]. Dostupné z: https://webgate.ec.europa.eu/tl-browser/#/

[10] *Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce* [online]. 2016 [cit. 2020-12-10]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297

[11] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. [4] *Seznam vydávaných kvalifikovaných prostředků pro vytváření elektronických podpisů v České republice.* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.mvcr.cz/clanek/seznam-vydavanych-kvalifikovanych-prostredku-pro-vytvareni-elektronickych-podpisu-v-ceske-republice.aspx

[12] Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) [online]. 2016 [cit. 2020-12-10]. Dostupné z: https://www.zakonypreludi.sk/zz/2016-272

[13] MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY. *Kvalifikovaný elektronický podpis.* [online]. 2020 [cit. 2020-11-25]. Dostupné z: https://www.minv.sk/?kvalifikovany-elektronicky-podpis-ode

[14] BUNDESMINISTERIUM DER JUSTIZ UND FUR VERBRAUCHERSCHUTZ. *Vertrauensdienstegesetz (VDG)* [online]. 2017 [cit. 2020-12-10]. Dostupné z: https://www.gesetze-im-internet.de/vdg/BJNR274510017.html

[15] ADOBE. *Electronic Signature Laws & Regulations – Germany*. [online]. Slovensko, c2020 [cit. 2020-11-28]. Dostupné z: https://helpx.adobe.com/sign/using/legality-germany.html

[16] RECHTSINFORMATIONSSYSTEM DES BUNDES. Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG) [online]. 2016 [cit. 2020-12-10]. Dostupné z: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585

[17] *Ustawa o usługach zaufania oraz identyfikacji elektronicznej* [online]. 2016 [cit. 2020-12-10]. Dostupné z: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160001579/T/D20161579L.pdf

[18] LE PREMIER MINISTRE, SUR LE RAPPORT DE LA GARDE DES SCEAUX, MINISTRE DE LA JUSTICE. *Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique* [online]. 2017 [cit. 2021-5-10]. Dostupné z: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035676246?r=ArrkhSPlby

[19] *Code Civil: Article 1367* [online]. [cit. 2021-5-10]. Dostupné z: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032042456/

[20] L'AUTORITÉ DE RÉGULATION DES COMMUNICATIONS ÉLECTRONIQUES ET DES POSTES. *Avis n° 2017-0462 du 18 avril 2017 sur un projet de décret relatif au service de recommandé électronique* [online]. 2017 [cit. 2021-5-10]. Dostupné z: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036897521?init=true&page=1&query=%C3%A9lectroniques+eidas&searchField=ALL&tab_selection=all

[21] JEFATURA DEL ESTADO. *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza* [online]. 2020 [cit. 2021-5-10]. Dostupné z: https://www.boe.es/eli/es/l/2020/11/11/6/con

[22] AGENZIA PER L'ITALIA DIGITALE. *Firma elettronica qualificata* [online]. 2021 [cit. 2021-5-12]. Dostupné z: https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata

[23] AGENZIA PER L'ITALIA DIGITALE. *La diffusione dei servizi fiduciari qualificati* [online]. 2020 [cit. 2021-5-12]. Dostupné z: https://eidas.agid.gov.it/Statistiche/Diffusione.pdf

[24] MINISTRY OF TRANSPORT AND COMMUNICATIONS. *Act on Strong Electronic Identification and Electronic Trust Services* [online]. 2019 [cit. 2021-5-12]. Dostupné z: https://finlex.fi/en/laki/kaannokset/2009/en20090617.pdf

[25] *Viestintä: Määräys sähköisistä tunnistus- ja luottamuspalveluista (Viestintävirasto 72 A/2018 M)* [online]. 2018 [cit. 2021-5-12]. Dostupné z: https://www.finlex.fi/fi/viranomaiset/normi/480001/42947

[26] TRAFICOM. *Electronic identification* [online]. 2021 [cit. 2021-5-13]. Dostupné z: https://bit.ly/3fE1GfB

[27] *Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista* [online]. 2009 [cit. 2021-5-13]. Dostupné z: https://www.finlex.fi/fi/laki/ajantasa/2009/20090617#L1

[28] INFRASTRUKTURDEPARTEMENTET RSED DF. *Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning* [online]. 2018 [cit. 2021-5-13]. Dostupné z: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20181486-med-instruktion-for_sfs-2018-1486

[29] KOMMUNAL- OG MODERNISERINGSDEPARTEMENTET. Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester) [online]. 2018 [cit. 2021-5-13]. Dostupné z: https://lovdata.no/dokument/NL/lov/2018-06-15-44?q=lov

[30] NKOM. *Om regelverket - eIDAS-forordningen* [online]. 2020 [cit. 2021-5-13]. Dostupné z: https://www.nkom.no/internett/elektronisk-id-og-tillitstjenester/eidas-forordningen

[31] *Gesetz vom 27. Februar 2019 über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz; SigVG)* [online]. 2019 [cit. 2021-5-17]. Dostupné z: https://www.gesetze.li/konso/2019114000

[32] DIE BUNDESVERSAMMLUNG DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT. *Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate* [online]. 2016 [cit. 2021-5-18]. Dostupné z: https://www.fedlex.admin.ch/eli/cc/2016/752/de

[33] ADOBE. *Electronic Signature Laws & Regulations - Switzerland* [online]. 2020 [cit. 2021-5-18]. Dostupné z: https://helpx.adobe.com/sign/using/legality-switzerland.html

[34] KLUKOVÁ, A. a T. VLASÁK. *Brexit – Zákon o vystoupení z Evropské unie 2018* [online]. 2019 [cit. 2021-5-20]. Dostupné z: https://www.epravo.cz/top/clanky/brexit-zakon-o-vystoupeni-z-evropske-unie-2018-110075.html

[35] *UK-EU TRADE AND COOPERATION AGREEMENT: Summary* [online]. 2020 [cit. 2021-5-20]. Dostupné z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/962125/TCA_SUMMARY_PDF_V1-.pdf

[36] REILLY, S. *EIDAS Regulation: Brexit and the electronic trust services providers law* [online]. 2021 [cit. 2021-5-20]. Dostupné z: https://docuten.com/en/blog/how-brexit-affects-the-electronic-trust-service-law/

[37] THE SECRETARY OF STATE. *The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019* [online]. 2019 [cit. 2021-5-21]. Dostupné z: https://www.legislation.gov.uk/uksi/2019/89/contents/made

[38] DOCUSIGN. *The impact of Brexit on electronic signatures: Legality of eSignature in a post-Brexit world* [online]. 2021 [cit. 2021-5-21]. Dostupné z: https://www.docusign.co.uk/blog/the-impact-brexit-electronic-signatures

[39] UNIFORM LAW COMMISSION. *Electronic Transactions Act* [online]. 2000 [cit. 2021-5-21]. Dostupné z: https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034

[40] TIBBERTS, M. *The Law of E-Signatures in the United States and Canada* [online]. 2020 [cit. 2021-5-21]. Dostupné z: https://www.bakermckenzie.com/en/insight/publications/2020/03/the-law-esignatures-us-canada

[41] SIGNEASY, M. *The UETA and the ESIGN Act* [online]. [cit. 2021-5-21]. Dostupné z: https://signeasy.com/resources/esign-act

[42] ADOBE SIGN. *U.S. Guide to Electronic Signatures* [online]. [cit. 2021-5-21]. Dostupné z: https://www.adobe.com/content/dam/dx-dc/pdf/ue/adobe-sign-us-guide-e-signatures-wp-ue.pdf

[43] *Electronic Signature Law of the People's Republic of China* [online]. 2004 [cit. 2021-5-23]. Dostupné z: https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn105en.pdf

[44] ADOBE SIGN. *Electronic Signature Laws & Regulations - China* [online]. [cit. 2021-5-23]. Dostupné z: https://helpx.adobe.com/sign/using/legality-china.html

[45] 工业和信息化部. *工业和信息化部关于公布2021年换发电子认证服务许可证企业名单（第一批）的通告* [online]. 2021 [cit. 2021-5-23]. Dostupné z: https://www.miit.gov.cn/zwgk/zcwj/wjfb/tg/art/2021/art_a5c322f87dc6467d92f847aeb0400c62.html

SEZNAM SYMBOLŮ A ZKRATEK

Zkratky:

eIDAS	Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
EU	Evropská unie
ESI	Elektronické podpisy a infrastruktury
ETSI	Evropský ústav pro telekomunikační normy
IETF	Komise pro technickou stránku internetu
NASES	Národná agentúra pre sieťové a elektronické služby
VDG	Německý zákon o důvěryhodných službách
GmbH	Společnost s ručením omezením (německy)
ESVO	Evropské sdružení volného obchodu (anglicky EFTA)
EHP	Evropský hospodářský prostor
Nkom	Norský komunikační úřad
ZertES	Federální zákon o certifikačních službách v oblasti elektronického podpisu a další aplikace digitálních certifikátů (švýcarský zákon)
TCA	Dohoda o obchodu a spolupráci (anglická smlouva s EU)
ICO	Úřad britského komisaře
UEATA	Zákon o elektronických podpisech v globálním a národním obchodě (americký zákon)
ESIGN	Zákon o elektronických podpisech v globálním a národním obchodu (americký zákon)

Zkratky v certifikátu ke kvalifikovanému elektronickému podpisu:

C	stát, resp. jeho mezinárodní poznávací značka (CZ)
CN	název, u fyzické osoby jméno a příjmení, u právní osoby název objektu
O	název firmy (První certifikační autorita, a.s.)
ST	kraj (Zlínský)
L	místo (Zlín, tř. Tomáše Bati 21, 76001)
GN	jméno (Marie)
SN	příjmení (Novotná)
SP	provincie
OU	oddělení nebo organizační jednotka
T	pozice v zaměstnání
P	pseudonym
E	adresa elektronické pošty

SEZNAM PŘÍLOH

Příloha A - Ukázka certifikátu

Certifikát slouží pouze jako ukázka, hodnoty jsou pozměněné od původního kvalifikovaného elektronického podpisu získaného z veřejně dostupného archivu První certifikační autority.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11807434 (0xb42aca)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CZ, CN=I.CA Qualified 2 CA/RSA 02/2016, O=První
certifikační autorita, a.s., serialNumber=NTRCZ-007
        Validity
            Not Before: Apr  1 04:13:23 2021 GMT
            Not After : Apr  1 04:13:23 2022 GMT
        Subject: CN=JMÉNO SUBJEKTU, GN=JMÉNO, SN=PŘÍJMENÍ, C=CZ,
O=FIRMA,         OU=ODDĚLENÍ,         organizationIdentifier=NTRCZ-007,
serialNumber=ICA - 10538512
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:dc:03:1d:28:5b:ae:eb:38:cd:1f:de:ea:21:
                    d7:46:dc:0e:f9:1d:0c:db:4f:86:4b:6f:23:3b:a1:
                    bb:27:00:76:7b:94:87:de:20:46:6c:d4:31:2c:fc:
                    e5:16:b3:3a:e8:6e:a4:2a:d5:e0:d1:28:26:0c:43:
                    5d:69:00:7c:ab:c3:83:65:41:a6:aa:d7:44:50:3a:
                    eb:81:28:df:d2:38:3d:d4:73:87:0d:6a:06:18:6e:
                    18:d4:32:e7:99:4f:2e:ac:7f:11:e7:14:87:3f:38:
                    15:a5:cb:00:dd:84:6a:86:8c:f4:49:47:c0:0f:f0:
                    97:27:ba:fb:29:4c:c7:73:37:ac:f3:4a:8d:f8:3b:
                    17:b9:6c:b7:cd:bc:ae:fe:8c:a4:83:af:2a:df:10:
                    9d:6f:fd:32:14:d6:47:51:2a:54:3c:fa:03:80:41:
                    d8:6f:94:ba:fe:76:59:68:67:f3:4c:e2:14:e9:13:
                    59:00:5d:dd:78:9a:c4:71:f8:cb:0f:f9:fd:30:9e:
                    c5:ff:9d:55:64:3c:c5:ac:0c:56:ad:11:ec:56:ac:
                    de:56:09:9d:31:b0:21:2f:9d:14:2c:55:41:41:17:
                    9e:55
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            I.CA Certificates Interconnection:
                ID: 5708610795806 (master)
                CertCount: 2
            I.CA Twin ID:
                5708610795806
            X509v3 Subject Alternative Name:
                email:EMAIL@EMAIL.cz
                othername:I.CA User ID:10538512
                othername:MPSV IK:1495459790

            Netscape Comment:
                9203050100061981
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
            X509v3 Basic Constraints:
                CA:FALSE
```

```
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.23624.10.1.30.1.1
                  CPS: http://www.ica.cz
                  User Notice:
                    Explicit Text: Tento kvalifikovany certifikat pro
elektronicky  podpis  byl  vydan  v  souladu  s  narizenim  EU  c.
910/2014.This  is  a  qualified  certificate  for  electronic  signature
according to Regulation (EU) No 910/2014.
                Policy: 0.4.0.194112.1.2

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://qcrldp1.ica.cz/2qca16_rsa.crl

                Full Name:
                  URI:http://qcrldp2.ica.cz/2qca16_rsa.crl

                Full Name:
                  URI:http://qcrldp3.ica.cz/2qca16_rsa.crl

            qcStatements:
                id-etsi-qcs-QcCompliance
                id-etsi-qcs-QcSSCD
                id-etsi-qcs-QcPDS
                  cs: https://www.ica.cz/Zpravy-pro-uzivatele
                  en: https://www.ica.cz/PDS
                id-etsi-qcs-QcType
                  id-etsi-qct-esign
            Authority Information Access:
                CA Issuers - URI:http://q.ica.cz/2qca16_rsa.cer
                OCSP - URI:http://ocsp.ica.cz/2qca16_rsa

            X509v3 Authority Key Identifier:

keyid:74:82:08:91:E3:D9:64:68:71:85:D6:EB:31:E4:72:DF:8B:26:B1:6D

            X509v3 Subject Key Identifier:

8A:57:18:CC:F3:B9:7A:BE:2D:88:C4:20:FB:1F:3F:16:41:30:B3:6A
            X509v3 Extended Key Usage:
                E-mail Protection
    Signature Algorithm: sha256WithRSAEncryption
         58:67:14:77:b2:bb:bf:24:68:6e:39:de:7b:10:5f:15:66:ea:
         53:dd:6e:53:32:fe:c2:95:ab:5b:ed:f7:5a:45:5c:0e:8e:d1:
         dc:b1:34:90:5d:a7:d7:40:4f:4d:a3:1a:df:7c:c9:24:44:de:
         c0:88:d4:4c:d1:61:ff:27:f7:19:04:9c:56:db:4e:8d:48:af:
         fa:d3:90:90:c0:9b:f8:c1:d2:f8:34:99:bb:59:21:49:86:2e:
         6c:fc:7b:d9:f4:59:2f:b4:61:ee:e1:22:64:65:cf:dc:e1:9b:
         13:2a:d4:b2:83:b1:69:df:53:98:96:a4:f2:eb:f0:b7:42:ed:
         b4:98:70:45:b3:5d:e3:7e:a6:a1:a8:f6:ca:f9:d7:5b:b0:46:
         51:2b:22:60:2d:0e:8d:2f:a5:3a:7f:48:80:c8:66:0e:a6:4a:
         d0:21:e9:c3:44:bc:cb:ab:85:07:e0:39:6d:3c:f6:c4:c1:22:
         55:be:a0:0a:ce:c3:89:f5:ec:c5:13:8e:8c:2a:74:76:7a:8b:
         17:5b:38:07:6a:a7:6f:a6:f6:4b:0a:12:3e:c5:e9:aa:88:b4:
         dd:6f:88:c3:67:29:57:8b:cc:19:fa:77:2e:46:91:61:fd:e9:
         08:47:07:d1:9c:16:87:72:2a:95:12:02:c5:7c:ed:d6:fc:58:
         0d:cd:1d:ad:0e:2f:1d:8e:f9:99:2a:4b:7e:6c:4e:00:cc:99:
         98:92:b7:22:fb:00:78:d3
```

Příloha B - Souhrn získaných informací

Tabulka 3: Souhrn získaných informací

	Polsko	Rakousko	Německo	Slovensko	Česko
eIDAS	ANO	ANO	ANO	ANO	ANO
Zákon	Zákon o usługach zaufania oraz identyfikacji elektronicznej	Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen	Vertrauensdienstegesetz	Zákon 272/2016 Sb. o důvěryhodných službách pro elektronické transakce na vnitřním trhu a o změně a doplnění některých zákonů	Vyhláška č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce
Kontrolní orgán	Narodowe Centrum Certyfikacji	Rundfunk und Telekom Regulierungs-GmbH	Bundensnetzagentur	Národní bezpečnostní úřad	Ministerstvo vnitra
Certifikační autority	Asseco Data Systems S.A. Krajowa Izba Rozliczeniowa S.A. EiroCerst Sp. z o.o. Polish Security Printing Works	Rundfunk und Telekom Regulierungs-GmbH PrimeSign GmbH A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH Swisscom IT Services	Bank-Verlag GmbH Deutsche Post AG Bundesagentur fuer Arbeit D-Trust GmbH	Prvá certifikačná autorita a. s. Ministerstvo Obrany Slovenskej republiky NASES Národný bepečnostný úrad	První certifikační autorita, a. s. Česká pošta, s. p. Eldentity a. s. Správa základních registrů (2019)

	Švédsko	Finsko	Itálie	Španělsko	Francie
eIDAS	ANO	ANO	ANO	ANO	ANO
Zákon	Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista Viestintä: Määräys sähköisistä tunnistus- ja uottamuspalveluista, Viestintävirasto 72 A/2018 M	Codice dell' amministrazione digitale Decreto Legislativo 7 marzo 2005, n. 82	Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique Avis n° 2017-0462 du 18 avril 2017 sur un projet de décret relatif au service de recommandé électronique
Kontrolní orgán	Post- och telestyrelsen	Liikenne- ja viestintävirasto Traficom	Agenzia per l'Italia Digitale	Ministerio de Asuntos Económicos y Transformación Digital	Agence Nationale de la Sécurité des Systèmes d'Information
Certifikační autority	TrustWeaver AB ZealiD AB	Digital and Population Data Services Agency	Ministero della Difesa Namirial S.p.A. Consiglio Nazionale del Notariato Azienda Zero	Anf Autoridad de Certificación Asociación Anf AC Consejo General de la Abogacía Española Ministerio de Empleo y Seguridad Social Logalty Prueba por Interposición, S.L.	Gendarmerie Nationale Docusign France Agence Nationale des Titres Sécurisés Cryptolog International

	Spojené království	Švýcarsko	Lichtenštejnsko	Island	Norsko
eIDAS	NE	NE	ANO	ANO	ANO
Zákon	(EU-UK Trade and Cooperation Agreement)	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate	Gesetz vom 27. Februar 2019 über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen	-	Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)
Kontrolní orgán	-	-	Amt für Kommunikation	-	Nasjonal kommunikasjonsmyndighet
Certifikační autority	Barclays Bank Plc British Relecommunications Plc Digidentity BV Entrust (Europe) Ltd	Swisscom (Schweiz) AG QuoVadis Trustlink Schweiz AG SwissSign AG Federal Office of Information Technology, Systems and elecommunication	FLZ-Anstalt Office for Communications	Audkenni ehf.	Bankenes ID-tjeneste AS Danske Bank Nordea Bank Abp filial i Norge Commfides Norge AS

	Čína	Amerika
eIDAS	NE	NE
Zákon	Electronic Signature Law of the People’s Republic of China	The Uniform Electronic Transactions Act Electronic Signatures in Global and National Commerce Act
Kontrolní orgán	-	-
Certifikační autority	Beijing Digital Certification Yixin Technology China Railway Xinhongyuan (Peking) Software Technology Fujian Digital Security Certificate Management	PandaDoc Signaturely SignRequest DocuSign