VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

ELEKTRONICKÉ PODEPISOVÁNÍ VE VEŘEJNÉ SPRÁVĚ V SOUVISLOSTI S NAŘÍZENÍM EIDAS

Autor práce: Aleš Mistaler
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Katedra právních oborů a bezpečnostních studií

2020

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Aleš Mistaler

Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Elektronické podepisování ve veřejné správě v souvislosti s nařízením eIDAS

Název bakalářské práce v anglickém jazyce: Electronic Signature in Public Administration in Accordance with eIDAS Order

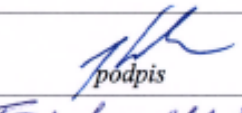
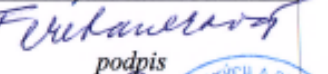
Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): 03/2019

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je porovnat stav elektronického podepisování ve veřejné právě před účinností unijního nařízení Evropského parlamentu a rady EU č. 910/2014 (eIDAS) a stav po ukončení dvouleté výjimky v oblasti elektronického podepisování tedy po 19. 9. 2018.

Student: Aleš Mistaler	16.3.2019 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	19.3.2019 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	22.3. 2019 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	27.3.19 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	1.4.2019 *datum*	 *podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MISTALER, A. *Elektronické podepisování ve veřejné správě v souvislosti s nařízením eIDAS : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2019. 63 s. Vedoucí bakalářské práce : RNDr. Růžena Ferebauerová

Klíčová slova: eGovernment, elektronický dokument, elektronický podpis, certifikát, kvalifikovaný prostředek, nařízení eIDAS.

Tato bakalářská práce pojednává o vývoji veřejné správy zejména v oblasti elektronického podepisování a porovnává stav před a po nabytí platnosti nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014.

Teoretická část je zaměřena na vývoj eGovernmentu a legislativu vztahující se k danému tématu. Další část objasňuje základní pojmy a prostředky potřebné k podepisování.

V praktické části je řešen postup práce s certifikáty, a to jejich obnova, záloha a generování žádosti o certifikát. V závěru práce jsou zhodnocena pozitiva i negativa spojená s účinkem tohoto nařízení.

ABSTRACT

MISTALER, A. *Electronic Signature in Public Administration in Accordance with eIDAS Order : Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2019. 63 p. Supervisor : RNDr. Růžena Ferebauerová

Key words: eGovernment, electronic document, electronic signature, certificate, qualified means, regulation eIDAS.

The bachelor thesis deals with development of public administration especially in the field of electronic signature and compares the state before and after entry info force of the European parliament and Council regulation number 910/2014 dated 23 July 2014.

The theoretical part is focused on the development of eGovernment and legislation connected with this topic. The next part explains the basic terms and means necessary for signing.

The practical part deals with the procedure of work with certificates, their renewal, backup and certificate request generating. In the end of the thesis the positive and negative sides connected with the effect of this regulation are evaluated.

Obsah

Úvod

V bakalářské práci se autor zabývá tématem elektronického podpisování ve veřejné správě, s tím související platnou legislativou a technickými prostředky, které jsou v současnosti platné.

Žijeme v době, která je zahlcena informacemi a různými druhy hybridních dokumentů papírovými a digitálními. Převod dokumentů do digitální podoby není v dnešní době problém, ale plná digitalizace bude podle odborníků ještě několik let trvat. Elektronické podepisování realizuje zabezpečení dokumentu konkrétní osobou, která dokument podepsala v daném reálném čase spolu s požadavkem na právní váhu a v souladu s technickými prostředky pro řešení.

Autor práce má 22 letou praxi ve státní správě, kde si prošel za tu dobu několik stádií vývoje státní správy – odbor informatiky, oddělení spisové služby, oddělení IT a správy dat, oddělení informatiky. V práci mapuje praktické postupy vycházející z jeho dlouholeté praxe - dřívější a taktéž současné aplikované postupy pro elektronizaci státní správy (technicky i legislativně), které posunují její vývoj ke zpřehlednění a zjednodušení nejen pro pracovníky státní správy, ale i pro jednotlivé osoby, firmy nebo instituce, které služeb státní správy využívají. Zákonnou moc v ČR reprezentuje volený Parlament, je nejvyšším zastupitelským orgánem státu. Vláda ČR představuje nejvyšší orgán výkonné moci, z toho vyplývá, že vláda řídí a kontroluje státní administrativní aparát.[1] Elektronické podepisování rovněž patří mezi administrativu řízenou a vykonávanou státem.

[1] BÍLÝ, J. *Základy společenských věd IV*. Ostrava : Key Publishing, 2009. s. 104-105

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je porovnat stav ve veřejné správě před účinností unijního nařízení Evropského parlamentu a rady EU č. 910/2014 (eIDAS) ze dne 23. července 2014 a stav po ukončení dvouleté výjimky v oblasti elektronického podepisování, daný účinností unijního nařízení od 19.09.2018.

Tato bakalářská práce má dvě části teoretickou a praktickou a obsahuje celkem čtyři základní kapitoly.

V první kapitole autor poukazuje na pojem eGovernmentu a zmíní jeho vývoj až po současnost, neboť dle jeho názoru je nezbytný k tomu, aby byla lépe pochopena nejen problematika týkající se elektronického podepisování ve veřejné správě, ale aby se také poukázalo na komunikační infrastrukturu veřejné správy v České republice, bez které by to nefungovalo a také zde zmíní přínos z jeho dosavadní praxe.

V druhé kapitole se autor zaměří na legislativu vztahující se k danému tématu, která byla platná před výše zmíněným unijním nařízením a jeho následnému začlenění do českého právního řádu. Také bude zmíněna legislativa příbuzná či navazující na tuto oblast.

Ve třetí kapitole autor vymezí základní pojmy související s elektronickým podepisováním zejména elektronický podpis, certifikát, certifikační autorita, kvalifikovaný prostředek, biometrický podpis apod.

Čtvrtá část je praktická bude zde popsáno a ukázáno, jak se generovala žádost o certifikát před unijním nařízením, jaké byly technické prostředky pro uložení certifikátu, jak se prováděla obnova certifikátu, jak se certifikáty zneplatňovaly, jak se připravovaly tokeny pro nové zaměstnance. Dále bude popsáno, jak se musel obnovit platný certifikát do 19.09.2018. Jak se po nabytí účinnosti unijního nařízení musí nakonfigurovat nový kvalifikační prostředek, jak se generuje žádost o certifikát. Jak se zneplatňuje certifikát na novém kvalifikovaném prostředku.

V závěrečné části bude uvedeno, co všechno se muselo zjistit a udělat před účinností unijního nařízení od 19.09.2018. Dále budou zmíněny poznatky z praxe. Pozitivní a negativní dopady tohoto unijního nařízení.

2 Vývoj eGovernmentu

Pojem eGovernment můžeme definovat několika způsoby, můžeme jej definovat takto: eGovernment představuje elektronickou komunikaci za pomoci technických a programových prostředků včetně současného připojení k internetu mezi státními organizacemi, mezi občanem nebo podnikateli a orgány moci veřejné navzájem. Tyto činnosti mají legislativní podporu a odpovědného garanta, v současné době je garantem Ministerstvo vnitra. Cílem eGovernmentu je co nejméně zatěžovat občany nebo podnikatele pro jednodušší a účelnější komunikaci s úřady, což se dnes již stává realitou. Dalšími přínosy eGovernmentu je modernizace veřejné správy, rychlá a zároveň jednoduchá komunikace, která je efektivní, spolehlivá a transparentní, nicméně další nespornou výhodou je úspora finančních prostředků, času pro řešení konkrétní žádosti nebo požadavku občana nebo podnikatele a současně je zapotřebí méně prostor a zaměstnanců pro výkon státní správy. Pojem eGovernment je součástí jazyka moderní informační společnosti a dalo by se říci, že pro něj není překlad v žádném světovém jazyce.[2]

2.1 Začátky v České republice

V 90. letech nastala první fáze elektronizace státní správy, kdy bylo potřeba nejdříve zajistit technicky celé úřady na místní, regionální a celostátní úrovni. Většina úřadů měla a má svůj odborný informační systém například na zpracování či evidenci dat, ekonomický informační systém, personální informační systém, později spisovou službu, které byly většinou dodány externími dodavateli a které je potřeba neustále zdokonalovat a upravovat, ať z důvodu technického vývoje nebo po stránce legislativních změn. Spolu s tímto rozvojem nastala nutnost tyto systémy napříč veřejnou správou propojit tak, aby mohly jednotlivé úřady mezi sebou spolu komunikovat. Jednou z hlavních podmínek toho, aby celý informační systém veřejné správy mohl fungovat, je vytvoření právních a samozřejmě také technicko – organizačních předpokladů ke sdílení dat. K tomuto cíli má sloužit vytvoření soustavy registrů veřejné správy, jejichž osou budou tzv. základní registry. Již v polovině 90. let byla zásadní shoda v tom, že mezi ně patří registr obyvatel.[3]

[2] FEREBAUEROVÁ, R., PEKÁREK, O. *Aplikovaná informatika*. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. s. 123
ISBN 978-80-87472-74-3
[3] MATES, P., SMEJKAL, V. *E-government v českém právu.* Praha : Linde, 2006. s. 54

V roce 1996 byl vytvořen samostatný *Úřad pro státní informační systém* (ÚSIS).[4] S cílem koordinovat informační politiku byla v říjnu 1998 jako poradní orgán vlády zřízena *Rada pro státní informační politiku.*[5] V lednu 2003 bylo zřízeno Ministerstvo informatiky, které se primárně zabývalo čtyřmi oblastmi, a to: Informační společnost (resp. Informační a komunikační technologie ICT, telekomunikace, poštovní služby a elektronický podpis.[6] V roce 2007 Ministerstvo informatiky skončilo a jeho agendu si rozdělilo: Ministerstvo průmyslu a obchodu a získalo dohled nad telekomunikacemi a poštovním trhem. Ministerstvo vnitra převzalo agendu v elektronické veřejné správě a stalo se zřizovatelem České pošty, dále také provozovatelem portálu veřejné správy. [7] Tento stav je stále platný i v současné době.

V období působnosti Ministerstva informatiky si autor práce vybavuje jeden z prvních úkolů nově zřízeného ministerstva, pro informatiky veřejné správy, kteří měli zabezpečit, aby u uživatelů PC (úředníků) byla na viditelném místě nejlépe na stole s PC viditelná schránka či kastlík s fakturou o nákupu PC včetně softwarové licence, dále měl být v kastlíku přiložen protokol o stavu veškerého software a hardware, který byl na konkrétním PC nainstalován a předán a příslušným informatikem a uživatelem podepsán.

2.2 Povinné elektronické podatelny

Daleko významnějším úkolem v působnosti Ministerstva informatiky v roce 2004 byla povinnost orgánů veřejné moci formou nařízením vlády zajistit provoz elektronické podatelny.[8] Elektronická podatelna kopíruje pracoviště podatelny fyzické, která je na každém úřadě a tvoří první vstupní komunikační bod pro veřejnost a v té době pracovala pouze analogově (v listinné podobě). Zavedení elektronické podatelny bylo pro občana jedním z prvních přínosů, že nemusel komunikovat s úřadem formou listinných zásilek nebo osobně, ale mohl pohodlně z domova v kterékoliv době komunikovat elektronicky.

[4] ŠPAČEK, D. *EGovernment cíle, trendy a přístupy k jeho hodnocení*. Praha : C.H. Beck, 2012. s. 54
[5] ŠPAČEK, D. *EGovernment cíle, trendy a přístupy k jeho hodnocení*. Praha : C.H. Beck, 2012. s. 55
[6] PETERKA, J. *Jaké bude nové ministerstvo informatiky?* [online]. eArchiv.cz, 2002 [cit. 2019-06-20]. Dostupné z WWW: <http://www.earchiv.cz/b02/b0925001.php3>.
[7] KÁLAL, J. *Ministerstvo informatiky už je minulostí* [online]. Lupa.cz, 2007 1. června [cit. 2019-06-20]. Dostupné z WWW: <https://www.lupa.cz/clanky/ministerstvo-informatiky-uz-je-minulosti/>.
[8] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. ARCHIV. *Informace o zřízení elektronických podatelen u orgánů veřejné moci* [online]. MVČR, © 2019 [cit. 2019-06-20]. Dostupné z WWW: <https://www.mvcr.cz/clanek/informace-o-zrizeni-elektronickych-podatelen-u-organu-verejne-moci.aspx>

Autor práce se podílel při rozhodování na tvaru a podobě adresy elektronické podatelny úřadu, kdy byla zřízena elektronická podatelna ústředního pracoviště a podatelny krajských úřadů. A to ve tvaru epodatelna@doména_úřadu.cz u ústředního pracoviště a epodatelna.kód_kraje@doména_úřadu.cz u krajského pracoviště. O zřízení elektronických adres podatelen bylo informováno příslušné ministerstvo, které je následně zveřejnilo na portálu veřejné správy. Aby tato komunikace byla považována za důvěryhodnou, musela být ze strany orgánu veřejné moci elektronicky podepsána. V praxi to vypadalo tak, že pracovnice podatelny na svém PC měla přidán svůj uživatelský účet a účet elektronické podatelny ve svém mailovém klientu, který spravovala. Příchozí maily na účet elektronické podatelny poté zaevidovala a postoupila dále k vyřízení. U odchozích mailů bylo v aplikaci Microsoft Outlook nastaveno, aby se automaticky připojoval elektronický podpis. Později s příchodem systému elektronické spisové služby, toto řešení bylo převzato a zaimplementováno do jednoho z modulů systému spisové služby a zcela zautomatizováno. Zavedením elektronických podatelen orgánů veřejné moci šlo o jedno z prvních komplexních elektronických podepisování ve veřejné správě.

2.3 Gestor eGovernmentu

Zrušením Ministerstva informatiky se odpovědným resortem v roce 2007 stalo Ministerstvo vnitra ČR, které i v současnosti eGovernment v ČR prezentuje podobou symbolu postaviček eGona (jeho jednotlivých orgánů) a Klaudie.[9] A tím český eGovernment v posledních několika letech posunulo směrem ke své elektronizaci. Aktuálně jsou na webových stránkách Ministerstva vnitra ČR v sekci eGovernment zařazeny tyto projekty: [10]

- „*Základní registry*
- *Czech POINT*
- *Datové schránky*
- *Komunikační infrastruktura veřejné správy a centrální místo služeb KIVS/CMS*

[9] SMEJKAL, V. *Datové schránky v právním řádu ČR: zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, s komentářem*. Praha : ABF, 2009. s. 11
[10] FEREBAUEROVÁ, R., PEKÁREK, O. *Aplikovaná informatika*. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. s. 123

- *Portál veřejné správy*
- *ISVS*
- *Služby vytvářející důvěru a elektronická identifikace*
- *Certifikáty – CSCA, CVCA*
- *Centrální nákup státu softwarových produktů*
- *Rada vlády pro informační společnost – program „Digitální Česko“*
- *Mezinárodní spolupráce*
- *Registr smluv*
- *Mobilní aplikace „Co dělat když…“*
- *Přístupnost internetových stránek a mobilních aplikací*
- *eGovernment cloud“*[11]

Dalo by se říct, že základem a začátkem, jak bylo zmíněno výše, je skutečně postavička eGona a jeho jednotlivé orgány mozek, srdce, prsty a oběhová soustava.

- „*Mozek: Základní registry veřejné správy*
- *Srdce: Zákon o eGovernmentu*
- *Prsty: Czech POINT*
- *Oběhová soustava: KIVS – Komunikační infrastruktura veřejné správy (telekomunikační síť)*“

Tyto základní orgány zabezpečují pro občany neobcházení úřadů, elektronické dokumenty mají stejnou platnost a význam jako papírové a ze spousty kontaktních míst mohou občané jednoduše komunikovat s více úřady a institucemi. [12]

V době, kdy autor práce vykonával funkci administrátora elektronického systému spisové služby, měl za úkol v administraci tohoto systému vizuálně kontrolovat a manuálně čistit adresář subjektů a osob, které se do něj ukládali automaticky činností

[11] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. EGOVERNMENT. *Alternativní navigace* [online]. MVČR, © 2019 [cit. 2019-06-27]. Dostupné z WWW: <https://www.mvcr.cz/egovernment.aspx>
[12] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. PROJEKTY. *eGON* [online]. MVČR, © 2019 [cit. 2019-06-28]. Dostupné z WWW: <https://www.mvcr.cz/clanek/egon-66.aspx>

uživatelů systému. Toto řešení nebylo ideální, protože docházelo ke vzniku mnoha duplicitních záznamů adres právnických, podnikajících a fyzických osob. Řešením a velkou úlevou se stalo právě propojení elektronického systému spisové služby přes API rozhraní se **Správou základních registrů**. Tímto propojením začal systém spisové služby ztotožňovat fyzické osoby dle zadaného data narození a podnikající fyzické osoby dle IČO. Tím bylo zaručeno, že vypravení elektronického dokumentu či písemnosti bude doručeno správnému existujícímu subjektu a zabezpečeno, že nebudou vznikat žádné duplicity.

Další vykonávanou funkcí byl přístup a administrace prostředí CzechPOINT@office, v tomto prostředí autor práce zaváděl a aktualizoval údaje všech pracovišť hlavně kontaktní adresy, adresy elektronických podatelen a ID datových schránek. Další činností bylo zakládání uživatelů (zaměstnanců) a přidělování rolí pro výkon působnosti úřadu. Pro personální oddělení šlo zejména o výpisy z Rejstříku trestů. Pro zaměstnance podatelen a administrativy šlo o konverzi z moci úřední z listinné podoby do elektronické a z elektronické do listinné. U nově založených zaměstnanců a u zaměstnanců, u kterých se po roce obnovovaly certifikáty, jak kvalifikovaný, tak komerční bylo třeba vždy zadat sériová čísla platných certifikátů. Také propojení **CzechPOINT** přes API rozhraní s elektronickým systémem spisové služby, přineslo tu výhodu, že při autorizované konverzi z moci úřední se dokument připojil do spisové služby pod požadované číslo jednací.

Autor práce vychází z praxe a ukazuje, jaké mají hlavní pilíře eGovernmentu význam pro státní správu, služby CzechPOINT, Datových schránek a Správa základních registrů jsou tu s námi již deset let, za tu dobu se osvědčily, fungují, vylepšují se a budou určitě ještě dlouho využívány.

2.4 Současný eGovernment

Základní pilíře eGovermentu jsou zavedeny již několik let, stěžejním bodem je aktuálnost a budoucnost.

2.4.1 Registr smluv

Registr smluv je informační systém, ve kterém mají mimo jiné i všechny státní instituce legislativně nařízenou povinnost zveřejňovat smlouvy nad 50 000,-Kč bez DPH. Povinnost uveřejňovat smlouvy nastala od 01.07.2016, správcem a provozovatelem systému je Ministerstvo vnitra, které také zřídilo datovou schránku pro Registr smluv, identifikátor je whbt3kp.[13]

Dalším praktickým úkolem autora práce bylo vyřešit nákup výplatního stroje k úhradě cen za poštovní služby. Tento proces trval přibližně šest měsíců a zakončen byl právě vložením do **Registru smluv**. Nejprve bylo nutné zpracovat důvody a podklady pro investiční komisi uvnitř úřadu a udělat průzkum trhu. Potřeba obměny nového zařízení bylo zejména z důvodu časté poruchovosti a nákladných oprav, dále staré zařízení mělo připojení k PC pouze přes USB port a kredit do něj musel jezdit dobíjet technik. Naproti tomu nové zařízení mělo rozhraní LAN (síťové), takže umělo komunikovat a dobíjet kredit online. Po odsouhlasení investiční komise bylo potřeba požádat nadřízené ministerstvo o investiční prostředky na realizaci. Průzkum trhu byl jednoduchý, neboť pro toto specializované zařízení byl pro ČR, Slovensko a Maďarsko pouze a výhradně jeden dodavatel. Veškeré potřebné dokumenty k tomuto úkonu byly založeny ve spisu v elektronickém systému spisové služby. Součástí byla i nová dohoda (smlouva) o používání výplatního stroje podepsaná elektronicky statutárním zástupcem organizace a zástupcem protistrany. Dále objednávka stroje a potvrzení objednávky smluvní strany včetně jejího souhlasu se zveřejněním textu této smlouvy v souladu s ustanovením zákona č.106/1999 Sb., o svobodném přístupu k informacím. Zakončení celého procesu je právě vložení do Registru smluv, které bylo opět realizováno přes elektronický systém spisové služby napojený na Registr smluv. Dodavatel systému spisové služby dodal i program (aplikaci) Anonymizer, který převáděl do souboru pdf strojově čitelného formátu s textovou vrstvou. Odkaz do Registru smluv je zde https://smlouvy.gov.cz/smlouva/2420718.

2.4.2 eObčanka

Dalším významným krokem a nakročením k digitalizaci veřejné správy je od 01.07.2018 zavedení občanských průkazů se strojově čitelnými údaji a kontaktním elektronickým čipem. Tento občanský průkaz by měl zefektivnit komunikaci mezi

[13] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Registr smluv* [online]. MVČR, © 2019 [cit. 2019-06-29]. Dostupné z WWW: <https://www.mvcr.cz/clanek/registr-smluv.aspx>

občany a státní správou a usnadnit přístup ke službám veřejné správy přes internet. Všechny nově vydané občanské průkazy samozřejmě mají elektronický čip, který je v defaultním nastavení pro všechny funkce eObčanky neaktivní. V tomto stavu občan s občanským průkazem funguje stejně jako s předešlým, tedy slouží jako základní průkaz totožnosti na území EU. Rozhodnutí o aktivaci elektronických funkcích eObčanky je čistě na občanovi, a to kdykoliv, to samé platí o deaktivaci. Jediné omezení aktivace je věk 15 let. Ztrátou eObčanky může dojít k ohrožení a zneužití identity. V tomto případě je podobný postup jako při ztrátě bankovní platební karty, a to neprodleného nahlášení na Policii ČR a zablokování elektronické funkce dokladu. eObčanka je samozřejmě zajímavější po aktivaci, kdy je možno na čip nahrát autentizační certifikát a certifikát určený pro elektronický podpis. V současné době jdou s novou občankou vyřídit základní služby: výpis z rejstříků trestů, potvrzení o pracovní neschopnosti, potvrzení o bezdlužnosti a eRecept. Výhledově bude možné podávat daňové přiznání, platit poplatky za komunální odpad a volit online. Náklady za vydání eObčanky jsou 200,- Kč, k tomu je zapotřebí čtečka čipové karty také kolem 200,- Kč a dále je třeba mít PC, notebook a internetové připojení.[14]

2.4.3 eGovernment cloud

Již v úvodu práce v podkapitole „2.1 Počátky v České republice“ autor zmiňuje, jaké všechny informační systémy provozuje každý úřad. Ten si dnes zajišťuje vývoj, provoz a bezpečnost vlastními prostředky. Tzn., že každý úřad má svou IT infrastrukturu, hlavně servery a data servery různého stáří, verzí operačního systému a výkonnosti provozované ve svých prostorech. Proto bylo vyzváno k přípravě strategického rámce Národního cloudu Ministerstvo financí a Národní bezpečnostní úřad ve spolupráci s Ministerstvem vnitra vládou ČR, která schválila nové strategické směřování a rozvoj v oblasti ICT služeb ve veřejné správě. Z dlouhodobé praxe a zkušeností v zahraničí i v soukromém sektoru se ukazuje, že model „cloud computingu“ - provoz ve velkých datových centrech, je efektivnější provozně i finančně a splňuje bezpečnostní požadavky. Tímto směrem by se ráda vydala také veřejná správa v České republice, proto je hlavním cílem vytvoření národního eGovernment cloudu. Jedním z přínosů by mohlo být, že v části data center vlastněných státem se budou systémy provozovat sdíleně pro všechny úřady, což je pro chod státu klíčové. Také půjde o velkou změnu v zajištění provozní

[14] REDAKCE, Finance.CZ. *eObčanka aneb má Česko konečně nakročeno do 21. století?* [online]. Mladá fronta a. s., © 2018. 11. července [cit. 2019-06-29]. Dostupné z WWW: <https://www.finance.cz/512161-eobcanka/>

podpory státní administrativy, na druhou stranu by to mohlo z části vyřešit dlouhodobý nedostatek IT odborníků ve veřejné správě.[15]

2.4.4 Rok 2018 - významný milník

Za významný milník českého eGovernmentu lze jednoznačně považovat rok 2018. V tomto roce se nejen slavilo 100. výročí založení Československa, ale i 25. výročí České republiky a s tím se také pojí národní doména. V Československu se používalo **.cs**, které vznikem České republiky bylo postupně nahrazováno **.cz**. V současnosti samozřejmě celá veřejná správa využívá doménu **.cz**. Pojem Digitální Česko byl již v minulosti využíván, nyní je nově schválen vládou ČR formou usnesení č. 629/2018 jako program nikoli jako koncepce s podtitulem „Vládní program digitalizace České republiky 2018+“. Jeho hlavním úkolem je ucelený další rozvoj eGovernmentu. Další významnou událostí tohoto roku bylo to, že byl zaveden Národní bod pro identifikaci a autentizaci (NIA). Díky němu je možné řešit elektronickou identifikaci fyzických osob, tím se českému eGovernmentu otevřela cesta, aby mohla identifikovat klienty svých služeb. V tomto období také začaly být vydávány nové elektronické občanské průkazy s čipem, to autor popisuje v podkapitole „2.4.2 eObčanka“. Po spuštění NIA a vydávání nových elektronických občanských průkazů byl také spuštěn předem avizovaný Portál občana, který tvoří centralizovaný přístup ke všem službám, které v současné době eGovernment nabízí. A také skončila platnost dvouletých výjimek z oblasti elektronického podepisování a pečetění, které je předmětem této bakalářské práce a je známé jako „nařízení eIDAS“.[16]

[15] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. ZPRAVODAJSTVÍ. *První krok k efektivně sdíleným ICT službám státu v eGovernment cloudu* - Ministerstvo vnitra České republiky. [online]. MVČR © 2019 [cit. 2019-08-14]. Dostupné z: <https://www.mvcr.cz/clanek/prvni-krok-k-efektivne-sdilenym-ict-sluzbam-statu-v-egovernment-cloudu.aspx>

[16] PETERKA, J. *Český eGovernment v roce 2018* [online]. eArchiv.cz, 2019 [cit. 2019-08-29]. Dostupné z WWW: <http://www.earchiv.cz/b19/b0102001.php3>

3 Legislativa elektronického podepisování

S rychlým rozvojem informačních technologií jsme dostali možnost přijímat, tvořit, podepisovat, šířit a uchovávat elektronické dokumenty. V určitém období na to bohužel legislativa nebyla připravená a technologii chyběla legislativní podpora. Postupem času legislativa začala brát v potaz elektronickou podobu dokumentů. Jedním z nejdůležitějších úkonů bylo, jak zrovnoprávnit originály elektronických dokumentů s analogovou (papírovou) formou dokumentu. To se podařilo v ČR počínaje rokem 2000 a zákonem o elektronickém podpisu, kdy elektronické dokumenty rovnocenně nahrazují analogovou (papírovou) formu. Díky spojení technologií a legislativy byla zajištěna jejich neomezená čitelnost, neporušitelnost a věrohodnost.[17] V této části kapitoly autor uvede legislativu vztahující se k elektronickému podepisování a jí příbuznou legislativu, tak jak se vyvíjela až po současnou aktuálně platnou.

3.1 Směrnice Evropského parlamentu a Rady

K jednomu z výchozích legislativních opatření vztahující se k elektronickému podepisování patří směrnice 1999/93/ES. Tato směrnice mimo jiné zmiňuje důležitost pro elektronickou komunikaci a obchod vyžadující „elektronické podpisy" a související služby, které umožňují ověřování pravosti dat. V **článku 1** s názvem „Oblast působnosti" se stanovuje účel této směrnice, který má usnadnit používání elektronických podpisů a přispět k jejich právnímu uznání. Stanovit právní rámec pro elektronické podpisy a některé ověřovací služby, aby bylo zajištěno řádné fungování vnitřního trhu. Dále určuje využití elektronických podpisů ve veřejném sektoru uvnitř vnitrostátních správních orgánů. **Článek 2** s názvem „Definice" zavádí pojmy *elektronický podpis*, *zaručený elektronický podpis*, *podepisující osobu*, *data pro vytváření podpisu*, *prostředek pro vytváření podpisu*, *prostředek pro bezpečné vytváření podpisu*, *data pro ověřování podpisu*, *osvědčení*, *kvalifikované osvědčení*, *ověřovatel*, *produkt pro elektronický podpis* a *dobrovolnou akreditaci*. Směrnice se také mimo jiné zabývá přístupem na trh, zásady vnitřního trhu, právními účinky elektronických podpisů, odpovědností, mezinárodními hledisky a ochranou dat. Součástí směrnice jsou celkem čtyři přílohy. Nejdůležitější je

[17] EARCHIVACE.CZ, Elektronická archivace, *Písemný vs. elektronický dokument* [online]. © 2014 eArchivace [cit. 2019-09-27]. Dostupné z WWW: <http://www.earchivace.cz/elektronicka-archivace/pisemny-vs-elektronicky-dokument/>.

z pohledu tématu této práce **příloha III**, kde jsou uvedeny požadavky na prostředky pro bezpečné vytváření elektronických podpisů. Mimo jiné zdůrazňují i to, že technické prostředky a postupy mají zajistit následující: *jen jedenkrát podepsat*, *data pro vytváření podpisu neodvozovat*, *zajistit utajení* a *chránit technickými prostředky proti padělání*. Další požadavek je, aby technické prostředky bránili proti zneužití elektronického podpisu třetí osobou. [18] Bohužel se tato směrnice postupem času ukázala jako nedostatečná. Například při používání elektronického podpisu nezajišťovala dostatečnou právní jistotu a kompatibilitu formátu zejména při zapojení subjektů z jiných členských států. Nezajištěním elektronického propojení evropských členských států nenaplnila svůj účel a po téměř 15 letech byla nahrazena nařízením eIDAS.[19]

3.1 Zákon č. 227/2000 Sb.

Vydáním směrnice 1999/93EC Evropského parlamentu a Rady, o zásadách společenství pro elektronické podpisy nastala povinnost České republice začlenit tématiku týkající se elektronického podpisu i do české legislativy. To se povedlo a dne 29.06.2000 byl ve Sbírce zákonů, zveřejněn zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Účelem tohoto zákona je úprava v souladu s právem Evropských společenství, používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. V první části zákona konkrétně v **§ 2** Vymezení některých pojmů přibyly oproti evropské směrnici pojmy jako: *elektronická značka*, *datová zpráva*, *elektronická data*, *držitel certifikátu*, *poskytovatel certifikačních služeb*, *kvalifikovaný certifikát*, *kvalifikované časové razítko* atd. Smyslem tohoto zákona o elektronickém podpisu je také umožnit použití digitálního podpisu v rámci elektronické komunikace jako ekvivalent podpisu vlastnoručního při běžné listinné formě komunikace.“[20] Bosáková k tomu uvádí následující: „*Snaha zákonodárce současně byla taková, aby zákon o elektronickém podpisu jako základní právní předpis pro tuto oblast byl z hlediska jeho obsahu a rozsahu co nejobecnější a současně technologicky pokud možno co nejméně závislý, aby při případné změně technologie nemuselo docházet současně i ke změně textu zákona*

[18] EUR-LEX.EUROPA.EU, *Access to European Union law* [online]. © 2019 [cit. 2019-12-20]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A31999L0093>.
[19] UREŠ, M. *eIDAS: pád digitální zdi v Evropě* [online]. CCB spol. s.r.o., 2001 - 2019 [cit. 2019-12-20]. Dostupné z WWW: <https://www.systemonline.cz/sprava-it/eidas-pad-digitalni-zdi-v-evrope.htm>.
[20] ZÁKONY PRO LIDI.CZ, *Zákon č. 227/2000 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-12-20]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2000-227>.

o elektronickém podpisu.“[21] Co se týká požadavků na prostředky pro bezpečné vytváření elektronických podpisů, jsou obdobné jako ve směrnici 1999/93EC. Zákon č. 227/2000 Sb., o elektronickém podpisu v **§ 17 odst. 3** navíc zmiňuje, prostředky pro vytváření elektronických podpisů musí být před svým použitím bezpečným způsobem vydány a data pro vytváření elektronických podpisů musí být důvěryhodným způsobem v těchto prostředcích vytvořena nebo do nich přidána. Dále tento zákon například řeší ověřování elektronických podpisů a elektronických značek, povinnosti podepisující a označující osoby, povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů, akreditaci a podmínky udělení akreditace pro poskytování certifikačních služeb, náležitosti kvalifikovaného certifikátu a kvalifikovaného systémového certifikátu, náležitosti kvalifikovaného časového razítka.[22] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) prošel za 16 let své existence mnoha změnami. Jeho Úplné znění s barevným vyznačením posledních změn je ke stažení v archivu Ministerstva vnitra v souvisejících dokumentech https://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx.

3.2 Zákon č. 440/2004 Sb.

Po čtyřech letech byl zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) novelizován. Archiv Ministerstva vnitra ČR sděluje následující „*Dne 26. července 2004 nabyla účinnosti novela zákona o elektronickém podpisu (č. 440/2004 Sb.). Tento předpis nově zavádí pojem kvalifikované časové razítko, které prokazuje existenci elektronického dokumentu v čase. Další novinkou je možnost používat elektronické značky. Pro ty se stejně jako pro zaručený elektronický podpis používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy.*“[23] Časovým razítkem se zabývá podkapitola „4.4 Časová razítka“. Elektronickou značku vysvětluje podkapitola „4.3 Elektronická značka a elektronická pečeť“.

[21] BOSÁKOVÁ, D. et al. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* Olomouc : ANAG, 2002. s. 10
[22] ZÁKONY PRO LIDI.CZ, *Zákon č. 227/2000 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-10-30]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2000-227>.
[23] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor Hlavního architekta eGovernment, Archiv, *Zákon č. 227/2000 Sb., o elektronickém podpisu* [online]. MVČR, © 2012. 1. října [cit. 2019-10-30]. Dostupné z WWW: <https://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

3.3 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES je na Úředním věstníku EU v jednotlivých úředních jazykových verzích Unie https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32014R0910.[24] Podle svého celého názvu se zabývá dvěma hlavními okruhy problémů **důvěryhodnými službami** a **elektronickou identifikací.** Toto nařízení je zčásti účinné od 01.07.2016, jako celek včetně eID (elektronická identifikace) od 29.09.2018 a má úplný přímý účinek s předností před vnitrostátními předpisy. Mimo jiné také přináší technologickou neutralitu a otevřenost inovacím a také povinnost vzájemného uznávání oznámených prostředků elektronické identifikace. Důvody přijetí eIDAS jsou zmíněny již v tzv. recitálu Nařízení: budování důvěry v on-line prostředí pro hospodářský rozvoj na jednotném digitálním trhu v EU, společný základ pro elektronickou komunikaci mezi občany, podniky a orgány veřejné moci pro efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a elektronického obchodu. [25]

Nařízení eIDAS obsahuje celkem čtyři oblasti. **Obecné ustanovení** čl. 1–5: předmět, působnost, definice, volné poskytování služeb vytvářející důvěru na vnitřním trhu, zpracování a ochrana údajů. **Elektronická identifikace** čl. 6-12: vzájemné uznávání, požadavky na systémy identifikace, úrovně záruky, notifikace, narušení bezpečnosti, odpovědnost, interoperabilita. **Služby vytvářející důvěru** čl. 13-45: e-podpis, e-pečeť, e-časové razítko, e-doporučené doručování, autentizace internetových stránek. **Elektronické dokumenty** čl. 46, ten definuje právní účinky elektronických dokumentů následovně „*Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu*.“[26]

Jedním z nejdůležitějších pojmů z hlediska tématu této práce je zcela určitě ***kvalifikovaný elektronický podpis***. V současné době jde o „nejsilnější“ typ elektronického podpisu, který je uznávaný napříč EU. Má právní účinek rovnocenný vlastnoručnímu podpisu. Nesmí mu být upírány právní účinky a nesmí být odmítán jako

[24] EUR-LEX.EUROPA.EU, *Access to European Union law* [online]. © 2019 [cit. 2019-12-29]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>.
[25] Interní materiály Agentura BOVA ze školení
[26] EUR-LEX.EUROPA.EU, *Access to European Union law* [online]. © 2019 [cit. 2019-12-29]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>.

důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu. Více než kvalifikovaný elektronický podpis členské státy v přeshraničním styku žádat nemohou. [27] V přílohách nařízení eIDAS jsou pak detailně popsány požadavky. **Příloha I**. – Požadavky na kvalifikované certifikáty pro elektronické podpisy. **Příloha II**. – Požadavky na kvalifikované prostředky pro vytváření elektronických podpisů. **Příloha III**. – Požadavky na kvalifikované certifikáty pro elektronické pečetě.[28]

V České republice se zabývá problematikou nařízení eIDAS Ministerstvo vnitra, které této problematice věnuje celou sekci na svých webových stránkách v záložce eGovernment / Služby vytvářející důvěru a elektronická identifikace https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx.

Také přední znalec této problematiky pan Jiří Peterka se na serveru Lupa.cz věnuje tomuto tématu pod názvem „seriál eIDAS“, kde déle než šest let publikuje své články.

Na toto téma je a bylo také konáno mnoho odborných seminářů a školení. Z výše uvedeného tedy vyplývá, že problematika unijního nařízení eIDAS je značně rozsáhlá a složitá i pro renomované odborníky.

3.4 Zákon č. 297/2016 Sb.

Zákon č. 227/2000 Sb., o elektronickém podpisu, byl nahrazen zákonem č. 297/2016 Sb., **o službách vytvářejících důvěru** pro elektronické transakce.[29] Cílem tohoto zákona je adaptace právního řádu České republiky na přijetí nařízení eIDAS pro oblast služeb vytvářející důvěru. V zákoně je upraveno pouze to, co nařízení výslovně nechává na úpravu vnitrostátním právním řádem. Stanovuje pravidla pro veřejnou správu, jak elektronicky podepisovat, pečetit a opatřovat dokument časovým razítkem.“[30] Zákon nabyl účinnosti dnem jeho vyhlášení 19. září 2016 a upravuje v návaznosti na přímo použitelný předpis Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro

[27] Interní materiály Agentura BOVA
[28] EUR-LEX.EUROPA.EU, *Access to European Union law* [online]. © 2019 [cit. 2019-12-30]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>.
[29] PRVNÍ CERTIFIKAČNÍ AUTORITA, *Novinky* [online]. První certifikační autorita, a.s. (I.CA) © 2019. 1. ledna [cit. 2019-12-30]. Dostupné z WWW: <https://www.ica.cz/novinky?IdNews=434>.
[30] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor eGovernmentu, *Služby vytvářející důvěru a elektronická identifikace.* [online]. MVČR, © 2019. 17. března [cit. 2019-12-30]. Dostupné z WWW: <https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx>.

elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES v **§ 1** následující: některé postupy poskytovatelů služeb vytvářejících důvěru, některé požadavky na služby vytvářející důvěru, působnost Ministerstva vnitra v oblasti služeb vytvářejících důvěru a sankce za porušení povinností v oblasti služeb vytvářejících důvěru.

Jednou z povinností kvalifikovaných poskytovatelů služeb vytvářejících důvěru v **§ 3** je uchovávat po dobu 10 let dokumenty související s vydáváním kvalifikovaných certifikátů. Po uplynutí této doby dále uchovávat po dobu 15 let údaje, na základě kterých byla ověřena totožnost žadatele o vydání kvalifikovaného certifikátu pro elektronické podpisy.

Podepisování dokumentu je uvedeno v **§ 5 - §7** povinnost pro „veřejnoprávní podepisující" stát, územní samosprávní celek a jiné osoby při výkonu působnosti v oblasti veřejné správy, kteří právně jednají, musí k podepisování elektronickým podpisem použít pouze ***kvalifikovaný elektronický podpis.***

V **§ 8 - § 10** je řešeno pečetění dokumentu, kde musí „veřejnoprávní podepisující" jedná-li při výkonu své působnosti, zapečetit dokument v elektronické podobě ***kvalifikovanou elektronickou pečetí.*** K pečetění elektronickou pečetí, lze použít pouze uznávanou elektronickou pečeť. Uznávanou elektronickou pečetí se rozumí zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť.

Použitím kvalifikovaného elektronického časového razítka se zabývá **§ 11**, pojednává o tom, že by měl „veřejnoprávní podepisující", který právně jedná při výkonu své působnosti a podepsal elektronický dokument, opatřit podepsaný elektronický dokument ***kvalifikovaným elektronickým časovým razítkem***. To samé platí i pro „veřejnoprávní podepisující", který právně jedná při výkonu své působnosti a zapečetil elektronický dokument, opatřit zapečetěný elektronický dokument kvalifikovaným elektronickým časovým razítkem.[31]

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 obsahovalo přechodné období, které dovolovalo používat dříve vydané certifikáty pro tvorbu elektronického podpisu po dobu jednoho roku. Česká legislativa to vyřešila v zákoně 297/2016 Sb.,

[31] INFORMACE, INFORMATIKA, eGOVERNMENT, *Svobodný přístup k informacím, ochrana osobních údajů, elektronický podpis, elektronické komunikace, elektronické úkony a konverze dokumentů, informační systémy veřejné správy, kybernetická bezpečnost, základní registry.* Ostrava : Sagit, 2014. ÚZ. s. 263-264

o službách vytvářejících důvěru v **§ 19 Přechodná ustanovení**. Konkrétně v odst. 1 je uvedeno „Po dobu 2 let ode dne nabytí účinnosti tohoto zákona lze k podepisování podle **§ 5** použít rovněž zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis.“[32] Pro veřejnou správu to znamenalo, že se nic nemění a může zatím využívat stávající prostředky a certifikáty k elektronickému podepisování, tak jako doposud, a to do 19. září 2018. Tato benevolence ale platila pouze pro naše vnitrostátní vztahy a pro české území. Použití kvalifikovaných prostředků (např. čipová karta či USB token) pro vytváření kvalifikovaných elektronických podpisů používaných v případě mezinárodní spolupráce, bylo platné již více než rok, dle pravidel plného znění nařízení eIDAS.[33]

K **§ 7** týkajícího se podepisování dokumentu „K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1.[34] má Peterka v jednom ze svých článků výhrady. Označuje ho za problémový a nešťastný z důvodu postavení na úroveň vlastnoručního podpisu (v soukromoprávních vztazích) i prostý elektronický podpis. Jde o podpis, kterým může být cokoliv, co je elektronické a co může někdo vydávat za svůj podpis. To může být například naskenovaný obrázek s ručním podpisem, emailová patička, vzorek vlastnoručního podpisu nasnímaný na dotykovém zařízení, číselný PIN atd. Tímto se otevírají možnosti pro toho, kdo by chtěl někoho jiného napálit či podvést. To Peterka potvrzuje i obavami senátorů konkrétně Miloše Vystrčila z návrhu na plénu Senátu plné znění tisk č. 306 https://www.senat.cz/xqw/xervlet/pssenat/hlasovani?action=steno&O=10&IS=5753&D=24.08.2016#b17073.[35]

3.5 Zákon č. 250/2017 Sb.

Zákon č. 250/2017 Sb., **o elektronické identifikaci** upravuje v návaznosti na přímo použitelný předpis Evropské unie upravující elektronickou identifikaci tj. Nařízení

[32] INFORMACE, INFORMATIKA, eGOVERNMENT, *Svobodný přístup k informacím, ochrana osobních údajů, elektronický podpis, elektronické komunikace, elektronické úkony a konverze dokumentů, informační systémy veřejné správy, kybernetická bezpečnost, základní registry.* Ostrava : Sagit, 2014. ÚZ. s. 266

[33] MUNIS, informační systém pro města a obce, *Nařízení eIDAS se znovu připomíná.* Praha [online]. © 2019 Triada, spol. s.r.o., [cit. 2019-11-18]. Dostupné z WWW: <https://www.munis.cz/art/548>.

[34] ZÁKONY PRO LIDI.CZ, *Zákon č. 297/2016 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-11-18]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2016-297>.

[35] PETERKA, J. Lupa.cz, *Po 16 letech existence přestává platit zákon o elektronickém podpisu* [online]. © 1998-2019 Lupa.cz, 2016. 19. září [cit. 2019-11-19]. Dostupné z WWW: <https://www.lupa.cz/clanky/po-16-letech-existence-prestava-platit-zakon-o-elektronickem-podpisu/>.

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 v **§ 1** je předmětem úpravy využití elektronické identifikace, působnost Ministerstva vnitra a Správy základních registrů na úseku elektronické identifikace a přestupky na úseku elektronické identifikace.

Základní definice, proč můžeme elektronickou identifikaci používat je v **§ 2** Prokázání totožnosti s využitím elektronické identifikace „*Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „kvalifikovaný systém“).*

Zákon se v ostatních **§** zabývá a vymezuje pojmy jako kvalifikovaný systém, kvalifikovaný správce, posuzování prostředku pro elektronickou identifikaci a systému elektronické identifikace, povinnosti kvalifikovaného správce, povinnosti držitele, povinnosti kvalifikovaného poskytovatele, působnost na úseku elektronické identifikace, **národní bod**, evidence vydaných prostředků pro elektronickou identifikaci, seznam kvalifikovaných správců a kvalifikovaných poskytovatelů, využívání údajů z informačních systémů veřejné správy na úseku elektronické identifikace a přestupky na úseku elektronické identifikace. Tento zákon nabyl účinnosti dnem 1. července 2018.[36]

Zjednodušeně řečeno je základem všeho ***národní bod pro identifikaci a autentizaci***. Správcem národního bodu je Správa základních registrů, která ho uvedla do ostrého provozu právě 1. července 2018 v souvislosti s nabytím účinnosti zákona č. 250/2017 Sb. Jedná se o informační systém zajišťující zprostředkování elektronické identifikace. Ta řeší vazbu mezi poskytovateli prostředků, kterými uživatelé prokazují svoji identitu a poskytovateli online služeb. Dále je zabezpečeno napojení na ohlášené systémy v rámci Evropské unie pomocí mezinárodního uzlu. Od 18. září 2018 mají povinnost (dle eIDAS) poskytovatelé elektronických služeb státu rozpoznávat a uznávat elektronickou identitu občanů členských států Evropské unie, které nahlásily ostatním státům své identitní prostředky a systémy. Webový portál www.eidentita.cz je veřejným rozhraním národního bodu pro přístup uživatelů a poskytovatelů online služeb. Prokazování totožnosti je proces v rámci elektronické komunikace mezi uživatelem a poskytovatelem identity, ten předá národní identitní autoritě informaci o ověření

[36] ZÁKONY PRO LIDI.CZ, *Zákon č. 250/2017 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-11-22]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2017-250>.

uživatele včetně jednoznačného indentifikátoru spojeného s jeho účtem v národní identitní autoritě. Na základě získaných informací si národní identita vyzvedne z registru obyvatel informace v rozsahu poskytované služby. Po výzvě národní identitní autority k udělení souhlasu uživatele s poskytnutím požadovaných údajů v případě jeho udělení, tyto údaje odešle spolu s identifikátorem poskytovateli. Identifikátor je tentokrát ve vztahu mezi uživatelem a předmětnou službou unikátní. Poté je uživatel přesměrován na stránky poskytované služby. Uživatel také může spravovat svůj profil na portálu eidentita.cz, kde může doplnit své údaje o telefonní číslo a e-mail, které je možné předávat poskytovatelům služeb kvůli zjednodušení komunikace s klientem. Dále také může uživatel spravovat udělené souhlasy, například je může trvale eliminovat. V současné době jsou dva způsoby prokazování totožnosti. Národní bod umožňuje přihlášení pomocí přihlašovacích údajů formou jména a hesla k uživatelskému účtu na portálu eidentita.cz. Ověřením totožnosti na kontaktním místě Czech POINT jsou údaje spolu se zadáním jednorázového SMS kódu poslány na mobilní telefon uživatele a ty je následně možno využívat jako identitní prostředek na úrovni důvěry.[37]

[37] PEŠEK, M. ředitel Správy základních registrů, *Národní bod pro identifikaci a autentizaci* [online]. CCB spol. s.r.o. 2018. 19. září [cit. 2019-11-23]. Dostupné z WWW: <http://m.systemonline.cz/it-security/narodni-bod-pro-identifikaci-a-autentizaci.htm>.

4 Pojmy související s elektronickým podepisováním

V této kapitole autor uvede a vysvětlí základní pojmy vztahující se k elektronickému podepisování. Pokud chce fyzická osoba - občan elektronicky podepisovat, stačí k tomu opravdu málo. Například navštívit pobočku České pošty poskytující služby Czech POINT, tam se dostaví osobně s občanským průkazem a vygenerovanou žádostí o certifikát, kterou si vygeneruje doma na svém PC, dle návodu příslušné certifikační autority.[38] Zaměstnanci veřejné správy stačí k vydání certifikátu v podstatě ten samý úkon. Avšak před tím, než vyrazí na pobočku České pošty, musí být zaveden zaměstnancem organizace odpovědným jednat s certifikační autoritou. Tento zaměstnanec se musí přihlásit na portál certifikační autority. Tam konkrétního zaměstnance zaeviduje, zadá jeho titul, jméno, příjmení, pracovní email, pracovní zařazení a rodné číslo.[39] Hlavní rozdíl je v tom, že občan získá elektronický podpis, kterým se podepisuje za sebe jako osoba – občan. Oproti tomu zaměstnanec veřejné správy se elektronickým podpisem podepisuje jako osoba - zaměstnanec a odpovědná jednat za úřad v konkrétní věci. Z výše uvedeného je patrné, že proces elektronického podepisování ve veřejné správě je daleko složitější jak technicky, tak i metodicky.

4.1 Podpis, elektronický podpis, digitální podpis, viditelný podpis, biometrický podpis

Pojem **podpis** není třeba představovat i v dávných dobách, kdy chudí lidé neuměli psát a číst, se uměli podepsat třemi křížky. Pojem podpis je tedy spojený výhradně s papírovou, listinnou či analogovou podobou. Můžeme ho nazývat vlastnoruční podpis. U tohoto typu podpisu můžeme ověřit pravost notářsky, soudně nebo úředně. Specialista, který se zabývá vlastnostmi vlastnoručního podpisu (typem inkoustu, tah a sklon pera, typ písma atd.) se nazývá grafolog.

U elektronického podpisu samozřejmě nic takového zkoumat nemusíme. **Elektronický podpis** je vlastně hodnota připojená k elektronickému dokumentu. A tato hodnota se tedy ověřuje. Je vyjádřena tak velkým číslem, že i v počítačové řeči posloupnosti jedniček a nul je tato hodnota ne moc vhodná. Srozumitelnější a efektivnější

[38] POSTSIGNUM, Postup pro získání certifikátu, *Fyzické osoby* [online]. Česká pošta © 2010 [cit. 2019-10-29]. Dostupné z WWW: <http://www.postsignum.cz/fyzicke_osoby.html>.
[39] POSTSIGNUM, Postup pro získání certifikátu, *Firmy, organizace, veřejná správa* [online]. Česká pošta © 2010 [cit. 2019-10-29]. Dostupné z WWW: <http://www.postsignum.cz/firmy_organizace_verejna_sprava.html>.

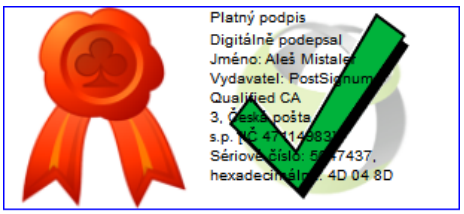
forma pro člověka je kódování, které si vystačí s méně znaky a je prezentováno textovým řetězcem. I tato varianta je však pro běžného uživatele PC dlouhým nesmyslným textem. V praxi s ním naštěstí pracují programy, které ověřují elektronický podpis a výsledek tohoto ověření zobrazují uživateli komfortně a srozumitelně.[40]

Digitální podpis je vlastně elektronický podpis s tím rozdílem, že výraz elektronický podpis je používán v praxi i v oblasti legislativy a zahrnuje i aspekty právní. Pojem digitální podpis je hlavně využíván v technologické oblasti. Tvorba digitálního podpisu je založena na hashovacích funkcích a asymetrické kryptografii. Digitální podpis má vlastnosti nepopiratelnosti, pravosti, zajištění integrity, rychlého a jednoduchého ověření.[41]

Viditelný podpis je také pojem, který je třeba zmínit. Můžeme mu, též říkat vizualizovaný podpis. To jsou údaje z elektronického podpisu vložené uvnitř textu elektronického dokumentu. Obdoba vlastnoručně podepsaného papírového dokumentu na obrázku č. 1 podepsání v aplikaci Adobe Acrobat Reader, obrázek č. 2 podepsání v aplikaci Software 602 Print2PDF.

Obrázek 1: Podpis v Adobe[42]

Obrázek 2: Podpis v Software 602[43]



Odborník ví, že toto elektronický podpis rozhodně není, ale pro spoustu uživatelů i vedoucích zaměstnanců to působí věrohodně a dostatečně. I když je tu s námi elektronický podpis již pár let, je stále potřeba vidět podpis či razítko (pečeť) v obsahu dokumentu.

Biometrický podpis se také řadí mezi viditelné digitální podpisy. U biometrického podpisu lze tvrdit, že je srovnatelný 1:1 s podpisem na listinném dokumentu. Realizuje se technologií, která umožňuje vlastnoručně podepsat a následně verifikovat podpis elektronického dokumentu. K tomuto úkonu je třeba specializovaný

[40] PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011. s. 29
[41] EARCHIVACE.CZ, Technologie, *Digitální podpis* [online]. © 2014 eArchivace [cit. 2019-09-30]. Dostupné z WWW: <http://www.earchivace.cz/technologie/digitalni-podpis/>.
[42] Vlastní zdroj
[43] Vlastní zdroj

hardware v podobě pera (pen) a „ploché destičky“ podpisový pad. Podpisový pad má v sobě zabudovaný šifrovací mechanismus a snímač tlaku. Pomocí snímače tlaku při podepisování osoby snímá fyziologické vlastnosti: tlak na pero, rychlost, zrychlení, sklon pera, dobu podpisu. Hned po podepsání je podpis zašifrován, tím je zabezpečeno, že se s ním nedá manipulovat, zneužít ho nebo zcizit.[44]

4.2 Digitální certifikát, osobní a systémový certifikát, kvalifikovaný certifikát a komerční certifikát

Digitální certifikát by se dal v tištěné podobě přirovnat k cestovnímu pasu či občanskému průkazu. V elektronické podobě je podepsanou datovou strukturou, která obsahuje veřejný klíč držitele certifikátu. Zaměstnanec certifikační autority právě porovnává údaje z občanského průkazu s údaji v žádosti o certifikát, jak je již zmíněno výše v úvodu této kapitoly. Digitální certifikát se skládá z několika položek - jedinečné jméno, platnost, položka vydavatel a předmět, algoritmus podpisu, pořadové číslo certifikátu a verze certifikátu.[45] Dále rozlišujeme certifikáty na osobní a systémové.

Osobní certifikát je vydáván výhradně jen fyzickým osobám.

Systémové certifikáty mohou být vydávány fyzickým osobám, právnickým osobám, organizačním složkám státu a orgánům veřejné moci. Najdou uplatnění při identifikaci serverů, šifrováním komunikace se servery, vytváření elektronických značek i vytváření časových razítek apod.

Další dělení certifikátů je na kvalifikované certifikáty a komerční certifikáty. Oba jsou ve veřejné správě hodně používány.

Kvalifikované certifikáty osobní i systémové se používají na podepisování elektronických dokumentů. Dále se dají využít na označování elektronických značek či tvorbu časových razítek, ověřování podpisů, značek a razítek. S kvalifikovanými certifikáty na rozdíl od komerčních certifikátů, počítá legislativa. V zákoně jsou vymezeny požadavky na kvalifikované certifikáty a na jejich obsah.[46]

[44] BIOMETRICKÝ PODPIS, *Co je biometrický podpis* [online]. Contrisys, s.r.o. © 2012 [cit. 2019-10-10]. Dostupné z WWW: <http://www.contrisys.com/co-je-biometricky-podpis>.
[45] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2. vyd. Brno : COMPUTER PRESS, 2009. s. 58-61
[46] PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011. s. 40-41

Komerční certifikáty mají svou významnou úlohu podle První certifikační autority (I.CA) „především tam, kde nelze s ohledem na platnou legislativu využít kvalifikované certifikáty. Je vhodný pro obchodní použití mimo oblast komunikace s orgány veřejné moci, na které se vztahuje povinnost využívat certifikáty kvalifikované. Nejčastěji se používá v komunikaci mezi komerčními subjekty pro šifrování a autentizaci. Jedná se především o neanonymní přístup na webové servery a předávání šifrovaných dat, jak e-mailovou poštou, tak prostřednictvím webových formulářů“.[47] V praxi se autor práce setkal hlavně s osobními kvalifikovanými certifikáty při podepisování elektronických dokumentů. Co se týče komerčních certifikátů, tak při přihlašování do služeb Czech POINT (výpis z Rejstříku trestů a konverze z moci úřední). Při autentizaci a identifikaci do ABO-K ČNB (internetové bankovnictví České národní banky), ePortal České správy sociálního zabezpečení, EZAK Elektronický nástroj pro správu veřejných zakázek, CRAB Centrální registr administrativních budov.

4.3 Elektronická značka a elektronická pečeť

V této podkapitole se seznámíme s další změnou, které nám zavedlo legislativní nařízení eIDAS. Před nařízením eIDAS byl znám pojem elektronická značka. S platností nařízení eIDAS byla zavedena elektronická pečeť.

Elektronická značka byla v podstatě to samé, co elektronický podpis s tím rozdílem, že mohly elektronicky podepisovat právnické osoby včetně organizačních složek státu. Podepisování mělo automatizovanou podobu - vše provádí stroj dle pravidel dříve zadaných člověkem. U nás se později automatizované podepisování obohatilo přidáváním elektronických značek. Tímto krokem se zabezpečilo to, že když šlo o elektronickou značku, mohla patřit fyzické i právnické osobě i organizační složce státu. V novém nařízení eIDAS zavedla Evropská unie něco podobného, zaměřila se na toho, kdo úkon podepisování provádí. A tak vznikl nový pojem **elektronická pečeť**. Elektronickou pečeť může vytvářet výhradně právnická osoba včetně organizační složky státu a může ji připojovat jen k tomu, čeho je sama původcem. Připojení elektronické pečetě k elektronickému dokumentu tedy není projevem vůle, ale deklarací toho, že je od konkrétní právnické osoby „od ní“, proto nelze elektronické pečetě přidávat na cokoliv

[47] PRVNÍ CERTIFIKAČNÍ AUTORITA, *Komerční certifikát* [online]. První certifikační autorita, a.s. (I.CA) © [cit. 2019-10-29]. Dostupné z WWW: <https://www.ica.cz/Komercni-certifikat>.

„cizího“. Tímto byl osud elektronických značek zpečetěn, přesto je bylo možné používat v období dvouleté výjimky, než vstoupilo v platnost nařízení eIDAS. [48]

4.4 Časová razítka

Při tvorbě papírových dokumentů zejména smluv je spolu s vlastnoručním podpisem další důležitou součástí i datum podpisu. Vlastnoruční podpis spolu s datem v listinné podobě tedy dostatečně zaručují identifikaci, vznik a platnost dokumentu (smlouvy). Další výhoda je v tom, že vlastnoruční podpis a datum se dodatečně těžko zaměňuje. V elektronické podobě je to přesně naopak, změny u elektronických dokumentů jsou snadné a rychlé. Z tohoto důvodu je nutné mít dokumenty podepsané a označené datem tak, aby nebyla dodatečná změna možná. Označení dokumentu časovým razítkem (Time stamp) nám zaručuje, že je dokument právně platný a stejný jako listinný dokument.[49] Časové razítko si představme jako datovou strukturu obsahující čas, otisk z dokumentu, pořadové číslo a jméno vydavatele razítka. O to vše se stará třetí nezávislá strana a tou je Autorita vydávající časová razítka (TSA - Time stamping authority). Autorita nemá za úkol zkoumat totožnost konkrétní osoby ani obsah dokumentu, ale pomocí časového razítka dokázat, že dokument existoval v konkrétním čase. Časové razítko lze ve veřejné správě využít hned v několika případech. Při tvorbě dokumentů, které opouštějí úřad, se spolu s elektronickým podpisem připojí i časové razítko. Tento úkon můžeme nazývat razítkování dokumentu a garantuje nám zapouzdření a existenci dokumentu v čase. Pozdější případná změna dokumentu by způsobila neplatnost časového razítka. [50] Veřejná správa má povinnost ze zákona zachovávat některé dokumenty i několik let a právě i v tomto případě má časové razítko uplatnění. Jako doplněk elektronického podpisu ho můžeme využít při archivaci elektronických dokumentů a všude tam, kde je potřeba prokázat, jak vypadal elektronický dokument v určitém okamžiku. A také prodloužíme platnost dokumentu. Časová razítka se dají koupit u certifikační autority formou balíčku (množství razítek ks) nebo paušál (počet razítek za 1 měsíc). [51] Většina orgánů veřejné správy měsíčně vyprodukuje i stovky

[48] PETERKA, J. Lupa.cz, *eIDAS: Elektronické značky a pečetě a rekviem za datovou zprávu* [online]. © 1998-2019 Lupa.cz, 2016. 4. července [cit. 2019-10-30]. Dostupné z WWW: <https://www.lupa.cz/clanky/eidas-elektronicke-znacky-a-pecete-a-rekviem-za-datovou-zpravu/>.
[49] HUMPOLEC, J. *Elektronické časové razítko jako doplněk elektronického podpisu* [online]. © 1996-2019 Economia, a. s., 2008. 5. května 11:15 [cit. 2019-10-30]. Dostupné z WWW: <https://tech.ihned.cz/c1-24518930-elektronicke-casove-razitko-jako-doplnek-elektronickeho-podpisu>.
[50] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2. vyd. Brno : COMPUTER PRESS, 2009. s. 345
[51] ČESKÁ POŠTA, Služby, *Časová razítka*. [online]. © 2018 [cit. 2019-10-31]. Dostupné z WWW: <https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka>.

elektronických dokumentů. S těmito dokumenty musí na základě zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, nakládat následovně: např. „*§ 63 odst. 3 veřejnoprávní původci uvedení v § 3 odst. 1 písm. a) až d), i), k) a m), kraje a hlavní město Praha vykonávají spisovou službu v elektronické podobě v elektronických systémech spisové služby, dále v souladu s § 64 příjem, označování, evidence a rozdělování dokumentů, a také podle § 65 vyřizování a podepisování dokumentů a podle § 3 odst. 1 povinnost uchovávat dokumenty a umožnit vývěr archiválií*“.[52] Elektronický systém spisové služby umí hlídat platnost časových razítek a automaticky přerazítkovávat elektronické dokumenty.

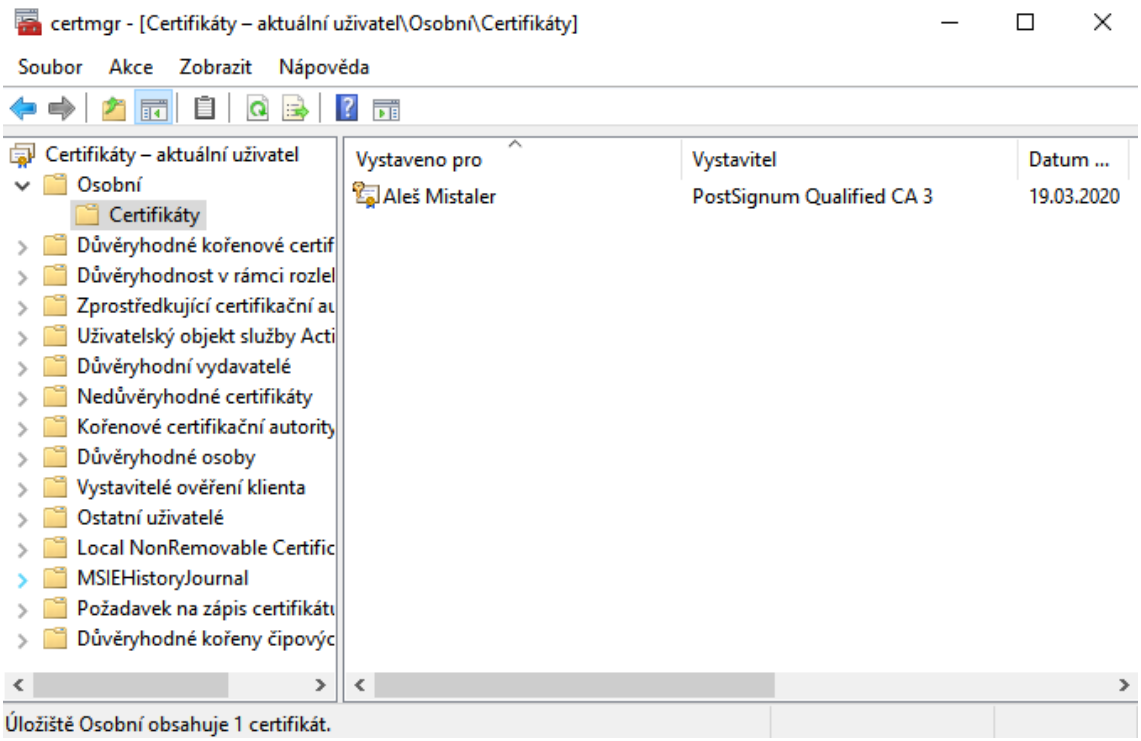
4.5 Úložiště certifikátů

Tato podkapitola se zabývá tím, jak chránit a kam bezpečně ukládat soukromé klíče a jiný citlivý kryptografický materiál. Nejsnadnější metodou je uložení na lokální disk PC, zároveň je to však značně rizikové, protože je certifikát uložen v systému Windows. Soukromý klíč je vázán na uživatelský profil v operačním systému Windows. Mezi další velká rizika je možnost stažením z internetu či spuštěním z emailového klienta „škodlivý software“ v podobě trojského koně. Trojský kůň může například přečíst přístupové heslo klíče nebo přečíst jeho rozšifrovanou podobu. Nevýhodou také je, že se dají data snadno zcizit. K bezpečnějším a efektivnějším úložištím patří třeba čipové karty, usb tokeny a HSM moduly.[53]

Certifikát ve Windows. Obsah úložiště certifikátů se v operačním systému Windows spustí příkazem certmgr.msc. Na obrázku č. 3 v podsložce osobní - certifikáty je vidět

[52] ARCHIVNICTVÍ A SPISOVÁ SLUŽBA, *Skartační řízení : zákon, vyhlášky, nařízení vlády*. Ostrava : Sagit, 2012-. ÚZ. s.4,29-30
[53] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2. vyd. Brno : COMPUTER PRESS, 2009. s. 37

Obrázek 3: Certifikát ve Windows[54]



certifikát přihlášeného uživatele. V dalších podsložkách jsou například důvěryhodné certifikační autority, kořenové certifikační autority, certifikáty ostatních uživatelů., které byly vydány důvěryhodnými certifikačními autoritami. Certifikáty ve Windows mají většinou přípony s koncovkou cer, der, pem, crt atd.

Čipová karta je jedním z nejrozšířenějších druhů úložišť. Je to plastová karta, která obsahuje čip, ten je buď zalitý přímo do karty, nebo vsazen do vyfrézované dutiny karty. Podle osazení je dělíme na kontaktní a bezkontaktní. Karty také musí splňovat předepsané rozměry dle ISO normy, nejčastěji však mívá velikost jako platební karta. Budoucnost bude přát spíše bezkontaktní variantě.[55] Aby mohla čipová karta komunikovat je potřeba vlastnit i čtečku čipové karty. Čtečka čipové karty je zpravidla propojena s PC přes USB rozhraní. U notebooků může být i integrovaný slot čtečky čipových karet. Na některých pracovištích veřejné správy je dnes již běžné, že zaměstnanci řeší vše pomocí čipové karty. Při vstupu do budovy úřadu přiloží kartu k přístupovému terminálu a jsou vpuštěni turniketem na pracoviště. Turniket je propojen s docházkovým systémem, do kterého mají přístup pro kontrolu docházky svých podřízených i vedoucí zaměstnanci. Docházkový systém je i propojen s personálním

[54] Vlastní zdroj
[55] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2. vyd. Brno : COMPUTER PRESS, 2009. s. 39

informačním systémem, který dle docházky vypočítává měsíční mzdu. Při příchodu do své kanceláře zaměstnanec zapne PC a vloží kartu do čtečky, ta ho autentizuje a automaticky přihlásí do systému Windows. No a touto kartou může úředník i *podepsat elektronický dokument* svým kvalifikovaným certifikátem. Dokonce i některé úřady mají zavedeno, že při jízdě služebním vozem musí ve vozidle přiložit kartu k zabudované čtečce, aby bylo zřejmé, kdo v určitou dobu vůz řídil. Čipové karty zkrátka mají v současné době obrovskou všestrannost, další využití je například zabezpečený tisk (z tiskárny se obsah vytiskne, až po přiložení karty), odkódování a zakódování přístupu a odchodu, odemykání a zamykání dveří, ve výtazích přístup do určitých pater, u dětí při výdeji jídla ve školních jídelnách nebo jako platba jízdného a předplatného v dopravních prostředcích. Podobné zařízení jako čipová karta je token.

Token na rozdíl od čipové karty nepotřebuje čtečku karty, připojuje se přímo do USB portu počítače. Je pro uživatele na používání přívětivější a řada z nich ho nosí připevněn na svazku klíčů a také je to ekonomičtější varianta oproti čipové kartě. Pracuje ale na stejném principu jako čipová karta. Primárně zajišťuje vyšší bezpečnost oproti přihlašování heslem a uživatelským jménem. Využívá dvou faktorovou autentizaci, která nesporně zvyšuje stupeň bezpečnosti. Jedním z faktorů je fyzické vlastnictví tokenu, druhým faktorem je nastavení PINu (hesla) chránící token před zneužitím. U PINu se dá nastavit jeho délka a maximální počet neplatných zadání. Při překročení limitu zadáním špatného PINu se token zablokuje. Správný PIN nás naopak přihlásí k tokenu a umožní využít funkce tokenu. Další hlavní funkcí tokenu je podepisování elektronického dokumentu kvalifikovaným certifikátem. Ten je na tokenu zastoupen formou privátního šifrovacího klíče a je vygenerován přímo v tokenu, proto není technicky možné ho z tokenu vyexportovat.[56] K čipové kartě i tokenu většinou bývá dodáván obslužný software (middleware), který je umožňuje konfigurovat nebo inicializovat. Dále také zabezpečuje komunikaci mezi ostatními aplikacemi od různých výrobců.

HSM modul (Hardware Security Module) je nejbezpečnější úložiště pro certifikáty a klíče. Jde o specializovaný hardware, který se dodává ve dvou variantách. Buď v podobě samostatného zařízení, nebo jako dedikovaná karta, která lze přidat do serveru. Ještě speciálnější jednotky se využívají v bankovnictví pro ochranu bankovních transakcí. Uplatnění těchto modulů je hlavně v již zmíněných bankách, ve velkých

[56] JELÍNEK, M. *Autentizační tokeny v praxi* [online]. CCB spol. s.r.o., © 2001-2019 [cit. 2019-10-31]. Dostupné z WWW: <https://www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm>.

korporátních společnostech, ale začínají se používat i ve veřejné správě. Vyplatí se hlavně při velkém počtu zaměstnanců 1000 a více. Vysoká bezpečnost proti odcizení je dána hlavně umístěním těchto modulů v „serverovnách“, které jsou chráněny kontrolou vstupu. HSM moduly k tomu ještě přidávají bonus v podobě fyzické bezpečnosti umožňující vymazání či dešifrování kryptografického materiálu v případě ruční manipulace s boxem. Další výhoda zabezpečení je v tom, že k těmto modulům nemusí mít přístup běžný administrátor, ale lze jiné osobě přidělit roli bezpečnostního administrátora. Moduly umí i zvyšovat efektivitu výpočetního výkonu kryptografické operace, centralizaci managementu klíčů a umí i mnoho dalších funkcí a operací. Velkou nevýhodou jsou ovšem vysoké pořizovací náklady.[57]

4.6 Certifikační autority

Certifikační autorita je třetí strana, která vydává certifikáty a označuje se zkratkou **CA**. Certifikační autoritu si můžeme provozovat sami na svém PC, dále ji může provozovat zaměstnavatel, máme i certifikační autority bank, které jsou využívány při internetbankingu. V legislativním vyjádření se nemluví o certifikační autoritě, ale o poskytovateli certifikačních služeb. Certifikační autority vydávající certifikáty definované zákonem (kvalifikované) a splňující další požadavky zákona nazýváme **kvalifikované certifikační autority**. Tyto autority mohou požádat stát o udělení akreditace pro výkon činnosti certifikačních služeb. Pokud splňují podmínky a vše dle zákona, získají akreditaci a stávají se **akreditovanou certifikační autoritou**. Občan, který chce jednat s orgány veřejné moci, musí mít uznávaný elektronický podpis formou kvalifikovaného certifikátu, vydaný právě akreditovanou certifikační autoritou. Akreditované certifikační autority zpravidla nemají stejnou strukturu svého organizačního členění, a proto jsou vnitřně členěny. Na **kořenové autority** a **podřízené** (zprostředkující) **autority**.[58] Před unijním nařízením eIDAS byly v ČR celkem, tři kvalifikovaní poskytovatelé certifikačních služeb, a to První certifikační autorita, a. s., Česká pošta, s. p., eIdentity a. s.[59] Účinkem unijního nařízení eIDAS můžeme využívat i evropské kvalifikované poskytovatele služeb vytvářející důvěru vydávající kvalifikované certifikáty. Jejich přehled je na webu EU Trust Service status (TSL)

[57] ASKON.CZ. *HSM moduly* [online]. ASKON INTERNATIONAL s.r.o., © 2019 [cit. 2019-10-10]. Dostupné z WWW: <http://www.askon.cz/Produkty/HSM-moduly/>.
[58] PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011. s. 42-44
[59] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor eGovernmentu: *Archiv* [online]. MVČR, © 2016. 30. května [cit. 2019-10-31]. Dostupné z WWW: <https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>.

http://tlbrowser.tsl.website/tools/index.jsp a na https://webgate.ec.europa.eu/tl-browser/#/ .[60]

4.7 Elektronický podpis dle eIDAS

Podkapitola elektronický podpis dle eIDAS je autorem záměrně vybrána jako zakončení celé kapitoly s názvem pojmy související s elektronickým podepisováním. Důvod je prostý, jde totiž o nejaktuálnější platnou záležitost. Dnem 19.09.2018 skončila dvouletá výjimka oproti nařízení eIDAS. Veřejné správě nastala povinnost podepisovat úřední elektronické dokumenty pouze kvalifikovanými elektronickými podpisy. To znamenalo, že orgány veřejné správy museli nakoupit kvalifikované prostředky pro vytváření elektronických podpisů. Kvalifikované prostředky (QSCD Qualified Signature Creation Device) jsou hardware, většinou USB tokeny nebo čipové karty. Na tento hardware je potřeba nahrát nový kvalifikovaný certifikát, který je vygenerován přímo na tokenu nebo čipové kartě. Výhodou kvalifikovaných prostředků je to, že z něj nejde vyexportovat soukromý klíč. Je to daleko bezpečnější řešení, než bez kvalifikovaného prostředku, kde hrozí získání kopie klíče nebo jeho hodnoty. Zároveň je zabezpečeno, že bez našeho vědomí a přítomnosti ho nikdo nezneužije. Před nařízením eIDAS měly většinou orgány veřejné moci hlavně z ekonomických důvodů nahrány certifikáty v systémovém úložišti Windows. Nyní mají „hmotnou věc“, kterou mohou třeba zamknout do zásuvky svého stolu, případně přenést na jiný počítač. A jak zjistí protistrana, že úředník podepsal dokument kvalifikovaným certifikátem na kvalifikovaném prostředku? Umístění soukromého klíče musí být v kvalifikovaném prostředku. Při vydání prvotního certifikátu dochází k vytvoření vazby token – žadatel o certifikát. Je evidována a kontrolována u certifikační autority. Z tohoto důvodu není technicky možné mít na tokenu více certifikátů jiných žadatelů. Ve vlastnostech podepsaného dokumentu při ověřování podpisu je v detailu certifikátu položka QC statements, kde je uvedeno Private key on QSCD. V češtině výpisy QC – prohlášení kvalifikovaného certifikátu. Více autor vysvětlí a popíše v praktické části.[61]

[60] PRŮŠA, J. Lupa.cz, *eIDAS a problémy s důvěryhodností kvalifikovanýchcertifikátů* [online]. © 1998-2019 Lupa.cz, 2017. 17. července [cit. 2019-10-31]. Dostupné z WWW: <https://www.lupa.cz/clanky/eidas-a-problemy-s-duveryhodnosti-kvalifikovanych-certifikatu/>.

[61] PETERKA, J. Lupa.cz, *Elektronické podpisy: v září skončí výjimka, budou úředníci připraveni?* [online]. © 1998-2019 Lupa.cz, 2018. 11. června [cit. 2019-11-01]. Dostupné z WWW: <https://www.lupa.cz/clanky/elektronicke-podpisy-v-zari-skonci-vyjimka-budou-urednici-pripraveni/?ic=serial-box&icc=text-title>.

5 Praktická část

V závěrečné kapitole autor uvede postupy ze dvou různých organizací, které aplikoval při své praxi. V ní popíše a vysvětlí, jak se pracovalo s certifikáty před nařízením eIDAS a co všechno se muselo udělat do 19.09.2018, kdy vstoupilo nařízení eIDAS v platnost a jak to funguje nyní. Před tím je potřeba ještě zmínit, že certifikát (pro zaměstnance) je vydáván na dobu určitou. V tomto případě se jedná o 1rok. Certifikát tedy má určitý cyklus životnosti. Začíná generováním žádosti o certifikát, vydáním vlastního certifikátu, případně může být revokován (odvolán), obnoven a nakonec mu vyprší platnost. Jednotlivé fáze životnosti certifikátu budou rovněž vysvětleny v následujících podkapitolách. V obou organizacích jsou využívány služby od akreditovaného poskytovatele certifikačních služeb České pošty (PostSignum).

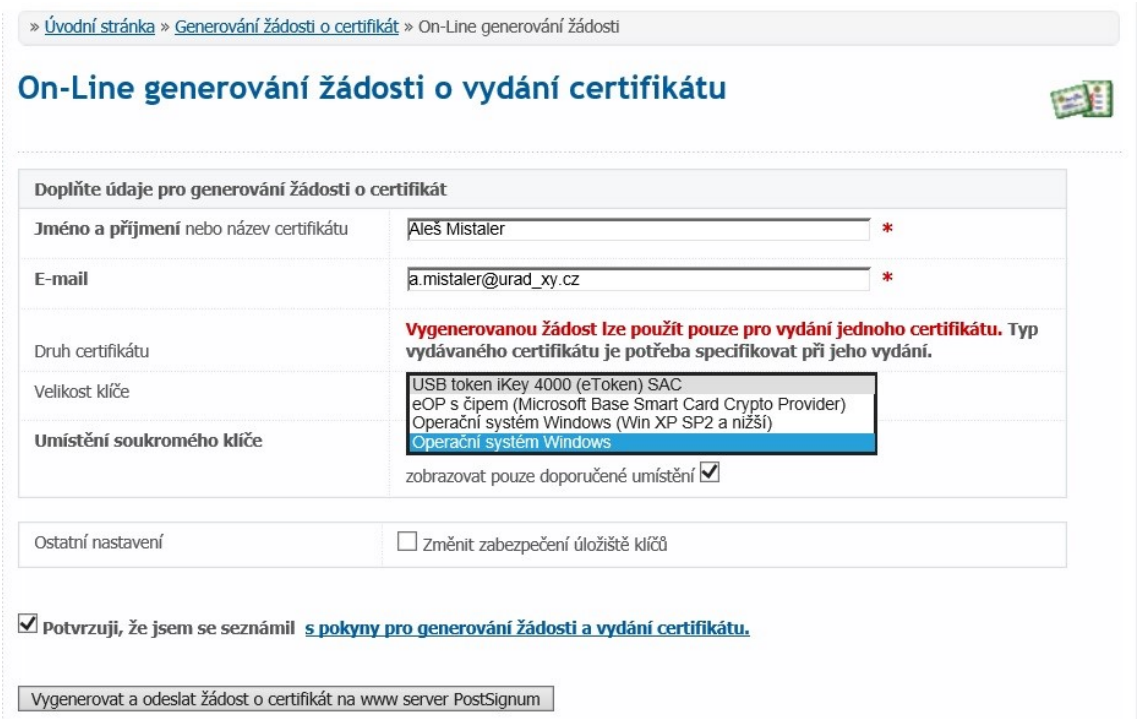
5.1 Generování žádosti o certifikát pro zaměstnance úřadu

Vše začíná požadavkem nadřízeného (ředitel odboru, vedoucí oddělení), zabezpečit pro jeho podřízeného zaměstnance elektronický podpis. V organizaci se rozjede proces, kdy osoba oprávněná jednat s certifikační autoritou z personálního oddělení získá údaje o zaměstnanci včetně rodného čísla zaměstnance (samozřejmě v souladu s GDPR). Na portálu akreditovaného poskytovatele certifikačních služeb ho zavede a zaměstnanci předá informaci, že si může vygenerovat certifikát. Tento postup platil před nařízením eIDAS a platí stále.

5.1.1 Generování žádosti před eIDAS

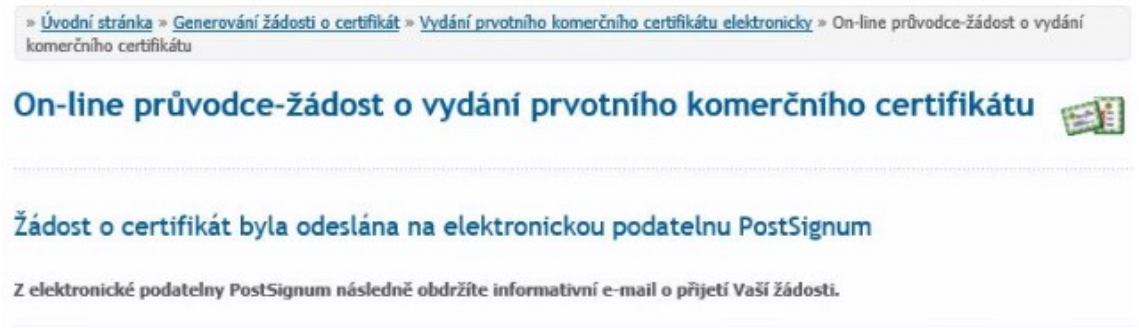
Dále zaměstnanec kontaktoval informatika s žádostí o vygenerování certifikátu. To se provádělo na webových stránkách PostSignum, v sekci úvodní stránka, generování žádosti o certifikát, On-Line generování žádosti o certifikát. Potom se vyplnilo jméno a příjmení, zaměstnanecký e-mail, jak je vidět na obrázku č. 4. Volba umístění soukromého klíče bylo možno vybrat Operační systém Windows, v tomto případě se certifikát nainstaloval do systému Windows na PC zaměstnance. Pokud se jako úložiště zvolil USB token iKey 4000 (eToken) SAC byl certifikát uložen na token. (Při používání tokenu iKey4000 musel být token před generováním žádosti zinicializován a musel na něm být nastaven PIN).

Obrázek 4: Výběr úložiště soukromého klíče[62]



Dále se zaškrtnul souhlas s potvrzením o pokynech pro generování žádosti a vydání certifikátu. A zvolena volba, vygenerovat a odeslat žádost o certifikát na www server PostSignum. Na další webové stránce PostSignum po „proklikání“ průvodcem

Obrázek 5: Zpráva odeslána na podatelnu Postsignum



generováním žádosti o certifikát se zobrazila informace o tom, že žádost byla odeslána na elektronickou podatelnu PostSignum. Poté následovala informace o zaslání informativního e-mailu o přijetí žádosti, to je vidět na obrázku č. 5. Následně do e-mailové schránky zaměstnance v řádu minut dorazilo oznámení o uložení žádosti o certifikát. Oznámení obsahovalo číslo ID žádosti a další pokyny k vyzvednutí certifikátu na pobočce České pošty obrázek č. 6.

[62] Vlastní zdroj

Obrázek 6: ID žádosti[63]


pá 02.03.2018 12:53

postsignum@cpost.cz

Oznameni o ulozeni zadosti o certifikat

Komu Mistaler Aleš

Podepsáno uživatelem Nastaly potíže s podpisem. Podrobnosti zobrazíte kliknutím na tlačítko podpisu.

request.req
Soubor: .req

Na server PostSignum byla uložena žádost o vydání certifikátu . Pro vystavení certifikátu je nutné se dostavit na pobočku České pošty se službou Czech POINT a při vydání certifikátu sdělit níže uvedené ID žádosti. Seznam poboček je uveden na webových stránkách PostSignum. S sebou na pobočku si vezměte doklad totožnosti (fyzické nepodnikající osoby dva doklady) a případně další požadované formuláře.

ID žádosti: 5612602512

Vygenerovanou žádost lze použít pouze pro vydání jednoho certifikátu. Pokud požadujete vydat více certifikátů, je nutno vygenerovat více žádostí.

Žádost o certifikát je přiložena zároveň k tomuto e-mailu. Na serveru bude uložena po dobu minimálně 30 dní.
Přiloženou žádost je možno využít pro vydání certifikátu, a to pokud by pracovník přepážky nedokázal najít žádost o certifikát dle předloženého ID. Je možné tedy přiložený soubor uložit na přenosné médium (USB disk) a předložit jej pracovníkovi přepážky pokud nebude schopen žádost o certifikát vyhledat na serveru dle předloženého ID (například po smazání žádosti na serveru).

Tímto je úkon generování žádosti o certifikát ukončen. Instalace vydaného certifikátu bude řešena později v jiné kapitole.

5.1.2 Výběr kvalifikovaných prostředků eIDAS

Před platností nařízení eIDAS bylo potřeba zajistit pro zaměstnance nové kvalifikované prostředky v souladu s platnou legislativou. Bývalé autorovo pracoviště používalo jako úložiště certifikátů operační systém Windows. Jen několik vedoucích pracovníků mělo token iKey4000 dále jen „**původní token**“. Nákup nových kvalifikovaných prostředků řešilo pomocí veřejné zakázky „Implementace centrálního řešení vzdáleného elektronického podpisu a pečetě podle nařízení eIDAS 2018“ https://zakazky.svscr.cz/contract_display_79.html. Název zakázky ukazuje, že toto řešení pokrývá elektronický podpis i elektronickou pečeť. Hardwarové řešení je zde modul HSM, které autor popisuje v kapitole „4.5 Úložiště certifikátů“. Na současném pracovišti bylo technické řešení jiné. V tomto případě šlo o přibližně stejný počet zaměstnanců cca 500. Vzhledem k tomu, že zde každý zaměstnanec vlastnil původní token, který byl využívaný hlavně v terénu (mimo kancelář), nebylo pochyb o stejném technickém řešení. To bylo realizováno nákupem 500ks kvalifikovaných prostředků Gemalto SaFeNet eToken 5110 CC včetně obslužného software u České pošty. http://www.postsignum.cz/etoken_5110_cc.html, dále jen „**token v souladu s eIDAS**“.

[63] Vlastní zdroj

Česká pošta tokeny před předáním předpřipravila - provedla záznam vnitřního sériového čísla prostředku a nahrála „servisní klíč“ autentizace prostředku.

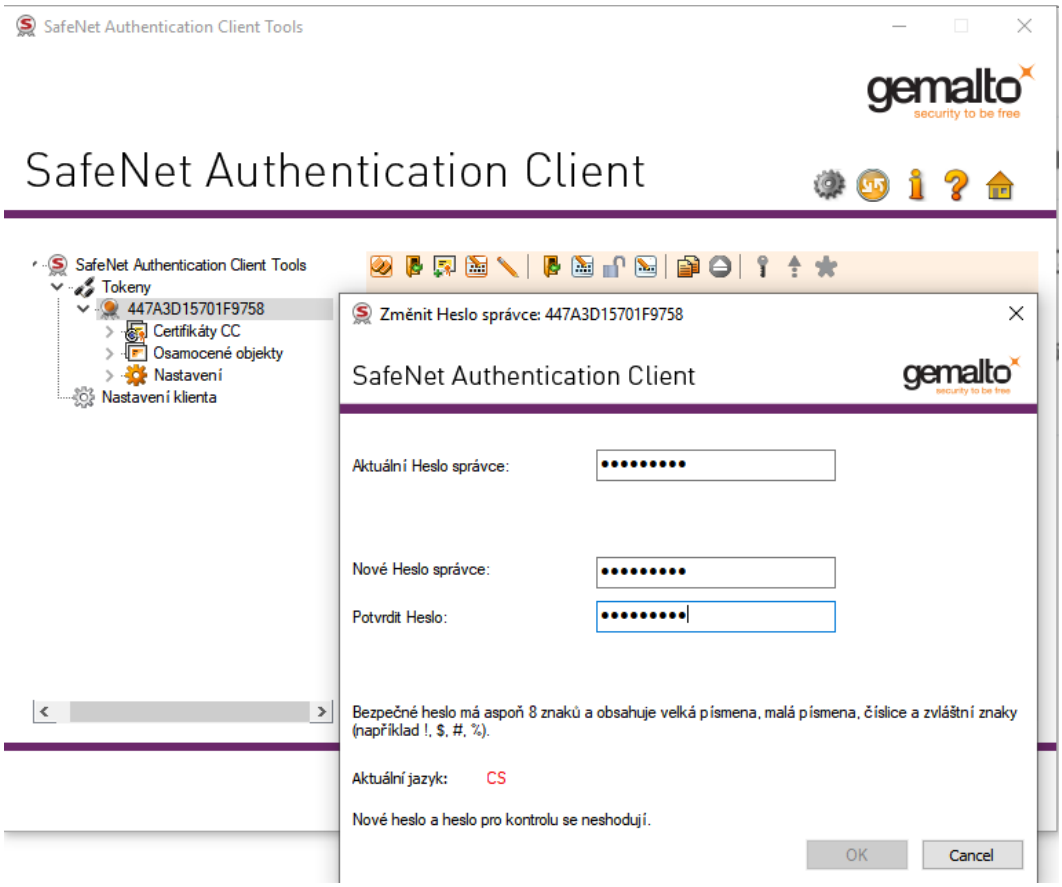
Později bylo dokoupeno pro potřeby ekonomického odboru 20ks USB TokenME včetně obslužného software http://www.postsignum.cz/etoken_5110_cc.html. Zaměstnancům z oddělení spisové služby a pracovníkům podatelen organizace byla koupena hlavně z důvodu používání elektronické pečetě k pečetění dokumentů čipová karta ProID+Q včetně čtečky a obslužného software http://www.postsignum.cz/proid_q.html. Před realizací nákupu si organizace ještě ujasňovala metodický postup formou dotazů na Ministerstvo vnitra ČR. A také si pozvala zástupce akreditované certifikační autority na schůzku ohledně přechodu na nové kvalifikované prostředky. Také byl nakoupen a vyzkoušen jeden testovací token, než se realizoval nákup 500ks.

K novým tokenům v souladu s eIDAS byla také dodána novější verze obslužného software (middleware) SafeNet Authentication Client verze 10.4. U původních tokenů byla dodána verze SafeNet Authentication Client verze 9.0. Verze 9.0 bohužel s tokeny v souladu s eIDAS nebyla kompatibilní a token nešel načíst, proto musela být na všech pracovních stanicích odinstalována. Po restartování pracovních stanic se nainstalovala nová softwarová verze 10.4, která je zpětně kompatibilní, takže umí pracovat i s původními tokeny.

5.1.3 Distribuce, popis a nastavení kvalifikovaných prostředků

Před předáním 500ks nových tokenů zaměstnancům bylo potřeba udělat seznam formou tabulky. V jednom sloupci bylo jméno zaměstnance v druhém sloupci sériové číslo tokenu ve třetím sloupci volné pole pro podpis zaměstnance a v posledním sloupci pole vrácení starého tokenu ano - ne. Várka 500ks byla rozdělena pro ústřední a regionální

Obrázek 7: Nastavení PUK[64]



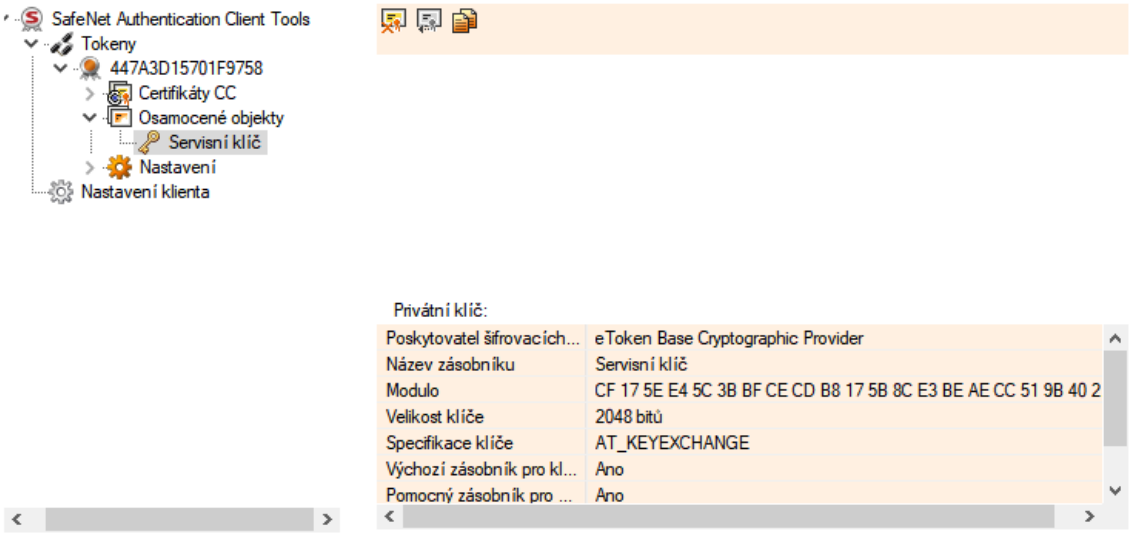
pracoviště přes příslušné informatiky. Další úkol čekal na informatiky v podobě nastavení hesla na tokenu v souladu s eIDAS, který je z výroby personalizován a obsahuje dvě oblasti, kvalifikovanou a veřejnou. Pro každou oblast je potřeba nastavit PIN a QPIN pro uživatele, PUK a QPUK pro správce. Standardně jsou hesla nastavena takto, pro uživatele: 12345678, pro správce: 87654321. Informatici přenastavili pouze heslo pro správce. Na obrázku č. 7 je vidět nastavení nového hesla správce, stejným způsobem se nastavují i ostatní hesla prostřednictvím horního panelu nad oknem změnit heslo správce viz obrázek č. 8.

Obrázek 8: Panel pro nastavení hesel[65]

Na obrázku č. 9 je vidět sériové číslo tokenu 447A3D15701F9758 a v osamocených objektech

[64] Vlastní zdroj
[65] Vlastní zdroj

Obrázek 9: Sériové číslo tokenu v souladu s eIDAS[66]



servisní klíč, to je zároveň veřejná část tokenu, kam se mohou instalovat nebo importovat ostatní certifikáty. Kvalifikovaná oblast je zobrazována v Certifikáty CC.

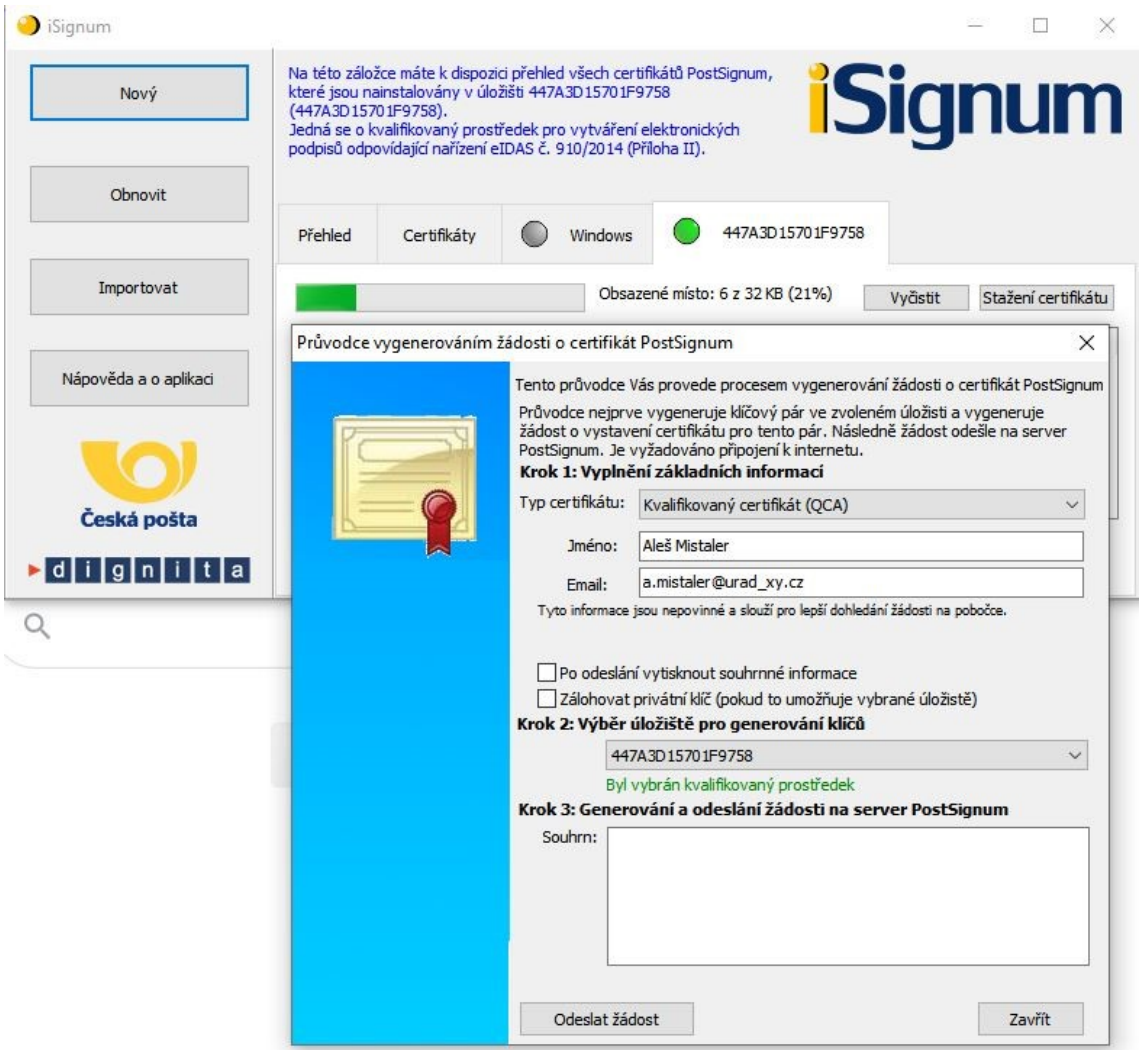
Takto nastavené tokeny byly připraveny pro nového žadatele o certifikát nebo pro obnovu certifikátu zaměstnance.

5.1.4 Generování žádosti po eIDAS

Po nabytí platnosti nařízení eIDAS již nelze generovat žádost o certifikát On-Line přes webové stránky Postsignum. Nyní k tomu slouží nástroj pro správu certifikátů iSignum, který je ke stažení zde http://www.postsignum.cz/programy_ke_stazeni.html. Po uložení aplikace iSignum.exe na lokální disk PC nebo notebooku uživatele, je možno aplikaci spustit. Předtím je ale potřeba připojit token v souladu s eIDAS do USB portu počítače a spustit obslužný software (middleware) tokenu SaFeNet Authentication Client a s uživatelem nastavit přístupové heslo k tokenu PIN a heslo k podpisu QPIN. To je uvedeno v podkapitole „5.1.3 Distribuce, popis a nastavení kvalifikovaných prostředků“. Pak už nic nebrání spuštění aplikace iSignum viz obrázek č. 10. Otevře se

[66] Vlastní zdroj

Obrázek 10: iSignum generování žádosti[67]



okno Průvodce vygenerováním žádosti o certifikát PostSignum. Vyplní se jméno, email a klikne se na, odeslat žádost. Následuje otevření oken se zadáním PINu a QPINu, po správném zadání se vygeneruje žádost o certifikát. ID žádosti je zasláno na mail žadatele.

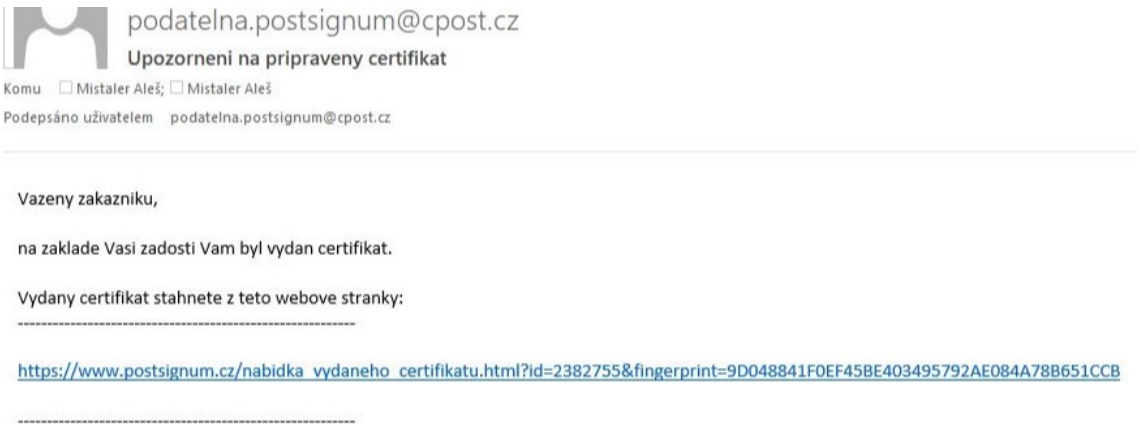
5.2 Instalace, obnova a zneplatnění certifikátu

5.2.1 Instalace, obnova a zneplatnění certifikátu před eIDAS

Instalace: do mailové schránky zaměstnance byl doručen mail o „*Upozornění na připravený certifikát*“ viz obrázek č. 11.

[67] Vlastní zdroj

Obrázek 11: Upozornění na připravený certifikát[68]



Po kliknutí na odkaz se načetla, stránka - Nabídka vydaného certifikátu viz obrázek č. 12. (použit z jiné nabídky certifikátu, kde jsou osobní údaje jiného zaměstnance zakryty červeně). Zde jsou k dispozici tři tlačítka. Protokol umožňoval stáhnout *protokol o vydání certifikátu*. Také bylo možné stáhnutí certifikátu ve *formátu DER* nebo *formátu PEM*.

Obrázek 12: Nabídka vydaného certifikátu[69]

Po potvrzení volby instalace vydaného certifikátu „instalaci certifikátu“ došlo k nainstalování certifikátu do úložiště certifikátů. To se určilo při umístění soukromého klíče obr. 4 v kapitole „5.1.1 Generování žádosti před eIDas“. Pak se postupovalo

[68] Vlastní zdroj
[69] Vlastní zdroj

dalšími potvrzovacími kroky, kdy se na konci objevilo oznámení „*Certifikát byl úspěšně nainstalován*“.

Obnovu certifikátu je nutno provádět v době platnosti expirujícího stávajícího certifikátu. Zaměstnanec obdrží informaci o blížícím se konci platnosti certifikátu do mailu. Tato informace je poslána certifikační autoritou 20 dní předem a pak 7dní předem. Obnova certifikátu se prováděla také na webových stránkách PostSignum, v sekci úvodní stránka, generování žádosti o certifikát, obnova certifikátu, On-line průvodce - žádost o vydání následného osobního certifikátu. V průvodci vydáním následného certifikátu se načetl a vybral certifikát s končící platností. Dále se odsouhlasily potvrzovací kroky a na konci se zobrazilo upozornění o úspěšné obnově certifikátu. Následně do mailové schránky zaměstnance v řádu minut bylo doručeno oznámení o požadavku obnovy certifikátu a po chvilce upozornění na nově vydaný certifikát. Pak se tento obnovený certifikát nainstaloval. V praxi se mnohokrát stalo, že zaměstnanci nenahlásili informatikovi požadavek o obnovu certifikátu a ten vypršel (vyexpiroval). V tomto případě byl stejný postup jako při vydání nového certifikátu. Pro zaměstnance to znamenalo, že musel znovu po jednom roce opět navštívit pobočku České pošty.

Zneplatnění certifikátu tzv. revokace se provádí v době, kdy je certifikát platný. Většinou v situacích při ukončení pracovního poměru, zařazením na jiné pracovní místo, změnou příjmení nebo jiných změnových údajů. Velkou roli, zde opět hraje osoba oprávněná jednat s certifikační autoritou. Po přihlášení se na zákaznický portál autority, může zneplatnit certifikát zaměstnance. Dále může dotčeného zaměstnance zablokovat. U jiných zaměstnanců může měnit údaje v podobě změn příjmení, pracovního zařazení atd. Vrácený token se předá informatikovi, ten z něj odstraní starý certifikát a připraví token pro nového zaměstnance.

5.2.2 Instalace, obnova a zneplatnění certifikátu po eIDAS

Instalace a **obnova** certifikátu je obdobná jako obnova certifikátu v přechodném období, která je detailně popsána v kapitole „5.3 Obnova certifikátu v přechodném období eIDAS“. Rozdíl je jen v tom, že zde již nefiguruje původní token a vše se realizuje na novém tokenu v souladu s eIDAS.

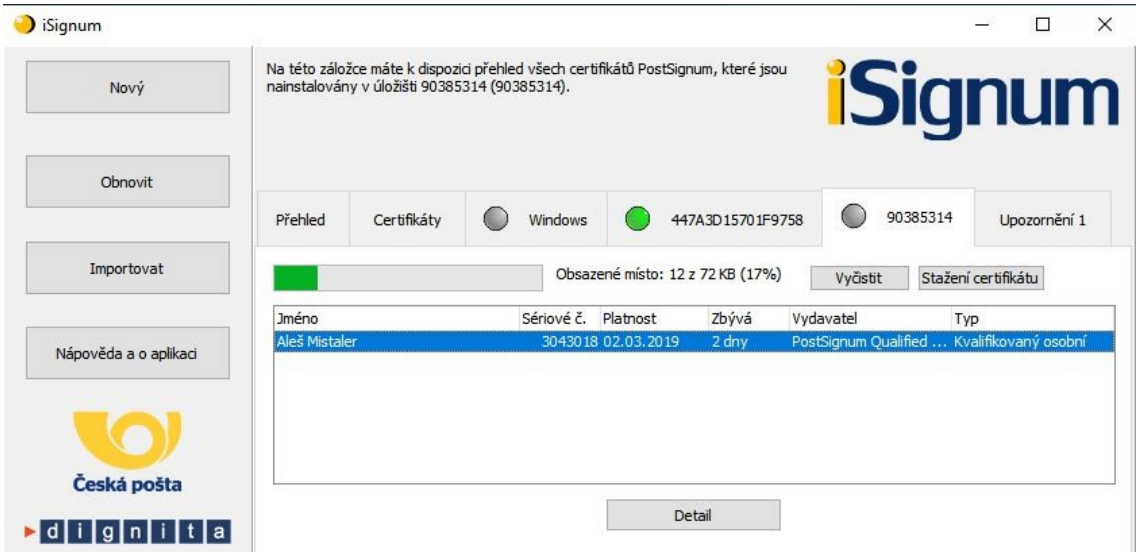
Zneplatnění je stejné, jako je uvedeno v podkapitole „5.2.1 Instalace, obnova a zneplatnění certifikátu před eIDAS“. Rozdílné je pouze to, že u tokenu v souladu s eIDAS vzniká vazba token – žadatel. O tom je psáno v kapitole“ 4.7 Elektronický

podpis dle eIDAS“. Důležitou roli zde opět má osoba oprávněná jednat s certifikační autoritou. V tom smyslu, že pošle email podepsaný svým kvalifikovaným elektronickým podpisem akreditované certifikační autoritě. Obsahem mailu je žádost o zrušení vazby token – žadatel. Bez zrušení vazby token-žadatel by nebylo možné token v souladu s eIDAS používat jiným zaměstnancem.

5.3 Obnova certifikátu v přechodném období eIDAS

Do 19.09.2018 museli mít všichni zaměstnanci obnoven certifikát na novém kvalifikovaném prostředku tokenu v souladu s eIDAS. Tento proces přecházení znamenal nastavit dvě nová uživatelská hesla k novému tokenu. Připojit současně do dvou USB portů PC nebo notebooku původní token a token v souladu s eIDAS. Dále přes obslužný software tokenu v souladu s eIDAS provést obnovu certifikátu. Volilo se mezi dvěma variantami. První varianta byla ta, že se obnova bude provádět na jednom notebooku v kanceláři, kam budou postupně chodit všichni zaměstnanci. Druhá varianta byla ta, že informatici budou obcházet jednotlivé zaměstnance v jejich kancelářích. Byla vybrána varianta číslo dvě. V příkladu je ukázána přímo autorova obnova, tak jak se řešila v přechodném období nařízení eIDAS. První krok je nastavení hesel nového tokenu, to je vysvětleno v podkapitole „5.1:3 Distribuce, popis a nastavení kvalifikovaných prostředků“. Obnova začíná spuštěním aplikace iSignum. Na obrázku č. 13 je vidět připojený původní token šedý „*puntík*“ číslo 90385314 a na něm je certifikát autora, který

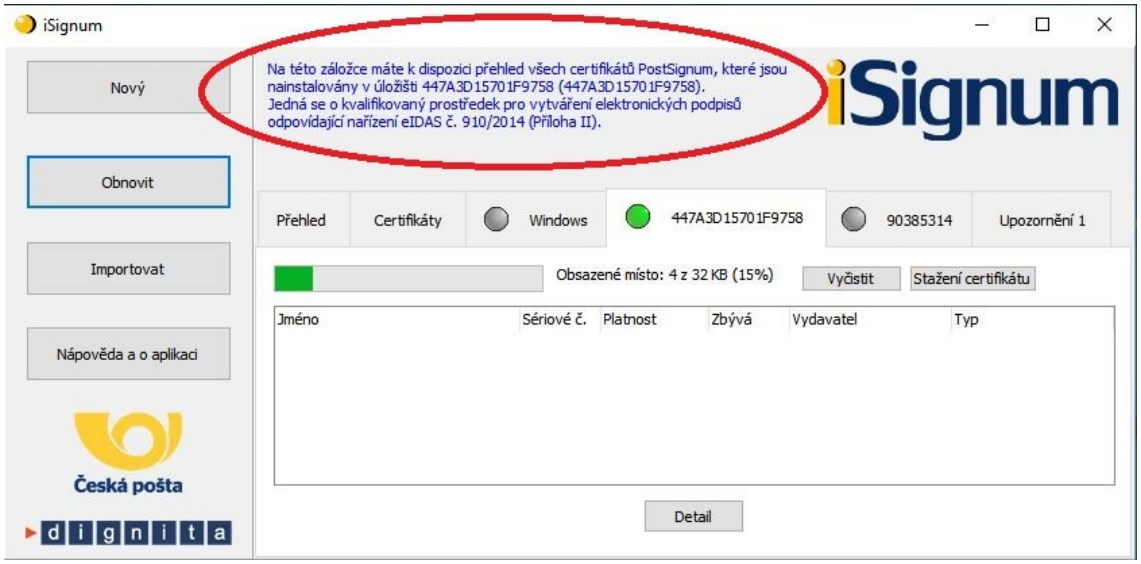
Obrázek 13: Certifikát umístěný na původním tokenu[70]



[70] Vlastní zdroj

vyprší za 2 dny. Následuje přepnutí na token v souladu s eIDAS zelený „*puntík*“ viz obrázek č. 14. Na tokenu v souladu s eIDAS není nainstalován žádný certifikát. Dále se klikne zpět na původní token, vybere se certifikát a následně klikne na tlačítko obnovit

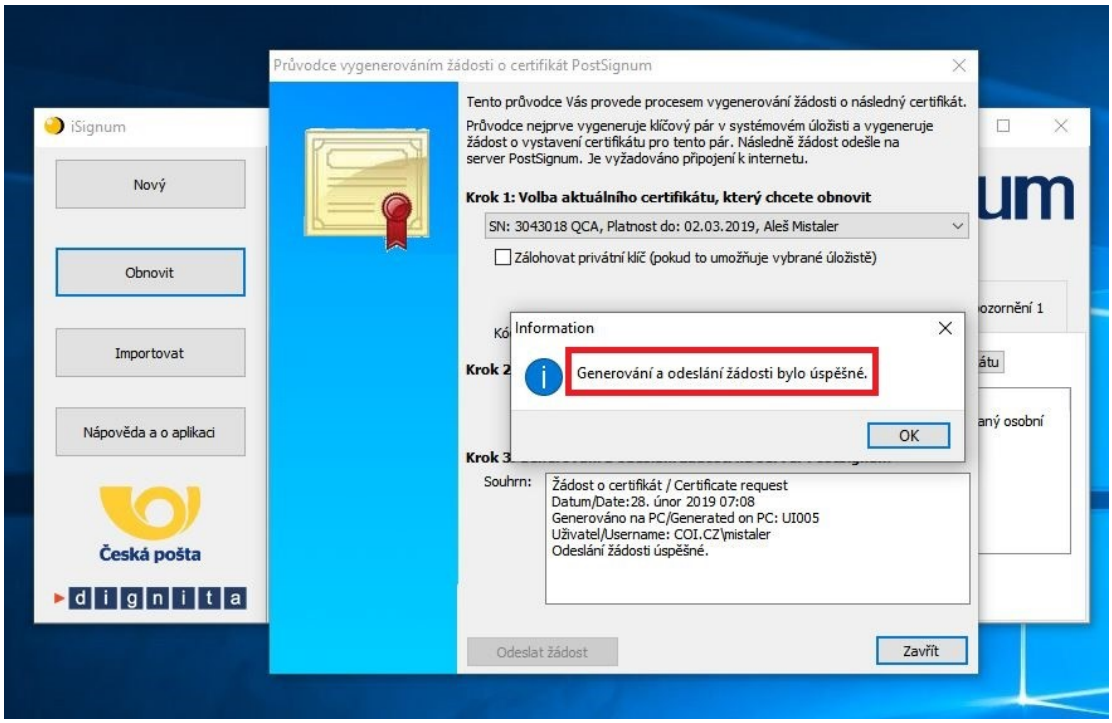
Obrázek 14: Prázdný nový token v souladu s eIDAS[71]



v modrém rámečku na obrázku č. 14. Tímto krokem začíná generování žádosti o obnovu certifikátu na token v souladu s eIDAS. Tato operace je zabezpečena přístupem k tokenům, takže postupně vyžaduje PIN původního tokenu, PIN pro přístup k tokenu v souladu s eIDAS a Digital Signature PIN pro přístup do kvalifikované části tokenu v souladu s eIDAS. Výsledek je vidět na obrázku č. 15 „*Generování a odeslání žádosti bylo úspěšné*“.

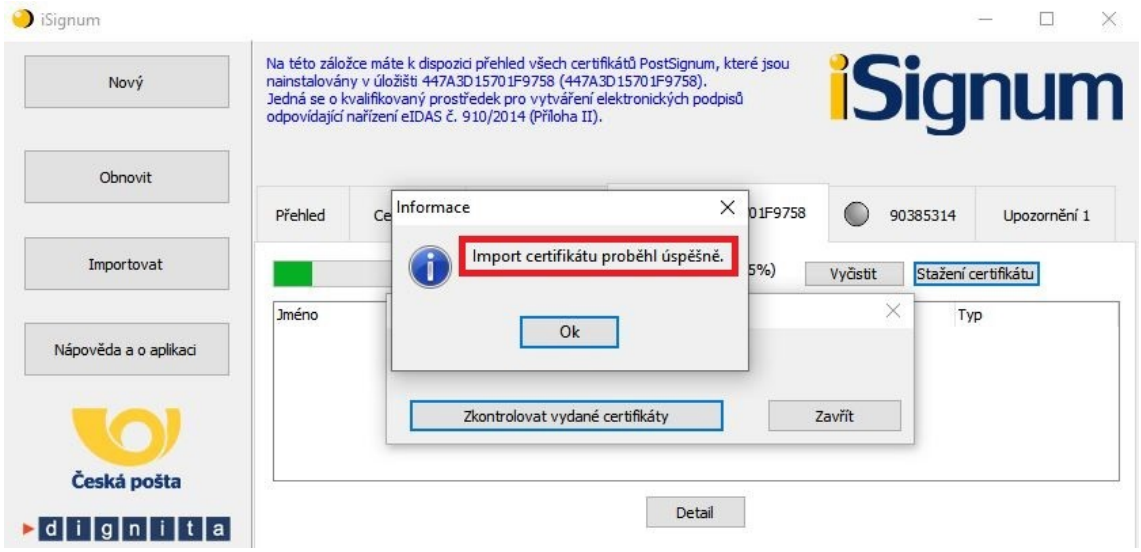
[71] Vlastní zdroj

Obrázek 15: Generování žádosti token v souladu s eIDAS[72]



Nyní se opět čeká na zprávu od podatelna.postsignum@cpost.cz. První přijde informace o doručení žádosti, poté upozornění na připravený certifikát. Dále se v iSignum přepne na token v souladu s eIDAS, klikne se na tlačítko „*stažení certifikátu*“, dále na „*zkontrolovat vydané certifikáty*“ a potvrdí volba „*import certifikátu*“. Po zadání PINu je

Obrázek 16: Import certifikátu na token v souladu s eIDAS[73]

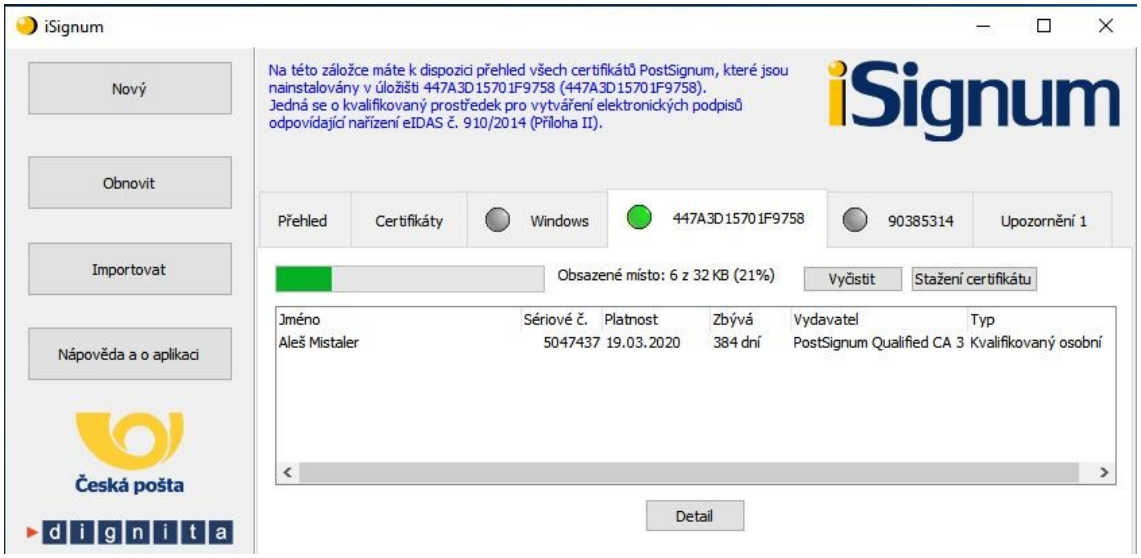


vidět výsledek na obrázku č. 16 „Import certifikátu proběhl úspěšně“.

[72] Vlastní zdroj
[73] Vlastní zdroj

V aplikaci iSignum se opět přepneme na token v souladu s eIDAS. Na obrázku č. 17 je vidět již autorův nový kvalifikovaný certifikát, který má platnost 384 dní a je nahrán na kvalifikovaném prostředku odpovídající nařízení eIDAS č. 910/2014 (Příloha II).

Obrázek 17: Nový certifikát na tokenu v souladu s eIDAS[74]

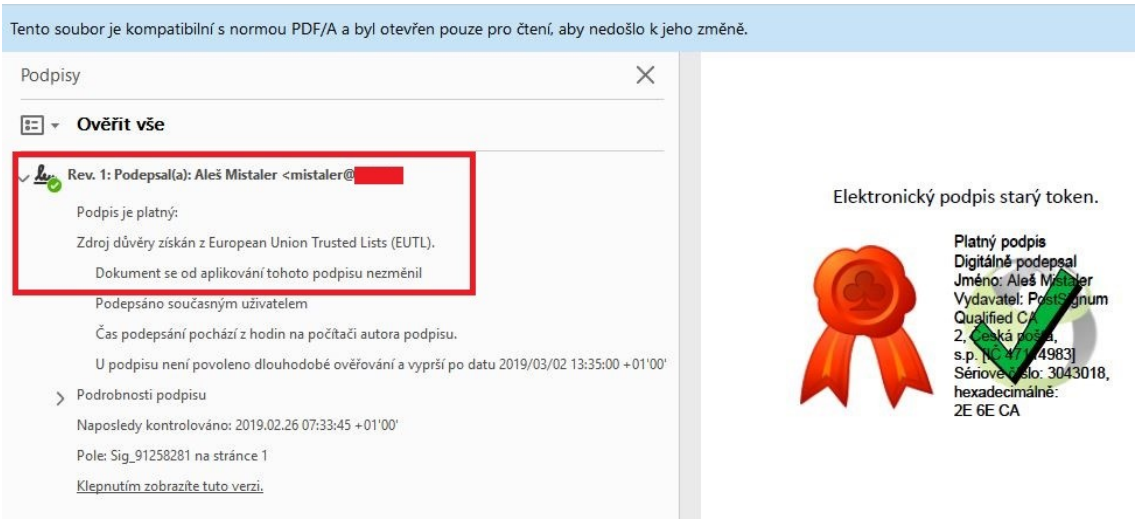


5.4 Rozdíly ve vlastnostech podepsaného elektronického dokumentu

V této kapitole autor poukáže na rozdíly ve vlastnostech podepsaného elektronického dokumentu. Dokumenty byly podepsány certifikátem uloženým na původním tokenu a kvalifikovaným certifikátem na token v souladu s eIDAS. K vytvoření elektronického dokumentu byla použita aplikace Microsoft Office Word 2016. Z ní byl soubor uložen do PC s příponou PDF. K podepsání elektronického dokumentu byla použita aplikace Software602 Print2PDF. Vlastnosti elektronicky podepsaného dokumentu jsou zobrazovány v Adobe Acrobat Readeru DC. Na obrázku č. 18 je vidět snímek z elektronicky podepsaného dokumentu původním tokenem, bylo využito tzv. viditelného podpisu, to je vidět v pravé části obrázku. Na levé straně v červeném rámečku je informace, že je podpis platný a byl ověřen na EU Trusted listu.

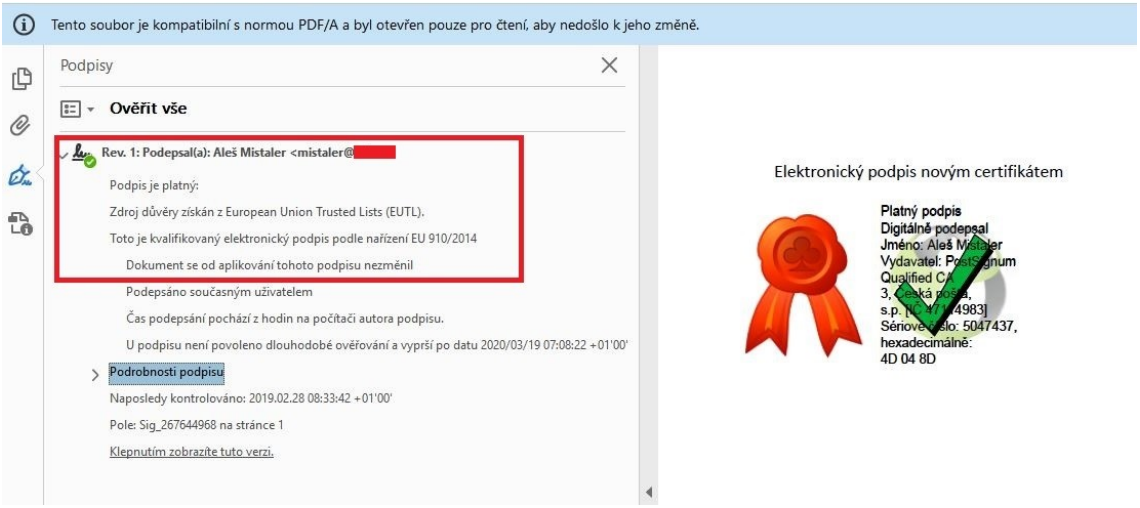
[74] Vlastní zdroj

Obrázek 18: Podepsání dokumentu původním tokenem[75]



Na obrázku č. 19 je snímek z elektronicky podepsaného dokumentu novým tokenem,

Obrázek 19: Podepsání dokumentu tokenem v souladu s eIDAS[76]

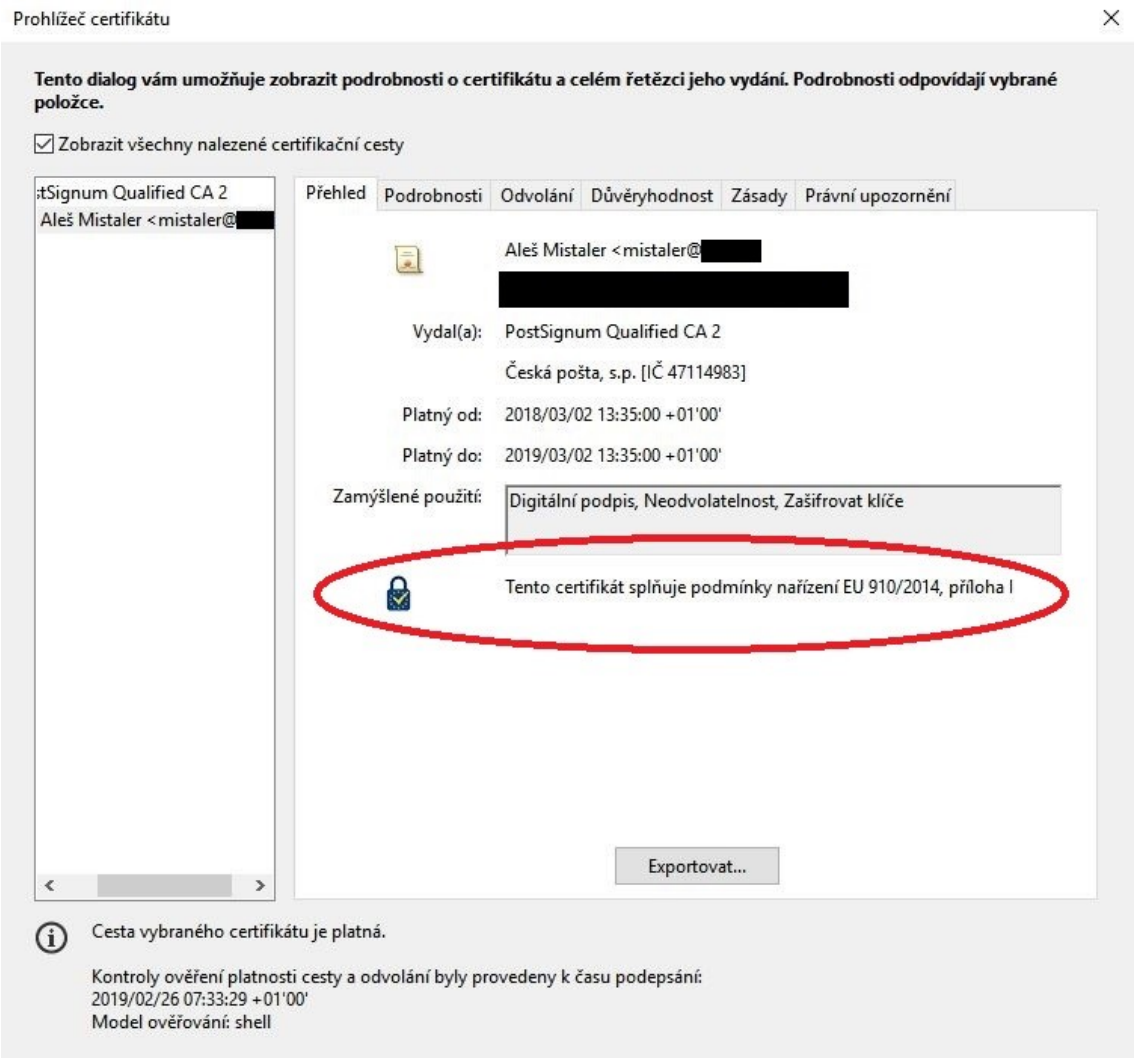


v pravé části obrázku, je vše obdobné jako na předchozím obrázku. Rozdíly jsou jen v sériovém čísle certifikátu, z toho vyplývá, že byl každý dokument podepsán jiným certifikátem jednoho autora. Další změna, která je vidět je u vydavatele certifikátu PostSignum Qualified CA 2 oproti PostSignum Qualified CA 3. Na levé straně v červeném rámečku je opět vše stejné až na „**Toto je kvalifikovaný elektronický podpis podle nařízení EU 910/2014**“. Další variantou v Adobe Acrobat Readeru DC je v prohlížeči certifikátů karta „Přehled“. Na obrázku č. 20 je vidět snímek z elektronicky

[75] Vlastní zdroj
[76] Vlastní zdroj

podepsaného dokumentu původním tokenem. V červené elipse je vidět, že tento certifikát splňuje podmínky nařízení EU 910/2014, příloha I.

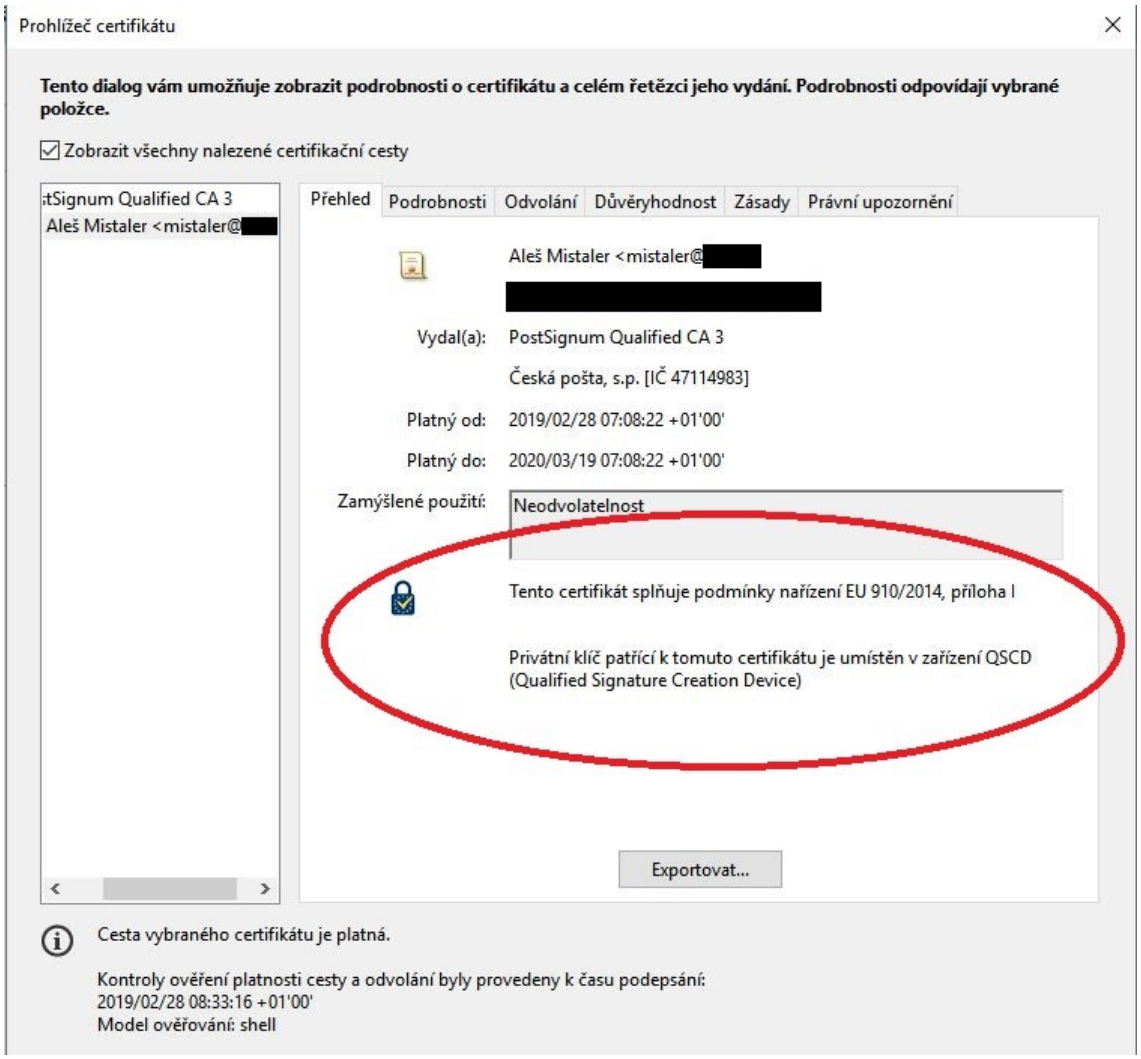
Obrázek 20: Adobe karta přehled původní token[77]



Na obrázku č. 21 je vidět ten samý snímek z elektronicky podepsaného dokumentu tokenem v souladu s eIDAS. V prohlížeči certifikátů na kartě „Přehled“ jsou opět vidět téměř shodné údaje.

[77] Vlastní zdroj

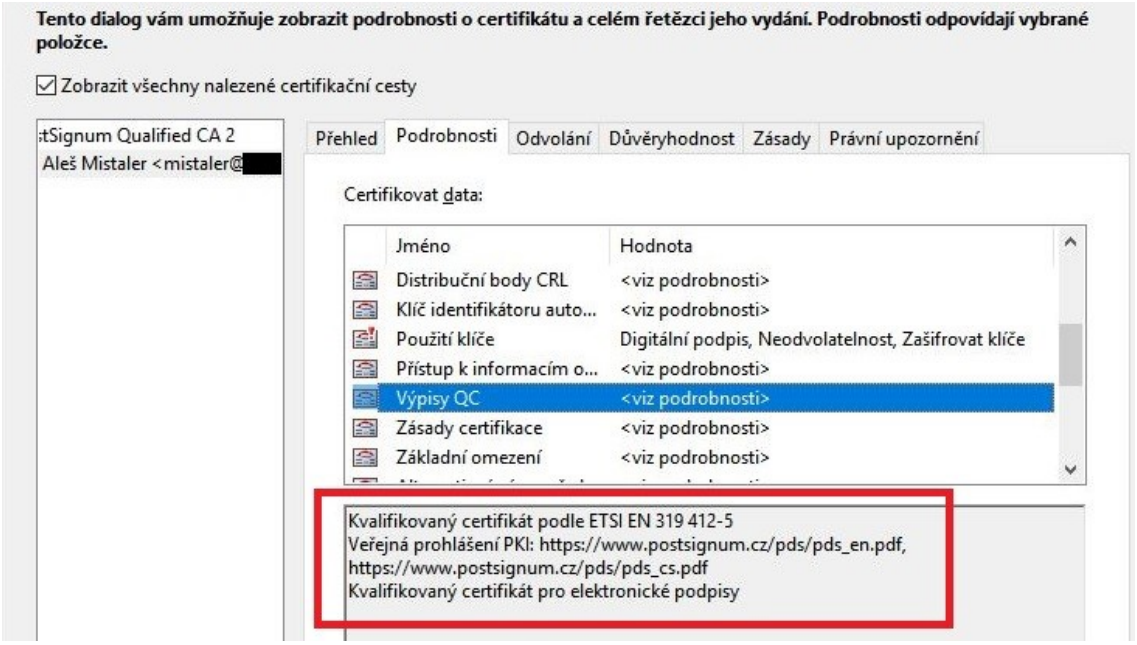
Obrázek 21: Adobe karta přehled token v souladu s eIDAS[78]



V červené elipse je navíc „**Privátní klíč patřící k tomuto certifikátu je umístěn v zařízení QSCD (Qualified Signature Creation Device)**“. Znovu je vidět změna u vydavatele certifikátu PostSignum Qualified CA 2 oproti PostSignum Qualified CA 3. Do třetice se podíváme v Adobe Acrobat Readeru DC v prohlížeči certifikátů karta „Podrobnosti“. Na obrázku č. 22 je vidět snímek z elektronicky podepsaného dokumentu původním tokenem. V podrobnostech „Výpisy QC“ je červeně orámováno: kvalifikovaný certifikát podle ETSI EN 319 412-5, veřejná prohlášení o PKI a kvalifikovaný certifikát pro elektronické podpisy.

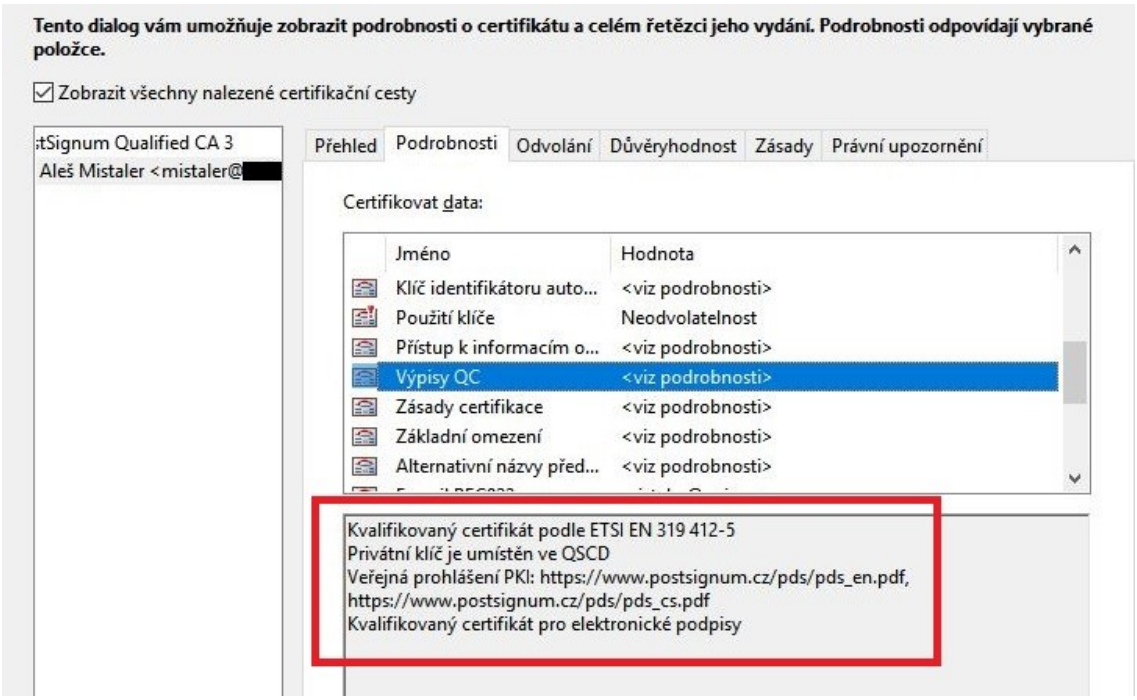
[78] Vlastní zdroj

Obrázek 22: Adobe karta podrobnosti původní token token[79]



Na obrázku č. 23 je opět ten samý snímek z elektronicky podepsaného dokumentu tokenem v souladu s eIDAS s téměř totožnými údaji.

Obrázek 23: Adobe karta podrobnosti token v souladu s eIDAS[80]



V podrobnostech „Výpisy QC v červeném orámování je zobrazeno navíc „**Privátní klíč**

[79] Vlastní zdroj
[80] Vlastní zdroj

je umístěn ve QSCD“ V levém horním rohu jsou rozdílní vydavatelé certifikátu PostSignum Qualified CA 2 oproti PostSignum Qualified CA 3.

Z uvedených příkladů je patrné, že rozdíly jsou minimální. Pro běžného uživatele je velmi obtížné rozeznat, zda jde o kvalifikovaný certifikát umístěný na kvalifikovaném prostředku dle nařízení eIDAS.

Závěr

Tato bakalářská práce popisuje a řeší elektronické podepisování ve veřejné správě. Zde se již od samého počátku propojuje oblast legislativní s oblastí informačních technologií. Toto spojení spolu funguje dvacet let a za tu dobu prošlo velkým vývojem. Za klíčové můžeme jednoznačně považovat „Nařízení Evropského parlamentu a Rady (EU) č. 910/2014“, o elektronické identifikaci a službách vytvářejících důvěru (zkráceně eIDAS). Podle něj lze rozdělovat elektronické podepisování dokumentů před jeho platností a po nabytí jeho účinnosti.

Hlavní rozdíl „před eIDAS“ byl v tom, že certifikát zaměstnance mohl být nainstalovaný v PC v operačním systému Windows na čipové kartě či tokenu. Ve všech případech šlo certifikát zálohovat (vyexportovat). To v praxi znamenalo, že pokud se musel počítač přeinstalovat (zavést nový operační systém) šlo zpětně ze zálohy certifikát k podpisu znovu nahrát do PC. To samé platilo v případě, kdy došlo k poškození či ztrátě tokenu, tak na nový token šel znovu nahrát (obnovit) certifikát ze zálohy. Také pokud zapomněl uživatel heslo k tokenu, stačilo „zinicializovat“ token, tím došlo k jeho naformátování – obnova do výchozího stavu a znovu ze zálohy naimportovat certifikát na token. Legislativa založená na směrnici EU 1999/93/EC pro elektronické podpisy požadovala používání bezpečných prostředků pro vytváření elektronických podpisů jako nejvyšší a právně závazné formy elektronických podpisů. Tato směrnice sice byla transponována do české národní legislativy formou zákona č. 227/2000 Sb., o elektronickém podpisu, nicméně v té době Česká republika ještě nebyla v EU, šla jinou cestou a rozhodlo se u nás (čipové karty/tokeny) po uživatelích nevyžadovat. Nejvyšší formou elektronického podpisu byl uznávaný elektronický podpis nevyžadující použití bezpečného klíče. V této době byla osvěta kolem elektronických podpisů mizivá, soukromý klíč nebyl uchováván bezpečně a často nechráněn, tudíž snadno zneužitelný. Jeho legislativní platnost jako ekvivalent k vlastnoručnímu podpisu byla alespoň akceptována vnitrostátně v rámci České republiky.

Oproti tomu nařízení eIDAS je svou povahou přímo aplikovatelné ve všech členských státech EU. Klade si za cíl vytvoření jednotného kybernetického prostoru v celé EU, v němž si úřady a jednotlivci budou předávat důvěryhodné elektronické dokumenty a kde budou odstraněny překážky fungování elektronických podpisových

nástrojů v celé EU. A také, zde budou platit jednotná pravidla pro práci s nimi. Právní vymahatelnost aktů prováděných digitálně bude potvrzena legislativně. „*Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu*.“ Daleko výrazněji je také kladen důraz na důvěryhodnost a bezpečnost, s tím jsou spojené i vysoké nároky na kvalifikované prostředky. Před 19.09.2018 se tedy musely začít řešit změny na požadavky úložišť certifikátů. Autorovo pracoviště šlo nejsnadnější cestou nákupem kvalifikovaných prostředků „tokenů“ u certifikační autority, u které má i smlouvu o dodávání akreditovaných certifikačních služeb včetně nových kvalifikovaných certifikátů. Z těchto důvodů byl i snadný přechod na nové tokeny spolu s obnovou stávajících certifikátů v souladu s eIDAS a nebyl problém realizovat tuto variantu u stovky zaměstnanců v poměrně krátkém čase. Bezpečnost nových tokenů je v první řadě vázána na jméno zaměstnance a certifikát se generuje přímo na tokenu a nejde zálohovat (vyexportovat). Také při ztrátě či poškození tokenu je nepoužitelný i při ztrátě hesel PIN a PUK je token zablokován a dojde ke znehodnocení prostředku.

V jednom ze svých článků „seriál eIDAS“ na Lupa.cz přední odborník na elektronické podpisy pan Jiří Peterka klade otázky typu - „Elektronické podpisy: v září 2018 skončí výjimka, budou úředníci připraveni? Už od září bude veřejná správa potřebovat certifikované čipové karty či USB tokeny a také nové certifikáty pro kvalifikované podpisy. Stihne vše pořídit včas?“

Autor práce odpovídá: ano, pane Peterko, úředníci byli připraveni a vše včas stihli!

Seznam použitých zdrojů

Literární zdroje

1. ARCHIVNICTVÍ A SPISOVÁ SLUŽBA, *Skartační řízení : zákon, vyhlášky, nařízení vlády.* Ostrava : Sagit, 2012. ÚZ. 112s. ISBN 978-80-7208-939-0
2. BÍLÝ, J. *Základy společenských věd IV*. Ostrava : Key Publishing, 2009. 157s. ISBN 978-80-7418-015-6
3. BOSÁKOVÁ, D. et al. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* Olomouc : ANAG, 2002. 141s. ISBN 80-7263-125-x
4. DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2. vyd. Brno : COMPUTER PRESS, 2009. 536s. ISBN 978-80-251-2619-6
5. FEREBAUEROVÁ, R., PEKÁREK, O. *Aplikovaná informatika.* České Budějovice: Vysoká škola evropských a regionálních studií, 2014, 151s. ISBN 978-80-87472-74-3
6. INFORMACE, INFORMATIKA, eGOVERNMENT, *Svobodný přístup k informacím, ochrana osobních údajů, elektronický podpis, elektronické komunikace, elektronické úkony a konverze dokumentů, informační systémy veřejné správy, kybernetická bezpečnost, základní registry.* Ostrava : Sagit, 2014. ÚZ. 432s. ISBN 978-80-7488-183-1
7. MATES, P., SMEJKAL, V. *E-government v českém právu.* Praha : Linde, 2006. 235s. ISBN 80-7201-614-8
8. PETERKA, J. *Báječný svět elektronického podpisu*. Praha : CZ.NIC, 2011. 429s. ISBN 978-80-904248-3-8
9. SMEJKAL, V. *Datové schránky v právním řádu ČR: zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, s komentářem.* Praha : ABF, 2009. 176s. ISBN 978-80-86284-78-1
10. ŠPAČEK, D. *EGovernment cíle, trendy a přístupy k jeho hodnocení.* Praha : C.H. Beck, 2012. 258s. ISBN 978-80-7400-261-8

Elektronické zdroje

1. PETERKA, J. *Jaké bude nové ministerstvo informatiky?* [online]. eArchiv.cz, 2002 [cit. 2019-06-20]. Dostupné z WWW: <http://www.earchiv.cz/b02/b0925001.php3>.

2. KÁLAL, J. *Ministerstvo informatiky už je minulostí* [online]. Lupa.cz, 2007 1. června [cit. 2019-06-20]. Dostupné z WWW: <https://www.lupa.cz/clanky/ministerstvo-informatiky-uz-je-minulosti/>.
3. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. ARCHIV. *Informace o zřízení elektronických podatelen u orgánů veřejné moci* [online]. MVČR, © 2019 [cit. 2019-06-20]. Dostupné z WWW: <https://www.mvcr.cz/clanek/informace-o-zrizeni-elektronickych-podatelen-u-organu-verejne-moci.aspx>.
4. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. EGOVERNMENT. *Alternativní navigace* [online]. MVČR, © 2019 [cit. 2019-06-27]. Dostupné z WWW: <https://www.mvcr.cz/egovernment.aspx>.
5. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. PROJEKTY. *eGON* [online]. MVČR, © 2019 [cit. 2019-06-28]. Dostupné z WWW: <https://www.mvcr.cz/clanek/egon-66.aspx>.
6. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Registr smluv* [online]. MVČR, © 2019 [cit. 2019-06-29]. Dostupné z WWW: <https://www.mvcr.cz/clanek/registr-smluv.aspx>.
7. REDAKCE, Finance.CZ. *eObčanka aneb má Česko konečně nakročeno do 21. století?* [online]. Mladá fronta a. s., © 2018. 11. července [cit. 2019-06-29]. Dostupné z WWW: <https://www.finance.cz/512161-eobcanka/>.
8. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. ZPRAVODAJSTVÍ. *První krok k efektivně sdíleným ICT službám státu v eGovernment cloudu* - Ministerstvo vnitra České republiky. [online]. MVČR © 2019 [cit. 2019-08-14]. Dostupné z: <https://www.mvcr.cz/clanek/prvni-krok-k-efektivne-sdilenym-ict-sluzbam-statu-v-egovernment-cloudu.aspx>.
9. PETERKA, J. *Český eGovernment v roce 2018* [online]. eArchiv.cz, 2019 [cit. 2019-08-29]. Dostupné z WWW: <http://www.earchiv.cz/b19/b0102001.php3>.
10. EARCHIVACE.CZ, Elektronická archivace, *Písemný vs. elektronický dokument* [online]. © 2014 eArchivace [cit. 2019-09-27]. Dostupné z WWW: <http://www.earchivace.cz/elektronicka-archivace/pisemny-vs-elektronicky-dokument/>.
11. EUR-LEX.EUROPA.EU, *Access to European Union law* [online]. © 2019 [cit. 2019-12-20]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A31999L0093>.

12. UREŠ, M. *eIDAS: pád digitální zdi v Evropě* [online]. CCB spol. s.r.o., 2001 - 2019 [cit. 2019-12-20]. Dostupné z WWW: <https://www.systemonline.cz/sprava-it/eidas-pad-digitalni-zdi-v-evrope.htm>.
13. ZÁKONY PRO LIDI.CZ, *Zákon č. 227/2000 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-12-20]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2000-227>.
14. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor Hlavního architekta eGovernment, Archiv, *Zákon č. 227/2000 Sb., o elektronickém podpisu* [online]. MVČR, © 2012. 1. října [cit. 2019-10-30]. Dostupné z WWW: <https://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.
15. EUR-LEX.EUROPA.EU, *Access to European Union law* [online]. © 2019 [cit. 2019-12-29]. Dostupné z WWW: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>.
16. PRVNÍ CERTIFIKAČNÍ AUTORITA, *Novinky* [online]. První certifikační autorita, a.s. (I.CA) © 2019. 1. ledna [cit. 2019-12-30]. Dostupné z WWW: <https://www.ica.cz/novinky?IdNews=434>.
17. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor eGovernmentu, *Služby vytvářející důvěru a elektronická identifikace.* [online]. MVČR, © 2019. 17. března [cit. 2019-12-30]. Dostupné z WWW: <https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx>.
18. MUNIS, informační systém pro města a obce, *Nařízení eIDAS se znovu připomíná.* Praha [online]. © 2019 Triada, spol. s.r.o., [cit. 2019-11-18]. Dostupné z WWW: <https://www.munis.cz/art/548>.
19. ZÁKONY PRO LIDI.CZ, *Zákon č. 297/2016 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-11-18]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2016-297>.
20. PETERKA, J. Lupa.cz, *Po 16 letech existence přestává platit zákon o elektronickém podpisu* [online]. © 1998-2019 Lupa.cz, 2016. 19. září [cit. 2019-11-19]. Dostupné z WWW: <https://www.lupa.cz/clanky/po-16-letech-existence-prestava-platit-zakon-o-elektronickem-podpisu/>.
21. ZÁKONY PRO LIDI.CZ, *Zákon č. 250/2017 Sb.* [online]. AION CS, s.r.o. © 2010 - 2019 [cit. 2019-11-22]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2017-250>.

22. PEŠEK, M. ředitel Správy základních registrů, *Národní bod pro identifikaci a autentizaci* [online]. CCB spol. s.r.o. 2018. 19. září [cit. 2019-11-23]. Dostupné z WWW: <http://m.systemonline.cz/it-security/narodni-bod-pro-identifikaci-a-autentizaci.htm>.
23. POSTSIGNUM, Postup pro získání certifikátu, *Fyzické osoby* [online]. Česká pošta © 2010 [cit. 2019-10-29]. Dostupné z WWW: <http://www.postsignum.cz/fyzicke_osoby.html>.
24. POSTSIGNUM, Postup pro získání certifikátu, *Firmy, organizace, veřejná správa* [online]. Česká pošta © 2010 [cit. 2019-10-29]. Dostupné z WWW: <http://www.postsignum.cz/firmy_organizace_verejna_sprava.html>.
25. EARCHIVACE.CZ, Technologie, *Digitální podpis* [online]. © 2014 eArchivace [cit. 2019-09-30]. Dostupné z WWW: <http://www.earchivace.cz/technologie/digitalni-podpis/>.
26. BIOMETRICKÝ PODPIS, *Co je biometrický podpis* [online]. Contrisys, s.r.o. © 2012 [cit. 2019-10-10]. Dostupné z WWW: <http://www.contrisys.com/co-je-biometricky-podpis>.
27. PRVNÍ CERTIFIKAČNÍ AUTORITA, *Komerční certifikát* [online]. První certifikační autorita, a.s. (I.CA) © [cit. 2019-10-29]. Dostupné z WWW: <https://www.ica.cz/Komercni-certifikat>.
28. PETERKA, J. Lupa.cz, *eIDAS: Elektronické značky a pečetě a rekviem za datovou zprávu* [online]. © 1998-2019 Lupa.cz, 2016. 4. července [cit. 2019-10-30]. Dostupné z WWW: <https://www.lupa.cz/clanky/eidas-elektronicke-znacky-a-pecete-a-rekviem-za-datovou-zpravu/>.
29. HUMPOLEC, J. *Elektronické časové razítko jako doplněk elektronického podpisu* [online]. © 1996-2019 Economia, a. s., 2008. 5. května 11:15 [cit. 2019-10-30]. Dostupné z WWW: <https://tech.ihned.cz/c1-24518930-elektronicke-casove-razitko-jako-doplnek-elektronickeho-podpisu>.
30. ČESKÁ POŠTA, Služby, *Časová razítka*. [online]. © 2018 [cit. 2019-10-31]. Dostupné z WWW: <https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka>.
31. JELÍNEK, M. *Autentizační tokeny v praxi* [online]. CCB spol. s.r.o., © 2001-2019 [cit. 2019-10-31]. Dostupné z WWW: <https://www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm>.
32. ASKON.CZ. *HSM moduly* [online]. ASKON INTERNATIONAL s.r.o., © 2019 [cit. 2019-10-10]. Dostupné z WWW: <http://www.askon.cz/Produkty/HSM-moduly/>.

33. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor eGovernmentu: *Archiv* [online]. MVČR, © 2016. 30. května [cit. 2019-10-31]. Dostupné z WWW: <https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>.
34. PRŮŠA, J. Lupa.cz, *eIDAS a problémy s důvěryhodností kvalifikovanýchcertifikátů* [online]. © 1998-2019 Lupa.cz, 2017. 17. července [cit. 2019-10-31]. Dostupné z WWW: <https://www.lupa.cz/clanky/eidas-a-problemy-s-duveryhodnosti-kvalifikovanych-certifikatu>.
35. PETERKA, J. Lupa.cz, Elektronické podpisy: v září skončí výjimka, budou úředníci připraveni? [online]. © 1998-2019 Lupa.cz, 2018. 11. června [cit. 2019-11-01]. Dostupné z WWW: <https://www.lupa.cz/clanky/elektronicke-podpisy-v-zari-skonci-vyjimka-budou-urednici-pripraveni/?ic=serial-box&icc=text-title>.

Ostatní zdroje

Interní materiály Agentura BOVA, Kybernetická bezpečnost a ochrana dat ve veřejném sektoru

Seznam obrázků