Univerzita Hradec Králové
Filozofická fakulta

Bakalářská práce

2018 Lukáš Konvalina

Univerzita Hradec Králové

Filozofická fakulta

Katedra pomocných věd historických a archivnictví

Elektronická identifikace

Bakalářská práce

Autor: Lukáš Konvalina

Studijní program: Počítačová podpora v archivnictví

Studijní obor: Počítačová podpora v archivnictví (BPARCHIV)

Vedoucí práce: Ing. Monika Borkovcová, Ph.D.

Univerzita Hradec Králové
Filozofická fakulta

Zadání bakalářské práce

Autor:	**Lukáš Konvalina**
Studium:	F14BP0008
Studijní program:	B3928 Technická podpora humanitních věd
Studijní obor:	Počítačová podpora v archivnictví
Název bakalářské práce:	**Elektronická identifikace**
Název bakalářské práce AJ:	Electronic identification

Cíl, metody, literatura, předpoklady:

Cílem práce je rozsáhlá analýza a nalezení úzkých míst služby elektronické identifikace (eIDAS) se zaměřením na problematiku ve veřejné správě v ČR. Práce se bude zabývat nařízením Evropského parlamentu a Rady EU o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a souvisejících, kde osoba podespala elektronický dokument, jehož prostřednictvím činí úkon ve vztahu k veřejné správě. Práce se bude zabývat případovou studií vázanou na Státní okresní archiv Hradec Králové a zaměřenou na dopady problémů elektronické identifikace při výkonu předarchivní péče a spisové služby. Součástí práce je i vyhodnocení rizik elektronické identifikace osob v souvislosti s možností zneužití dat a nedostatečnou bezpečností identifikačních systémů a identifikace možných hrozeb.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. EUR-Lex [online]. 2014 [cit. 2017-11-05]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ Digitální agenda pro Evropu. EUR-Lex [online]. 2010 [cit. 2017-11-05]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52010DC0245R(01)&from=EN Zákon č. 250/2017 Sb.: Zákon o elektronické identifikaci. Zákony pro lidi [online]. 2017 [cit. 2017-11-06]. Dostupné z: https://zakonyprolidi.cz/cs/2017-250/zneni-20180701 Vyhláška č. 259/2012 Sb.: Vyhláška o podrobnostech výkonu spisové služby. Zákony pro lidi [online]. 2015 [cit. 2017-11-26]. Dostupné z: https://zakonyprolidi.cz/cs/2012-259/zneni-20150101

Garantující pracoviště:	Katedra pomocných věd historických a archivnictví, Filozofická fakulta
Vedoucí práce:	Ing. Monika Borkovcová, Ph.D.
Oponent:	Mgr. Martin Landsmann

Datum zadání závěrečné práce: 20.12.2017

Prohlášení studenta

Čestně prohlašuji, že tato práce je mým vlastním autorským dílem. Práci jsem vypracoval samostatně a uvedl jsem všechny prameny, literaturu a zdroje, které jsem při vypracování práce použil nebo z nich čerpal.

.....

Ve Výravě dne Lukáš Konvalina

Poděkování

Rád bych poděkoval paní Ing. Monice Borkovcové Ph.D. za vedení práce a odborné rady při jejím zpracovávání. Mé poděkování patří také Státnímu okresnímu archivu Hradec Králové za poskytnuté informace.

Anotace

Cílem práce je rozsáhlá analýza a nalezení úzkých míst služby elektronické identifikace (eIDAS) se zaměřením na problematiku ve veřejné správě v ČR. Práce se bude zabývat nařízením Evropského parlamentu a Rady EU o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a souvisejících, kde osoba podepsala elektronický dokument, jehož prostřednictvím činí úkon ve vztahu k veřejné správě. Práce se bude zabývat případovou studií vázanou na Státní okresní archiv Hradec Králové a zaměřenou na dopady problémů elektronické identifikace při výkonu předarchivní péče a spisové služby. Součástí práce je i vyhodnocení rizik elektronické identifikace osob v souvislosti s možností zneužití dat a nedostatečnou bezpečností identifikačních systémů a identifikace možných hrozeb.

Klíčová slova:

Elektronická identifikace, eIDAS, BPMN

Annotation

The work's goal is a wide analysis and seeking narrow areas of service of electronical identification (eIDAS), focused on a problem in Czech Republic's public administration. The work will focus on an edict of European Parlament and European Council about electronical identification and services making faith in electronic altransactions of the inner trade and the related, where the person signed an electronical document, which makes a deed to the public administration. It will focus on external study connected to the State district archives of Hradec Kralove and focused on the consequences of electronical identification problems while doing before-archiving care and ERDMS. One part of the work is even to evaluate the risks of electronical identification of men, according to an option of unusage of the data for good and lack of identification systems‘ security and identification of possible thread.

Key words:

Electronic identification, eIDAS, BPMN

Obsah

Úvod

Postupující proces digitalizace, se dotýká téměř všech aspektů lidského života a dosahuje v míře větší či menší na prakticky všechny státy světa. Digitalizace je zkrátka součástí globalizačního procesu, který je, jak je známo, objektivní a nelze ho zastavit, pouze korigovat směr a způsob, kterým bude ubíhat. Tvrzení, že každý čin může mít svá pro a proti, přičemž záleží na úhlu pohledu každého pozorovatele, by se dalo označit skoro až za filosofické, ale tato bakalářská práce z něj, zjednodušeně řečeno, vychází.

Práce se věnuje postupujícím procesům digitalizace v oblasti elektronické identifikace, jejímž dalším, nebo přesněji nejbližším dílčím krokem v českém prostředí, je přijetí zákona 250/2017 o Elektronické identifikaci. Tento zákon, ač nepředstavuje výraznou změnu a je jen malým krůčkem, předznamenává pokračování trvání dlouhodobého procesu elektronické identifikace dokumentů, ale i osob.

Protože však pojem elektronická identifikace skýtá řadu významných rizik a úskalí, jež je třeba zohledňovat, je hlavním tématem práce analýza, vztahující se na procesy zpracovávání dokumentů v analogické podobě i v podobě digitální. Tyto dva postupy, ač mají stejný výchozí bod a stejný cíl, se od sebe svými rozdílnými prostředky, metodami a postupy výrazně odlišují. Zlomovým prvkem tohoto odlišení se stalo zavedení systému eIDAS, který ustanovil právní charakter digitálních dokumentů a postavil je z hlediska právního na úroveň dokumentů analogových.

Ač je zavádění všeho nového (myšleno skutečně obecně) vždy doprovázeno mnoha superlativy vycházejících nejčastěji z úst tvůrců a propagátorů těchto změn, je třeba si nekriticky všímat i možných rizik a snažit se vynést na světlo i sebenepatrnější úskalí daného problému tak, aby vznikl komplexní pohled na danou událost. Proto ani tato práce nepřistupuje k otázce elektronické identifikace jako k nezbytné evoluci, neboť nejde o přirozený vývoj vycházející z požadavků a zájmů většiny občanů, ale spíše jako k revoluci, která má své cíle a záměry, a která skýtá jistá úskalí.

1. Legislativa

České archivnictví se zakládá na zákoně č. 499/2004 Sb. Zákon o archivnictví a spisové službě. Tento zákon je rozdělen do několika částí, přičemž tato práce se ve své praktické části vztahuje především na zákon č. 259/2012 Sb. Vyhláška o podrobnostech výkonu spisové služby.

Pro tuto práci jsou rovněž stěžejní zákony vztahující se k postupujícím procesům digitalizace v českém i evropském prostředí. Tyto zákony vycházejí z nařízení Evropského parlamentu a rady Evropské unie 910/2014. V legislativě ČR se jedná o zákon č. 250/2017 Sb. Zákon o elektronické identifikaci.

1.1. Nařízení Evropského parlamentu 910/2014 (eIDAS)

Za účelem postupujícího procesu digitalizace států Evropské Unie, bylo 23. července 2014 vydáno nařízení Evropského parlamentu a rady EU vztahující se k elektronické identifikaci a služeb vytvářejících důvěru pro elektronické transakce.[1]

V rámci tohoto nařízení byla zrušena směrnice 1999/93/ES, která platila do této doby a vztahovala se především k elektronickým podpisům, avšak v nedostatečné míře, neboť byla příliš zastaralá a nezohledňovala nové postupy a metody. Nařízení 910/2014 se tak vztahuje nejen k elektronickým podpisům, které následně dále rozvádí, ale i k dalším bodům služeb vytvářejících důvěru, jmenovitě k elektronickým pečetím, časovým razítkům, službám elektronického doporučeného doručování, certifikátům pro autentizaci webů a též k bezpečnému ověřování všeho výše uvedeného.

1.1.1. Příčina vzniku nařízení 910/2014

Nové nařízení staví na tvrzení, kdy jsou elektronické transakce spotřebiteli i podniky opomíjeny z důvodu nedostatečné důvěry v ně. Dosavadní nařízení vztahující se k elektronické identifikaci tedy nebyly dostatečné. Cílem nového nařízení, jež se vztahuje převážně na systémy elektronické identifikace členských

[1] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN

států EU a poskytovatele služeb vytvářejících důvěru v ně, bylo proto navýšit důvěryhodnost elektronických transakcí na vnitřním trhu a stanovit základní bezpečnostní pravidla, která by byla základem pro bezpečnou komunikaci, čímž by byla posílena využitelnost a efektivnost elektronických transakcí.[2]

1.1.2. Vzájemná spolupráce států EU při nařízení 910/2014

Systémy elektronické identifikace vytvářejí tři stupně bezpečnostních záruk systémů, tedy tři stupně spolehlivosti uváděné totožnosti osob – jedná se o nízkou úroveň záruky, značnou úroveň záruky a vysokou úroveň záruky[3]

Dle článku 6 však nařízení počítá se vzájemným uznáváním elektronické identifikace i mezi členskými státy EU. Tato přeshraniční autentizace je logicky podmíněna využitím stejné nebo vyšší úrovně záruky, čímž je zajišťována přibližně stejné úroveň zabezpečení. Souběžný rozvoj digitalizace v členských státech EU je proto nezbytný pro plné dosažení cíle, který si zákon vytyčuje.[4]

V případě narušení bezpečnosti mají členské státy povinnost okamžitého pozastavení nebo zrušení dané autentizace a oznámení stavu ostatním členským státům. Stejný proces musí následovat v případě napravení problému.[5] Touto oznamovací povinností je zajišťována spolupráce mezi členskými státy EU a zajišťována bezpečnost. V případě nevyřešení problému do tří měsíců od zrušení autentizace je však stát povinen systém elektronické identifikace zrušit. Odpovědnost za způsobenou škodu přejímá oznamující stát, stejně jako strana, jejíž prostředky byly zneužity. Nelze se proto vyhnout jistému podezření, že jak

[2] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN

[3] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN, článek 8

[4] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN, článek 6

[5] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN, článek 10

stát, tak i firmy poskytující systémy elektronické identifikace, se mohou pokusit bezpečnostní průniky zatajit, aby se vyhnuly postihům a též snížení renomé.

Vzájemná spolupráce mezi členskými státy EU v rámci elektronické identifikace zahrnuje též vzájemnou pomoc v otázce zkušeností, postupů, či hodnocení. Dle článku 17 jsou členské státy povinny spolupracovat s dohlížejícím vyšším orgánem, který má za úkol dohlížet nad kvalifikovanými poskytovateli služeb skrze audity, udělovat, či odebírat jim status kvalifikovaného poskytovatele, zajišťovat bezpečnost, analyzovat stav a podávat hlášení Komisi EU.[6]

1.1.3. Služby vytvářející důvěru dle nařízení 910/2014

Nařízení rady EU 910/2014 stanovuje pět kvalifikovaných služeb vytvářejících důvěru a zajišťujících tak jasnou identifikaci. Tyto služby budou podrobněji popsány v následujících kapitolách. Jedná se o:

1) Elektronický podpis, který v případě kvalifikovanosti má mít stejnou váhu jako podpis analogový, tedy ruční.

2) Elektronickou pečeť, která v případě kvalifikovanosti má zajišťovat integritu a správnost původu dat, k nimž je pečeť připojena.

3) Elektronické časové razítko, které v případě kvalifikovanosti má zajišťovat správnost data a času ve spojení s integritou dat, k nimž je razítko připojeno.

4) Službu elektronického doporučeného doručování, které v případě kvalifikovanosti má zajišťovat integritu dat, jejich odeslání identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a též správnost času odeslání a přijetí.

5) Autentizaci internetových stránek, která má zajišťovat bezpečnost webových stránek.

[6] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN, článek 17

1.2. Zákon 297/2016 o službách vytvářejících důvěru

Dne 19. září 2016 byl uveden v platnost zákon, vycházející z nařízení EU 910/2014, jehož významem je připravit právní řád ČR na přijetí příští fáze eIDASu. Zákon v podmínkách ČR ustanovuje obecná pravidla pro procesy elektronického podepisování, pečetění a aplikování časových razítek. Tímto zákonem byl rovněž zrušen předchozí zákon o elektronickém podpisu (227/2000 Sb.) Od 1. července 2017 byl zákon novelizován. Aktuální znění zákona nyní upravuje okolnosti bezpečnostních postupů služeb vytvářejících důvěru.[7]

1.2.1. Působnosti ministerstva a Správy základních registrů dle 297/2016

Dle zákona 297/2016 orgán dohledu nad kvalifikovanými poskytovateli plní ministerstva vnitra. Ministerstvo tak má právo zneplatnit kvalifikované certifikáty na základě podezření narušení bezpečnosti (padělání, zneužití nebo vytvoření na základě nepravdivých údajů). V takovém případě má ministerstvo rovněž povinnost zveřejňovat seznamy kvalifikovaných poskytovatelů obsahující informace o službách, jež poskytují.[8]

1.2.2. Metody zajištění bezpečnosti dle zákona 297/2016

Kvalifikovaný poskytovatel služeb vytvářejících důvěru má ze zákona povinnost po dobu deseti let uchovávat dokumenty související s vydáváním kvalifikovaných certifikátů vztahujících se k elektronickým podpisům, pečetím, razítek i webů. Po uplynutí této lhůty poskytovatel stálé uchovává údaje o totožnosti žadatele certifikátu.[9]

[7] Zákon č. 297/2016 Sb.: Zákon o službách vytvářejících důvěru pro elektronické transakce. *Zákony pro lidi* [online]. 2016 [cit. 2018-02-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297

[8] Zákon č. 297/2016 Sb.: Zákon o službách vytvářejících důvěru pro elektronické transakce. *Zákony pro lidi* [online]. 2016 [cit. 2018-02-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297, par 13

[9] Zákon č. 297/2016 Sb.: Zákon o službách vytvářejících důvěru pro elektronické transakce. *Zákony pro lidi* [online]. 2016 [cit. 2018-02-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297, par 3

1.3. Zákon 250/2017 o elektronické identifikaci

1. července 2018 vchází v účinnost zákon o elektronické identifikaci vztahující se přímo na Nařízení Evropského parlamentu a rady EU č. 910/2014. Zákon je dalším dílčím krokem postupujícího procesu digitalizace, zaměřuje se především na elektronickou identifikaci osob a týká se jejího základního využití v praxi. Upravuje působnosti Ministerstva vnitra a Správy základních registrů v této otázce, a upravuje též přestupky vztahující se ke správě elektronické evidence. Tento zákon upřesňuje termín kvalifikovaný systém, jako systém, který je spravován kvalifikovaným správcem, splňuje patřičné normy, postupy, umožňuje poskytování služeb národního bodu.[10]

1.3.1. Kvalifikovaný systém

Zákon pracuje s pojmem „Kvalifikovaný systém," jehož význam je vysvětlen řadou podmínek, který tento pojem vyžaduje pro své významové naplnění. Jedná se o systém elektronické identifikace, který je schopen splňovat patřičné normy, postupy a nařízení stanovené předpisem EU, přičemž tento systém je spravován kvalifikovaným správcem, jímž se rozumí státní orgán, či osoba s dostatečnou udělenou akreditací pro správu systému. Zákon počítá se správou systému elektronické identifikace nejen státním orgánem, ale i akreditovanou osobou, tedy správou soukromého sektoru. Zákon nicméně vytyčuje podmínky pro udělení akreditace, přičemž za zásadní bod lze považovat nutnost splnění norem a požadavků Evropské unie.

Ministerstvo vnitra rozhoduje o udělení akreditace kvalifikovaného systému a vytyčuje podmínky pro udělení:

- žadatel o akreditaci musí splňovat technické specifikace, normy a postupy stanovené EU.
- musí být zajištěna bezúhonnost žadatele
- musí existovat pojištění v případě škod způsobených správou kvalifikovaného systému

[10] Zákon č. 250/2017 Sb.: Zákon o elektronické identifikaci. *Zákony pro lidi* [online]. 2017 [cit. 2018-01-08]. Dostupné z: https://zakonyprolidi.cz/cs/2017-250/zneni-20180701

- je třeba vypracovaného plánu pro ukončení činnosti
- systém elektronické identifikace musí umožňovat poskytování služeb národního bodu.[11]

1.3.2. Národní bod

Národní bod je informační systém veřejné správy, který podporuje proces elektronické identifikace a autentizace skrze kvalifikovaný systém. V rámci dodržení interoperability mají být správcem zajištěny všechny požadavky stanovené evropskou unií v 2015/1501. Dle paragrafu 20, je ze zákona správcem národního bodu stanovena Správa základních registrů.[12]

Národní bod zaznamenává identifikátory pro elektronickou identifikaci (údaje o ní), pro držitele v rámci kvalifikovaného systému a též v rámci online služeb.

Správa základních registrů pro vykonávání elektronické identifikace využívá z informačních systémů veřejné správy jména, příjmení, adresy, data a místa narození a případně data a místa úmrtí.

11 Zákon č. 250/2017 Sb.: Zákon o elektronické identifikaci. *Zákony pro lidi* [online]. 2017 [cit. 2018-01-08]. Dostupné z: https://zakonyprolidi.cz/cs/2017-250/zneni-20180701, par 5

12 Zákon č. 250/2017 Sb.: Zákon o elektronické identifikaci. *Zákony pro lidi* [online]. 2017 [cit. 2018-01-08]. Dostupné z: https://zakonyprolidi.cz/cs/2017-250/zneni-20180701, par 20

2. Nařízení eIDAS v prostředí ČR

Nařízení eIDAS („Elektronická identifikace a služby“) v našem prostředí vstupuje v platnost od 17. září 2014 v rámci nařízení EU 910/2014. Projekt eIDAS má za úkol pomocí vytvořených standardů zajišťujících bezpečnost elektronických transakcí, navýšit důvěryhodnost služeb na jednotném trhu EU. Vychází tedy z postupujícího procesu digitalizace a požadavku stanoveného Evropskou unií. Projekt eIDAS proto stanovuje základní pravidla svých cílů, kterými jsou:

1) Vytvoření právní jistoty – nutnost využití certifikačních prostředků pro online služby. Tímto cílem je zajišťována bezpečnost a z ní vycházející důvěryhodnost v online služby.

2) Adresování všech fází elektronické transakce (včetně archivace digitálních stop transakce)

3) Vytvoření právního rámce pro komplexní a vzájemně se doplňující soubor nástrojů a služeb – s cílem vytvořit důvěryhodné prostředí pro el. transakce. Jednotlivé služby jsou jednotlivě specifikované, avšak navzájem se doplňují.[13]

Nařízení eIDAS uznává kvalifikované elektronické podpisy, časová razítka i pečetě. V rámci elektronické identifikace systém eIDAS směřuje k co nejvyšší úrovní interoperability, tedy v rámci globalizačního procesu zajištění uznávání elektronických identifikací i za hranicemi (aktuálně v rámci prostoru států Evropské unie).

Protože služby elektronické identifikace se navzájem ovlivňují a doplňují, cílem eIDAS je taktéž jejich vzájemné přesné vymezení dle účelu a možností použití, jejich vyhranění a též jejich přesné definování pro veřejnost.

2.1. Elektronická identifikace

Elektronická identifikace je postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují fyzickou, či právnickou osobu.

[13] Ondřej Felix. Cíle a oblasti regulace eIDAS (Ondřej Felix). In: *Youtube* [online]. 15. 6. 2016 [cit. 2018-03-15]. Dostupné z: https://www.youtube.com/watch?v=loLkgFpzVUk

Prostředkem elektronické identifikace je pak hmotná, či nehmotná jednotka obsahující osobní identifikační údaje.

2.2. Využití eIDAS a členění

Služby vztahující se k systému eIDAS lze rozčlenit dle řady kritérií. Uživatelsky nejsnazším a nejlépe pochopitelným rozdělením je členění dle způsobu využívání - online a offline využívání. Elektronická identifikace je ve své podstatě založená na vytvoření a využití elektronické identity. Jedná se tedy o prvek online využití přímo vyžadující souvislost se systémem eIDAS. Služby vytvářející důvěru v elektronické transakce, jmenovitě elektronický podpis, elektronická pečeť a časové razítko (vše bude podrobněji popsáno níže), se neobejdou bez online využití při vytváření, ale následně už je lze využívat offline.[14]

2.3. Budoucnost elektronické identifikace v ČR

V průběhu roku 2018 bude v rámci postupujícího procesu elektronické identifikace docházet k rozmachu elektronické identifikace osob.

2.3.1. Občanské průkazy s čipem

Elektronické občanské průkazy s čipy jsou v ostré praxi zaváděné už od roku 2012. Od roku 2018 bude hromadně zaváděn nový občanský průkaz s čipem, který splňuje požadavky nařízení eIDAS. Průkaz má zajišťovat jednoznačnou vazbu mezi fyzickou identitou občana a jeho identitou elektronickou. Občanský průkaz s čipem obsahuje digitální informace odpovídající fyzickému obsahu průkazu, tedy stejné údaje jako na kartičce, ale v elektronické podobě.

Čipové občanské průkazy jsou opatřeny bezpečnostním osobním kódem (BOK). Elektronická identita občana je uložena v registru ROB. Osobní kód BOK bude znám pouze občanovi, občan jej při obdržení elektronického průkazu zadá do registru ROB, kde je uložen. Tím je zajištěna vyšší bezpečnost vůči zcizení a především lze ověřit spojitost mezi osobou a doloženým občanským průkazem

[14] Ondřej Felix. Cíle a oblasti regulace eIDAS (Ondřej Felix). In: *Youtube* [online]. 15. 6. 2016 [cit. 2018-03-15]. Dostupné z: https://www.youtube.com/watch?v=loLkgFpzVUk

elektronicky, tedy takřka jednoznačně, na rozdíl od „pouhého“ ověřování podobnosti (na základě fotografie).

2.3.2. Možnosti využití OP s čipem

Krom běžného fyzického předložení občanské průkazu může občan svoji identitu prokázat i zadáním kódu BOK.[15] Obsah ROB registru je srovnán se zadaným kódem a v případě jejich shodnosti je identita občana potvrzena.

Pomocí speciálních čtecích zařízení může občan zadat svůj osobní identifikační kód (OIK), čímž je zajištěn přístup k identifikačnímu certifikátu a tedy umožnění vlastní identifikace. Protože soukromý klíč nelze z čipu vyexportovat, nelze jej samostatně zcizit a zneužít.

V případě ztráty občanského průkazu občan po nahlášení svého BOK. Protože čip obsahuje až na očekávatelné výjimky (foto a podpis) stejné informace jako ty uvedené n průkazu lze vložením čipu do patřičného zařízení a zadáním kódu pak toto zařízení informace z čipu obdrží. To znamená že údaje mohou být odeslány třetí straně bez přímé fyzické přítomnosti občana.

Klasické „offline“ funkce občanského průkazu bude nadále využívána především pro ověřování totožnosti a výše věku v otázkách kontroly, tedy například při ověření plnoletosti u prodejen alkoholu.

2.3.3. Teoretické možnosti zneužití

Je velice brzy na zhodnocení funkčnosti a správnosti zavedení občanských průkazu s novým čipem, ale přesto lze nastolit otázky, na něž buď chybí odpověď pro veřejnost, nebo není dostatečná. Jedná se především o otázky, nakolik jsou informace z občanského průkazu chráněny vůči zneužití třetí stranou. Do jaké míry lze zajistit správnost čtecích zařízení, jaká je trvanlivost čipu a jeho odolnost vůči mechanickému i jinému poškození a zda je morálně správné, aby o identifikaci člověka na té nejzákladnější úrovni rozhodoval „nečlověk.“

[15] Petr Kuchař. Plány MV (Petr Kuchař - hlavní architekt eGovernmentu MV). In: *Youtube* [online]. 20. 4. 2017 [cit. 2018-03-15]. Dostupné z: https://www.youtube.com/watch?v=Z-fPkOC9tM4

2.3.4. Obecné nařízení o ochraně osobních údajů

Na základě Evropského nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)[16] vejde 25. května 2018 v platnost zákon o ochraně osobních údajů, přezdívaný ve zkratce GDPR (General Data Protection Regulation). Cílem GDPR je zajistit ochranu osob minimalizací údajů, které jsou o nich zveřejňovány, shromažďovány a ukládány. Stejně tak je cílem technické zabezpečení údajů a v důsledku toho ochrana obyvatel vůči zneužití jejich osobních údajů třetí stranou.

GDPR se v podmínkách ČR dotkne všech fyzických i právnických osob, které přicházejí do styku s osobními údaji. Může se jednat o zveřejňování fotografií nebo záznamů žáků ve školách, ale i shromažďované údaje obchodníků o zákaznících. Nařízení hovoří o pojmu Správce, což může být fyzická i právnická osoba, která má na starosti určení účelu a prostředků pro zpracování osobních údajů.[17]

Avšak již nyní si lze všímat obav některých skupin, či institucí, pro které bude GDPR znamenat výrazné omezení a nutnost velmi pečlivě zohledňovat veškeré kroky ve vztahu k zveřejňování osobních informaci. Kupříkladu oblíbený sociální web Spolužáci.cz již nyní ukončuje svoji činnost z důvodu problematických změn, které by vyhovovaly GDPR.[18]

2.3.5. Plné zavedení eIDAS

Od 28. září 2018 má být v prostředí státních systémů ČR plně zaveden systém eIDAS. V praxi to znamená, že veškeré úřady musejí být připraveny na přijímání elektronických dokumentů po stránce technologické, správní i odborné. Musejí

[16] Nařízení Evropského parlamentu a rady EU 2016/679. *EUR-Lex: Přístup k právu evropské unie* [online]. 27. dubna 2016 [cit. 2018-04-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:32016R0679

[17] Základní příručka. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-04-06]. Dostupné z: https://www.uoou.cz/zakladni%2Dprirucka/ds-4744/p1=4744

[18] KAPUCIÁNOVÁ, Aneta. Služba Spolužáci.cz na konci srpna končí. *Seznam.cz: Sblog* [online]. 4. dubna 2018 [cit. 2018-04-11]. Dostupné z: https://blog.seznam.cz/2018/04/sluzba-spoluzaci-cz-na-konci-srpna-skonci/

být schopny po právní stránce akceptovat dokumenty opatřené identifikačními službami stanovenými eIDASem. Plné zavedení eIDAS je zároveň krokem globalizace, je to krokem který ČR přiblíží a prováže s Evropskou unií, neboť systém eIDAS je jednotný pro všechny státy EU, což znamená, že každý stát musí být v ideálním případě schopen přijímat a ověřovat certifikované elektronické dokumenty i ze zahraničí, respektive z ostatních států EU.

3. Služby vytvářející důvěru a jejich rizika

V prostředí úřadů a archivů, hlavně v záležitostech předarchivní péče a spisové služby, se přichází do styku s mnoha elektronickými dokumenty, jejichž původce je třeba identifikovat a zajistit správnost i bezpečnost přenosu a doručení dokumentů. Metod elektronické identifikace dokumentů je několik a dle nařízení eIDAS je třeba na dokumenty opatřené uznávaným elektronickým podpisem (popř. značkou) nahlížet stejně jako na podepsaný dokument analogový. Právní hodnota obou dokumentů je v takovém případě shodná.

3.1. Elektronický podpis

Elektronický podpis je základní a nejběžnější druh elektronické identifikace užívaný v otázce archivnictví (a nejen v něm). Jedná se o údaj v elektronické podobě, jež je přiložený k datové zprávě a slouží k jednoznačnému ověření identity podepsané osoby. Největším rizikem použitelnosti elektronického podpisu je relativně krátká životnost kvalifikovaných certifikátů. [19] Tím se částečně vytváří rozpor mezi záměrem EU o zvýšení četnosti využívání elektronických transakcí, a otázkou nejen ohledně pohodlnosti při využívání, ale především bezpečnosti transakcí. Omezená životnost nevyhnutelně způsobuje i omezené možnosti využití v praxi. Řešením může být zavedení podpisů s prodlouženou možností ověřování[20]

Elektronický podpis je založený na nutnosti využití dalších zařízení pro jeho přečtení. Zatímco pro analogový podpis a jeho ověření postačí lidské oko, pro přečtení elektronického podpisu je vyžadováno elektronické zařízení schopné jej přečíst. Stejně tak tomu je v případě jeho vytváření. Elektronický podpis navíc není svazován s žádným nosičem. Zatímco ruční podpis je fyzicky přítomen na povrchu dokumentu, podpis elektronický není neoddělitelnou součástí samotného dokumentu.

[19] LECHNER, Tomáš. *Elektronické dokumenty v právní praxi.* Praha: Leges, 2013, 256 s. ISBN 978-80-87576-41-0., str 61

[20] PETERKA, Jiří. *Báječný svět elektronického podpisu* [online]. Autorská verze. Praha: CZ.NIC, 2011 [cit. 2018-01-18]. ISBN 978-80-904248-3-8., str 339

3.1.1. Princip ověření

Ověřování pravosti elektronického podpisu, neboli provedení autentizace, je stavěno na datech nazývaných klíče. Osoba při vytváření elektronického podpisu zároveň generuje tzv. soukromý (privátní) klíč a pro ověření podpisu se generuje druhý veřejný klíč. Porovnání těchto klíčů je základem zajištění ověřitelnosti a určení pravosti elektronického podpisu. Tím je zároveň podpis chráněn proti padělání, jelikož ač jsou k ověření dokumentu zapotřebí oba klíče, odvodit druhý na základě prvního nelze a to díky metodám pokročilého asymetrického šifrování při jejich vzniku. Jinými slovy, oba klíče tvoří pár a vlastnictví jednoho klíče (i kdyby se jednalo o klíč soukromý), nestačí k tomu, aby bylo možné odhalit klíč druhý, tudíž je podepsaný dokument chráněn i vůči zcizení jednoho z klíčů. Vlastnictví veřejného klíče v rukách další osoby slouží k ověření, nicméně je třeba stvrdit, že veřejný klíč skutečně tvoří pár s „naším“ soukromým klíčem. Pro potřeby ověření se užívá pojem certifikát, což je ověření, že daná osoba je držitelem daného soukromého klíče.[21]

3.1.2. Certifikát

Certifikáty jsou tedy způsobem ověření pravosti podpisu. Existuje jich několik typů. Základní typy certifikátů se dělí na osobní a systémové. Oba typy lze dále dělit na kvalifikované certifikáty, což jsou certifikáty vymezené zákonem, tedy dá se o nich mluvit jako o certifikátech ověřených. Vydání certifikátu může provádět téměř každý, ovšem kvalifikované certifikáty mohou vydávat pouze kvalifikované certifikační autority, které se v případě splňování zákonem ustanovených požadavků stávají akreditovanými. [22] V případě probíhajícího ověřování pak následuje několik kroků:

1) ověření, zda je platný elektronický podpis

2) ověření, zda je platný připojený certifikát

[21] PETERKA, Jiří. *Báječný svět elektronického podpisu* [online]. Autorská verze. Praha: CZ.NIC, 2011 [cit. 2018-01-18]. ISBN 978-80-904248-3-8.

[22] PETERKA, Jiří. *Báječný svět elektronického podpisu* [online]. Autorská verze. Praha: CZ.NIC, 2011 [cit. 2018-01-18]. ISBN 978-80-904248-3-8.

3) ověření, zda je připojený certifikát kvalifikovaný (vydaný akreditovaným poskytovatelem certifikačních služeb)[23]

Nejprve je tedy ověřena platnost el. podpisu (tedy že obsah dokumentu nebyl od vytvoření podpisu nijak změněn). V případě porušení této podmínky však nelze definovat jakékoli změny, k nimž v dokumentu došlo. Proto se podpis na dokumentu stává bezpředmětným a dokument jakoby nijak podepsán nebyl a ještě může být pozměněn. Druhým krokem je ověření, zda platnost certifikátu stále platí. To samo o sobě ale nezaručuje, že k podpisu došlo v době platnosti certifikátu, proto je pro přesné určení data používána jiná identifikační služba - časové razítko. Třetím a posledním krokem je ověření, zda jsou certifikační údaje důvěryhodné, tedy zda jeho vydavatel je ověřeným poskytovatelem certifikátů.

3.1.3. Působnost ministerstva

Ministerstvo vnitra dle zákona zajišťuje dohled nad poskytovateli kvalifikovaných certifikátů. Je to právě ministerstvo, které může zneplatnit vybrané certifikáty, či odebrat akreditaci poskytovatelům. Ministerstvo dále zajišťuje a zveřejňuje informace o poskytovatelích certifikátů a vede seznamy certifikátů.[24]

3.1.4. Přestupky

V případě zneužití značky důvěry fyzickou osobou, respektive porušení nařízení komise EU 2015/806 lze dle zákona pokutovat až do výše 2000000 Kč. Právnická osoba se dopouští porušení zákona v případech, kdy po ukončení činnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru neeviduje, či neposkytuje příslušné informace.

Kladené nároky na poskytovatele služeb vytvářejících důvěru se liší. Poskytovatel služeb se dopouští přestupků v případě nezajištění technických a

[23] LECHNER, Tomáš. *Elektronické dokumenty v právní praxi.* Praha: Leges, 2013, 256 s. ISBN 978-80-87576-41-0., str 78

[24] Zákon č. 297/2016 Sb.: Zákon o službách vytvářejících důvěru pro elektronické transakce. *Zákony pro lidi* [online]. 2016 [cit. 2018-02-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297

organizačních opatření ohledně bezpečnosti jeho služeb anebo v případě opožděného oznámení narušení bezpečnosti.

3.1.5. Rizika elektronického podpisu

Snahy o postupující digitalizaci znamenají navyšování důležitosti elektronického podpisu při transakcích. Elektronický podpis je již natolik akceptován a uznáván, že plní úlohu jakési běžné elektronické podoby úředně ověřeného podpisu. Stejně jako lze analogový dokument a digitální dokument postavit do jedné roviny, lze tak na základě zákona stejně posuzovat analogový i digitální podpis.

Zajištění elektronické identifikace, v tomto případě hlavně certifikace, však může být svěřena i akreditovaným soukromoprávním subjektům. Otázkou tak zní, zda ač má elektronický podpis váhu úředně ověřeného podpisu, nenachází-li se právě v otázce poskytovatelů certifikátů rizikové místo.

Druhým úzkým místem elektronického podpisu je jeho samotná elektronická podoba. Tato skutečnost způsobuje, že pochopení přesného fungování, principu a samotného technického provedení elektronického podpisu je mnohonásobně složitější než pochopení podpisu analogového. Tak vzniká prostor nejen pro chybování z neznalosti, ale i pro možnosti podvodu a zneužití elektronického podpisu.

Dalším nedostatkem se může jevit omezená doba platnosti kvalifikovaného certifikátu, ale též bezpečnost šifrování, neboť vzhledem k prudkému vývoji výpočetní techniky může být vyvinut počítač schopný současné šifrovací algoritmy snadno prolomit. Speciálně na pozicích, kdy je manipulováno s velmi citlivými tajnými dokumenty by mohlo takovéto prolomení znamenat výrazné bezpečnostní ohrožení firem i státu. Ředitelství velkých firem, ministerstva nebo tajné služby, tam všude by mohl hrozit průlom, neboť může jít o citlivé uzly funkčnosti státu. I jediné zjištěné prolomení, by navíc znamenalo automatický konec důvěryhodnosti všech takto šifrovaných dokumentů, neboť bezpečnost už by nebylo možné zaručit. Tvrzení, že vynaložení úsilí na prolomení jediného

citlivého dokumentu by bylo zbytečné, se tedy dá považovat za liché, neboť prolomení jednoho znamená ohrožení a dosti možná i zneplatnění všech.

V neposlední řadě lze rizika elektronického podpisu vnímat i na filosofické a psychologické úrovni. Člověk ze své hmotné, materiální podstaty, má mnohem blíže k analogovému podpisu, kdy dochází ke kontaktu pera a papíru, kdy je vynakládána určitá fyzická aktivita a kde s ohledem na minulost dochází k pokračování určité významné tradice stvrzování dokumentu vlastnoručním podpisem. Proto z filosofického i lidského hlediska bude člověku, který má dostatečné schopnosti a znalosti k vlastnoručnímu podepisování, analogový podpis vždy bližší.

Na obranu elektronického podpisu je však třeba dodat, že se jedná o jediný (respektive nejzákladnější) způsob ověření elektronického dokumentu, jelikož elektronický dokument ze své podstaty nelze podepsat klasickým analogovým způsobem (lze podepsat nanejvýše jeho nosič, nikoli přímo dokument). Zároveň v otázce elektronického dokumentu probíhá zcela jiný proces jeho přečtení, který není závislý na lidských vjemech a tak minimalizuje riziko zaměnění, či ve stručnosti nesprávnou identifikaci osoby. Problém ručního podpisu často bývá jeho nečitelnost, což u elektronického podpisu nehraje roli.

3.2. Elektronická pečeť

Elektronická pečeť je podobně jako el. podpis službou vytvářející důvěru a stejně jako podpis je definována v několika úrovních důvěry. Elektronická pečeť zajišťuje a chrání obsah dokumentu, přičemž je zároveň spojena s původcem. Pečeť tedy prokazuje původce a pravost.

3.2.1. Rizika elektronické pečeti

Na rozdíl od elektronických podpisů, jejichž míra i doba používání je větší, jsou elektronické pečetě relativně málo známé a málo využívané. Jejich rozmach (ať už nucený, či dobrovolný) logicky vyžaduje zajištění prostředků, technologie a kapacit pro jejich běžné využívání, tedy nejen vytváření neboli pečetění dokumentu, ale též jejich čtení u příjemce.

3.3. Elektronické časové razítko

Elektronické časové razítko je údaj v datové podobě, který má úroveň elektronického podpisu, čili je založen na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Elektronické razítko musí splňovat tři pravidla.

1) Je jednoznačně spojené s označující osobou a umožňuje její identifikaci prostřednictvím kvalifikovaného certifikátu.

2) Bylo vytvořena a připojena k datové zprávě pomocí prostředků pro vytváření elektronických značek.

3) Je k datové zprávě připojeno takovým způsobem, že lze zjistit jakoukoli následnou změnu dat.

Časové razítko spojuje daný čas a datum s obsahem dat tak, aby bylo možné ověřit, zda nebylo s daty manipulováno. Podoba dat v době orazítkování je tedy ověřitelná.

Elektronická značka ale po technologické stránce je v zásadě stejná jako elektronický podpis. Rozdíly jsou pouze významové a právní. Praktické využití elektronických časových značek je především v otázce datových schránek.[25]

3.4. Elektronické doporučené doručování a datové schránky

Datová schránka slouží pro ukládání dokumentů (v omezené velikosti dané kapacitou) a komunikaci mezi uživateli formou přijímání i odesílání zpráv mezi jinými datovými schránkami. Jedná se o pokročilou a více zabezpečenou variantu emailu. Datová schránka vyžaduje autorizaci. Datových schránek existuje několik typů.

Elektronické doporučené doručování je však dle nařízení eIDAS odlišné. Dokument odeslaný a přijatý prostřednictvím služeb elektronického doručování má stejnou právní úroveň jako analogový dokument. V případě využití služeb elektronického doporučeného doručování proto platí domněnka integrity dat,

[25] LECHNER, Tomáš. *Elektronické dokumenty v právní praxi.* Praha: Leges, 2013, 256 s. ISBN 978-80-87576-41-0.

správnost data a času odeslání i přijetí a jednoznačná identifikace odesílatele i příjemce.

Rozdíl mezi doporučeným doručováním a datovými schránkami vychází z jejich původu. Zatímco zavedení elektronického doporučeného doručování je důsledkem nařízení eIDAS, datové schránky jsou zřízené státem, přesněji ministerstvem vnitra na základě žádosti. Datové schránky jsou výrazně omezeny svou kapacitou, ale ta se v průběhu posledních let zvyšuje v souvislosti s četností jejich využívání.[26]

[26] GALVAS, Miroslav. Datové schránky. *Epravo.cz* [online]. 13. července 2017 [cit. 2018-04-11]. Dostupné z: https://www.epravo.cz/top/clanky/datove-schranky-106059.html

4. Metody vedení spisové služby s ohledem na eIDAS

Spisová služba je zajišťování úkonů spojených s přijímáním, evidencí, oběhem, vyřizováním, značením, ukládáním, odesíláním a vyřazováním dokumentů. Tento proces v jistých upravených podobách probíhá už prvního evidování dokumentů, od vzniku prvních úřadů a počátků správy. Ale na přelomu 21. stol. dochází k významnému milníku, neboť s rozvojem výpočetních technologií se začínají vytvářet dokumenty v elektronické podobě. A stejně tak jsou doposavad analogové dokumenty převáděny do digitální podoby. Tím začíná nová éra správy, která se v podmínkách České republiky plně rozmáhá s přijetím eGovernmentu a eIDASu. Celý proces spisové služby je možné rozčlenit dle mnoha kritérií, ale pro účely této práce postačí rozdělení na příjem analogového a digitálního dokumentu, přičemž podoba dokumentu nehraje až takovou roli. Oba typy dokumentu přinášejí určitá úskalí a jejich nalezení umožňuje vytyčit výhody i nevýhody obou.[27]

4.1. Obecný koloběh dokumentu

1) Příjem dokumentu na podatelně, opatření podacím razítkem v den doručení dokumentu. Písemnost se jménem zaměstnance na prvním místě adresy vyžaduje nejprve doručení. Písemnost se stupněm utajení se předává neotevřená s příslušným podacím razítkem. Obálka je ponechána jako součást písemnosti splňuje-li patřičná kritéria, jinak je vyřazena.

2) Vyřízení písemnosti – po zaevidování je písemnost předána patřičnému úřadu. V případě vzniku spisu (dokumenty týkající se stejné věci), je spis evidován pod nejvyšším číslem jednacím a již není rozdělován.

3) Úprava dokumentu – Podepsání dokumentu, orazítkování

4) Odeslání písemnosti – Nejběžněji poštou, případně elektronicky. Dále odesílání faxem, telegramem nebo jinými způsoby.

[27] Vyhláška č. 259/2012 Sb.: Vyhláška o podrobnostech výkonu spisové služby. *Zákony pro lidi* [online]. 2015 [cit. 2018-01-06]. Dostupné z: https://zakonyprolidi.cz/cs/2012-259/zneni-20150101

5) Uložení dokumentu – Uložení písemnosti s přidělenými náležitostmi (skartační znak, skartační lhůta). Pokud je písemnost nadále potřebná, není ukládána na spisovně, ale na patřičném místě úřadu. Zaznamenání vyřízení podání do podacího deníku.

4.1.1. Úskalí elektronických dokumentů s ohledem na vybavenost úřadu

Se zavedením systému eIDAS roku 2014 byla většina úřadů nucena uzpůsobit své možnosti a pracoviště pro přijímání a zpracovávání dokumentů nejen v analogové, ale i v elektronické podobě. Tento proces není jen skokový, ale trvalý, neboť s rozmachem digitálního světa stále postupuje i do současnosti. Pro provádění procesů spisové služby elektronicky je vyžadováno vybavení dle standardů státních informačních systémů. Samozřejmostí je kvalifikovaný pracovník, který je schopen přijímat a zpracovávat elektronické dokumenty a též ověřovat jejich platnost skrze elektronické podpisy, razítka a další prvky identifikace. Stejně tak je nutno počítat s mnoha novými přibývajícími postupy, což vyžaduje stále kvalifikovanější pracovníky, kteří budou schopni reagovat na rychlý vývoj elektronických dokumentů a elektronické identifikace.

Všechny tyto podmínky úzce souvisejí s finanční stránkou, neboť je pro úřady nezbytné zajišťovat funkčnost pracovišť, včetně nákupu software pro výkon spisové služby a stejně tak jsou zřejmé výdaje na nové zaměstnance, či přeškolování původních.

4.1.2. Úskalí elektronických dokumentů s ohledem na kvalitu nosičů

Dalším zřejmým úskalím elektronických dokumentů je jejich trvanlivost. Nosiče digitálních dokumentů jako jsou CD disky, či DVD disky jsou stále ještě mladé a jejich maximální životnost mnohdy nelze jednoznačně ověřit praktickou zkušeností, neboť kvalita disků se různí s ní i jejich životnost. Obecně je udávána životnost CD, DVD i BR disků až sto let, ovšem jen v případě vysoce kvalitního vypalování dat, optimálních podmínek uskladnění a minimální opotřebovanosti. Praxe však říká, že životnost nelze jednoznačně odhadnout bez reálných zkušeností, které ale u média starého ani ne 40 let není kde vzít.

Životnost disků je navíc pouze podružný problém. Mnohem závažnější je extrémně rychlý vývoj informačních technologií, který jednak způsobuje, že dosavadní disky budou v průběhu pár let zastaralé a za druhé, a to je mnohem závažnější riziko, rychlý vývoj počítačů způsobuje, že novější typy už nejsou vybaveny (ať už po stránce HW či SW) k přečtení starších nosičů.[28]

Otázka životnosti tak zcela postrádá svoji prioritu, neboť uložené digitální dokumenty, které nedokáže vybavení úřadu přečíst lze metaforou připodobnit hypotetické situaci, kdy všichni pracovníci úřadu jsou zcela slepí. Řešením může být využívat starší operační systémy, ale ty mohou obsahovat bezpečnostní trhliny a nebudou pravděpodobně schopny přečíst moderní formáty dokumentů. V takovém případě je pak nutné pracovat nejen s moderními technologiemi pro zpracování moderních typů dokumentů, ale i těmi zastaralými anebo provádět průběžnou konverzi dokumentů.

[28] CUBR, Ladislav. *Dlouhodobá ochrana digitálních dokumentů.* Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

5. Kauzy

Během let fungování služeb elektronické identifikace došlo k několika bezpečnostním průlomům, které přinejmenším reálně dokazují, že proces elektronického zabezpečování dokumentů není dokonalý a skýtá rizika, jež mohou mít dalekosáhlý dopad na uživatele i poskytovatele těchto služeb.

5.1. Kauza COMODO

V březnu 2011 proběhl útok na poskytovatele certifikátů COMODO. Útočník si nechal vystavět 9 platných certifikátů. Firma COMODO patřičné certifikáty okamžitě revokovala a pokusila se informovat své uživatele.[29] Na tomto místě se však nachází další kritické místo, neboť jestliže firma ztratí svoji důvěryhodnost, jak lze následně důvěřovat jejím prohlášením o vyřešení problémy a o ujištění další bezpečnosti?

5.2. Kauza DigiNotar

Mnohem závažnější kauza se týká nizozemské certifikační autority DigiNotar. Ta je známým akreditovaným poskytovatelem i SSL certifikátů (s rozšířenou validací). Útočníkovi se však podařilo si více než 500 SSL certifikátů zajistit na různá jména.

Oproti COMODO byla reakce DigiNotar pomalejší a revokace proběhla se zpožděním. Jeden certifikát však revokován nebyl a skrze něj byl proveden rozsáhlý útok na uživatele v Iránu. Revokace tohoto certifikátu proběhla až téměř po měsíci od počátku útoku, což ve výsledku nejen ohrozilo množství uživatelů, ale též vyvolalo nedůvěru vůči společnosti Google na nějž byl podvodný certifikát vystavěn. Důsledky této krize jsou však mnohem dalekosáhlejší, neboť DigiNotar se stala pro výrobce softwareu využívající její certifikáty nedůvěryhodnou a to i v otázce certifikátů, které napadeny nebyly a byly zcela v pořádku. DigiNotar ztratil i vlastní akreditaci a doposavad velké a významného poskytovatele

[29] PETERKA, Jiří. Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. *Lupa.cz: Server o českém internetu* [online]. 20. září 2011 [cit. 2018-03-25]. Dostupné z: https://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/

certifikátů se stala pochybná firma, které jediný, ač masivní útok, nenávratně poškodil pověst i rozvoj.[30]

Oba tyto útoky se přihlásila tatáž osoba, kterou měl být jedenadvacetiletý student z Iránu. Pouštět se v této otázce dál, by znamenalo přistoupit na spekulace a zohlednit globální politické události, což ale rozhodně není cílem této práce. Přesto však lze na základě logiky nadnést, že pokud jediný hacker dokáže zdiskreditovat prosperující certifikační společnost, ohrozit důvěryhodnost napadeného webu a desítkám lidí způsobit rozsáhlé potíže a škody, pak je riziko potenciálního zneužití elektronického ověřování velmi vážné a zcela regulérně může sloužit i pro politické účely.

[30] PETERKA, Jiří. Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. *Lupa.cz: Server o českém internetu* [online]. 20. září 2011 [cit. 2018-03-25]. Dostupné z: https://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/

6. Znázornění procesů koloběhu dokumentů

Pro znázornění koloběhu dokumentu od jeho původce po archivaci lze použít mnoho modelovacích programů pro vytváření schémat. Účelem modelovacích jazyků je vytvořit názorný diagram úkonů a jejich vzájemného propojení. Diagram, který bude splňovat požadavky autora, ať už jsou jakékoli. Proces modelování lze rozčlenit do tří kroků. První je vytyčení vstupního a výstupního bodu. Lze je snadno odhalit otázkami jaký je výchozí stav a co je náš cíl. Oblast mezi výchozím a výstupním bodem, je předmětem druhého kroku modelování. Je třeba vytyčit jednotlivé dílčí procesy mezi vstupním a výstupním bodem. Poslední fází je stanovení vazeb mezi dílčími procesy.

IDEF - Modelovací jazyk se syntaxí a sémantikou umožňující vytvářet grafický náhled na systém či organizaci. Pro potřeby sledování procesu koloběhu dokumentu je však nevhodný.

EPC - Diagramy EPC jsou vhodné na určování posloupnosti aktivit. Skládají se ze tří základních prvků. Aktivity, události a logické spojky.

BPMN diagram - BPMN diagramy se skládají z malého množství grafických prvků, což je činí výhodné pro prezentace pro veřejnost, která není příliš obeznámená s modelovacími procesy a také pro názorný náhled na zobrazovaný proces.

6.1. Stavební prvky BPMN diagramu v programu Bizagi Process Modeler

Výhody BPMN diagramu jej činí univerzálním prostředkem pro představení procesu, v němž je začleněno několik účastníků nebo několik dílčích procesů najednou. Cílem BPMN diagramu například v rámci firem, může být umožnit všem účastníkům pochopit jejich roli v rozsáhlém procesu a ukázat jakým způsobem ovlivňují činnosti ostatních. Stejně tak lze představit dlouhodoběji trvající proces vztahující se k jednomu konkrétnímu dokumentu.

Název	Značení	Popis
Tokové objekty (Flow)		Skupina objektů, které souvisí s informacemi v průběhu procesu.
Události (Events)	Zelené kroužky (začátek), žluté kroužky (průběh), červené kroužky (konec).	Události, jimiž proces začíná (značeny zelenými kroužky), události, které se odehrávají přímo v procesu (oranžové kroužky) a také události, kterými proces končí (červené kroužky).
Aktivity (Tasks)	Obdélník se zaoblenými rohy	Znázorňují nějakou činnost, k níž v daném okamžiku dochází. V případě, že v sobě aktivita zahrnuje i další proces, nazývá se subprocesem a je označena znaménkem plus.
Brány (Gates)	Žlutý kosočtverec	Označují rozdělení procesů, například když dva a více procesů běží paralelně anebo když na základě volby je vybrán jeden proces (jedna větev).
Artefakty (Artifacts)		Upřesňující informace, dodatečné poznámky a kategorizace aktivit. Nemají vliv na chod procesu.
Skupina (Group)	Přerušovaný obdélník	Seskupuje aktivity pod nějaký společný jmenovatel, např. dle původce, či oblasti.
Poznámka (Annotation)	Textový rámeček	Vysvětlující text spojený s vybraným objektem.
Spojovací objekty (Connectors)		Slouží k propojení ostatních objektů navzájem.
Sekvenční tok (Sequence flow)	Černá plná šipka	Určuje pořadí objektů.
Asociace (Association)	Přerušovaná čára	Spojuje objekty s dodatečnými vysvětlujícími informacemi.
Tok zpráv (Message flow)	Přerušovaná čára s šipkou	Určuje tok zpráv mezi účastníky procesu

Tabulka 1 – Základní stavební prvky BPMN diagramu, Lukáš Konvalina

6.2. Obecný koloběh běžného dokumentu (např. daňového přiznání) před eIDAS

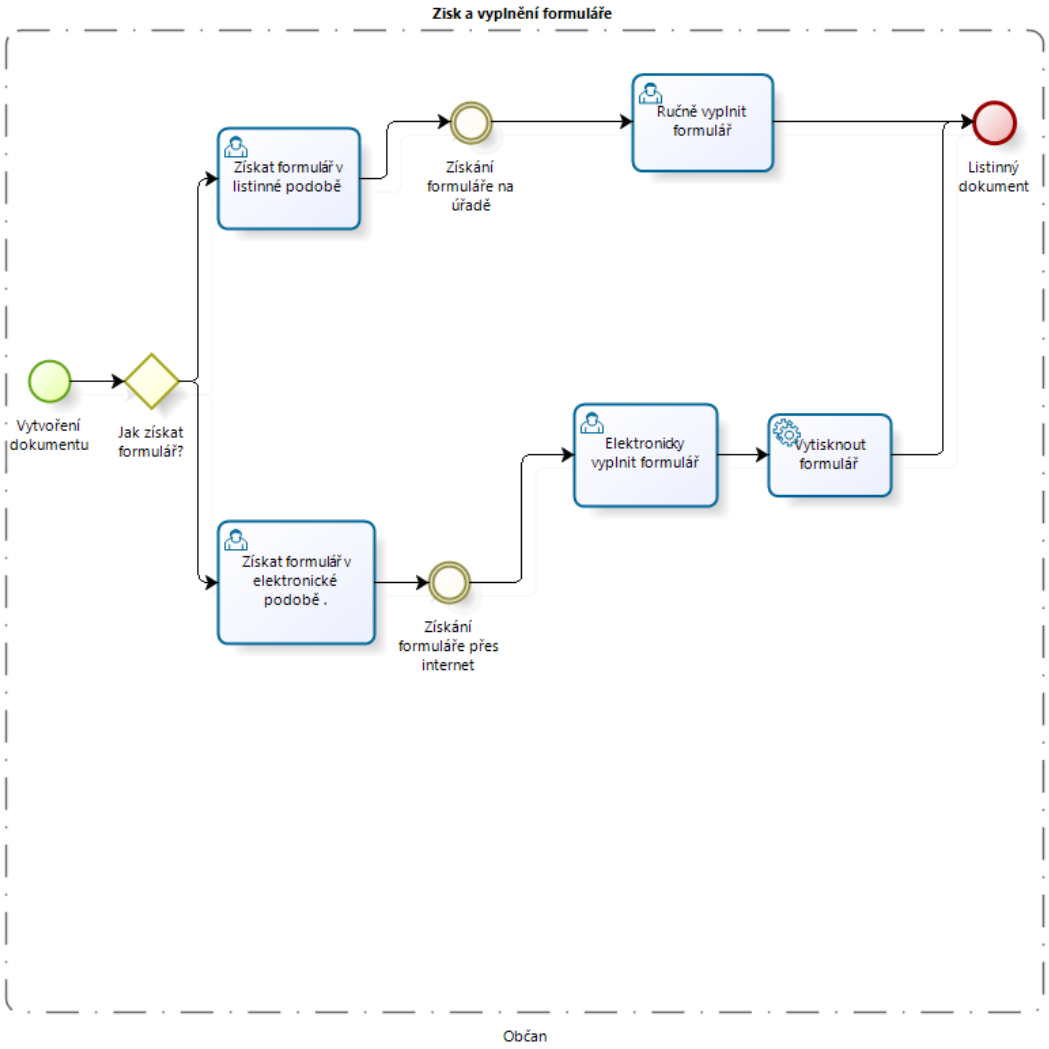
Protože zavedení nařízení eIDAS způsobilo změny v možnostech přijímání dokumentů úřady a archivy, lze představit dva odlišné koloběhy dokumentů. První se vztahuje na dobu před eIDAS a založen převážně na manipulaci s analogovým dokumentem, druhý se vztahuje na dobu po zavedení eIDASu a znázorňuje možnosti a požadavky, které eIDAS přináší. Rozdíl mezi oběma koloběhy dokumentů je po stránce procesů nejvýraznější v oblasti přijímání dokumentu úřadem, tedy ve fázi na přelomu činnosti občana a instituce.

6.2.1. Zisk a vyplnění formuláře

Výchozí situace: Občan má povinnost vyplnit a odeslat formulář (např. daňového přiznání) na patřičný úřad

Občan může formulář dokumentu získat v základní listinné podobě na příslušném úřadě. Přirozenou komplikací může být vzdálenost úřadu, tedy obtížná dostupnost, finanční náročnost cesty anebo časová náročnost.

Jinou možností získání formuláře je jeho elektronická podoba na webových stránkách úřadu. Požadavkem je v takovém případě připojení k internetu, využití patřičného software pro jeho přečtení (popř. vyplnění) a následně výstupního zařízení pro jeho vytištění do analogové podoby. Jedná se o proces vyžadující technické zázemí a určitou počítačovou gramotnost. Časová náročnost je však výrazně snížena s ohledem na vzdálenost občana od úřadu. Využití formuláře v elektronické podobě má taktéž výhodu v možnosti automatického dopočítávání částek na základě přednastavených parametrů a vzorců.



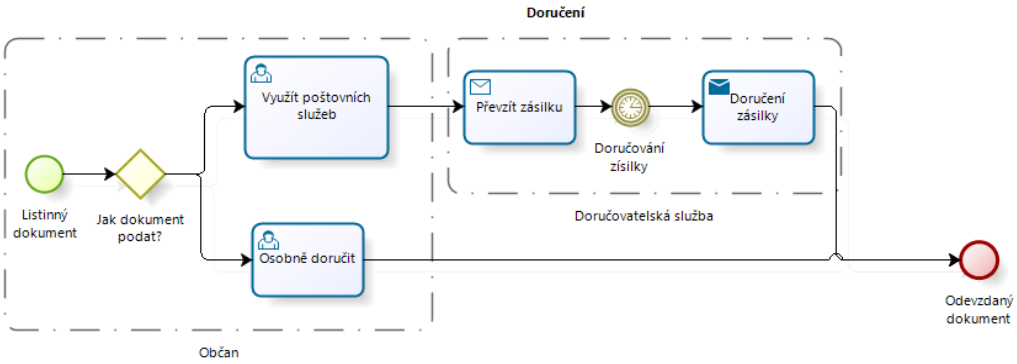
Obrázek 1 - Zisk a vyplnění formuláře, Lukáš Konvalina

6.2.2. Doručení dokumentu

Vyplněný formulář je připravený na doručení na podatelnu úřadu. Zaslání vyplněného dokumentu na úřad může proběhnout pomocí doručovatelské služby. V prostředí ČR je nejběžnější využívání služeb České pošty. Tato metoda vyžaduje návštěvu pobočky příslušné instituce, identifikaci, tedy ověření totožnosti pracovníkem a uhrazení nákladů spojených se službou. V konkrétním případě daňového přiznání je lhůta pro odevzdání dokumentu striktně omezená, tudíž občas musí počítat s určitou délkou procesu doručování zásilky.

Druhou variantou je osobní doručení na úřad. Tato metoda sice vyžaduje osobní účast na podatelně úřadu, avšak ze své podstaty umožňuje přímou a

okamžitou kontrolu správnosti formuláře úředníkem a v případě jeho nesprávnosti též případné upravení obsahu.



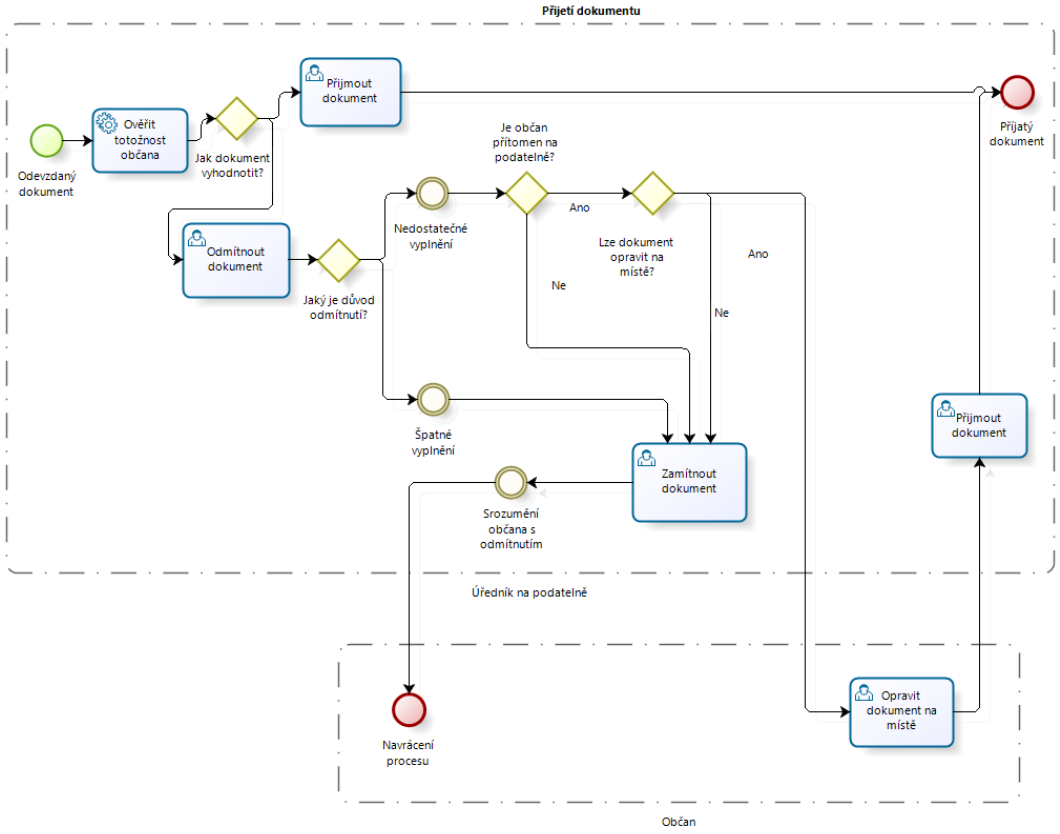
Obrázek 2 – Doručení, Lukáš Konvalina

6.2.3. Přijetí dokumentu

Úředník na podatelně může formulář přijmout, či odmítnout, nesplňuje-li některé povinné údaje. Odmítnutí může proběhnout z důvodu špatného vyplnění. Tím je zapříčiněn návrat k počátku procesu a jeho opakování. Odmítnutí může proběhnout též z důvodu nedostatečného vyplnění. Pokud nesprávné, či chybějící údaje mají charakter pouze drobných a opravitelných chyb, je na základě praktické zkušenosti teoreticky možné formulář správně vyplnit přímo na podatelně, bez nutnosti návratu na počátek procesu.

V případě možného upravení dokumentu je dokument na místě vyplněn a přijat úřadem. V případě nemožnosti upravení dokumentu, je dokument úřadem odmítnut a je třeba postupovat znovu od výchozího bodu procesu. Možnost teoretické opravy dokumentu na místě, je pochopitelně podmíněna osobní účastí, tedy nikoli za využití doručovatelských služeb.

Výstupní bod: Správně vyplněný dokument byl podatelnou úřadu přijat.



Obrázek 3 – Přijetí dokumentu, Lukáš Konvalina

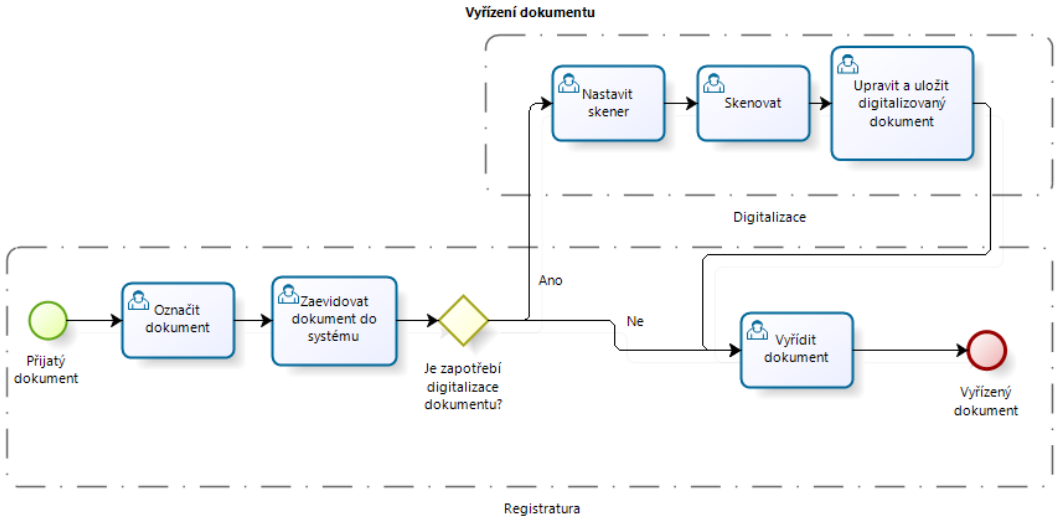
6.2.4. Vyřízení dokumentu

Správně vyplněný dokument byl podatelnou přijat a v rámci spisové služby úřadu s ním musí být patřičně naloženo, dle obecných požadavků a kritérií.

Probíhá proces označení dokumentu a zaevidování přijetí dokumentu od občana do příslušné evidence. Zajištění dokumentu podacím razítkem a následné předání dokumentu do kanceláře (registratury). Úředník pracuje s listinným dokumentem, ale povaha dokumentu může vyžadovat jeho okamžitou digitalizaci. Před rozmachem digitálních technologií probíhala evidence převážně písemně. V současnosti je evidence digitální za pomoci technologie skenování a příslušného software. Proběhne proces digitalizace příslušným pracovníkem a uložení naskenovaného dokumentu do příslušné evidence.

Zároveň je provedeno vyřízení věcného obsahu dokumentu, což může vyžadovat informování příslušné instituce, či fyzické osoby, nebo zápis do patřičného registru, případně fyzické doručení dokumentu jinému subjektu. Po

vyřízení je dokument následně odeslán k uložení v archivu. Dokument je založen do spisu (případně dojde k vytvoření nového spisu, je-li to zapotřebí) a dojde k jeho archivaci.



Obrázek 4 – Vyřízení dokumentu, Lukáš Konvalina

6.3. Obecný koloběh běžného dokumentu (např. daňového přiznání) po eIDAS

Systémem eIDAS nejvíce ovlivněná oblast v otázce koloběhu obvyklých dokumentů je na přelomu činnosti občana a instituce. Proto ostatní části diagramů nebudou příliš odlišné.

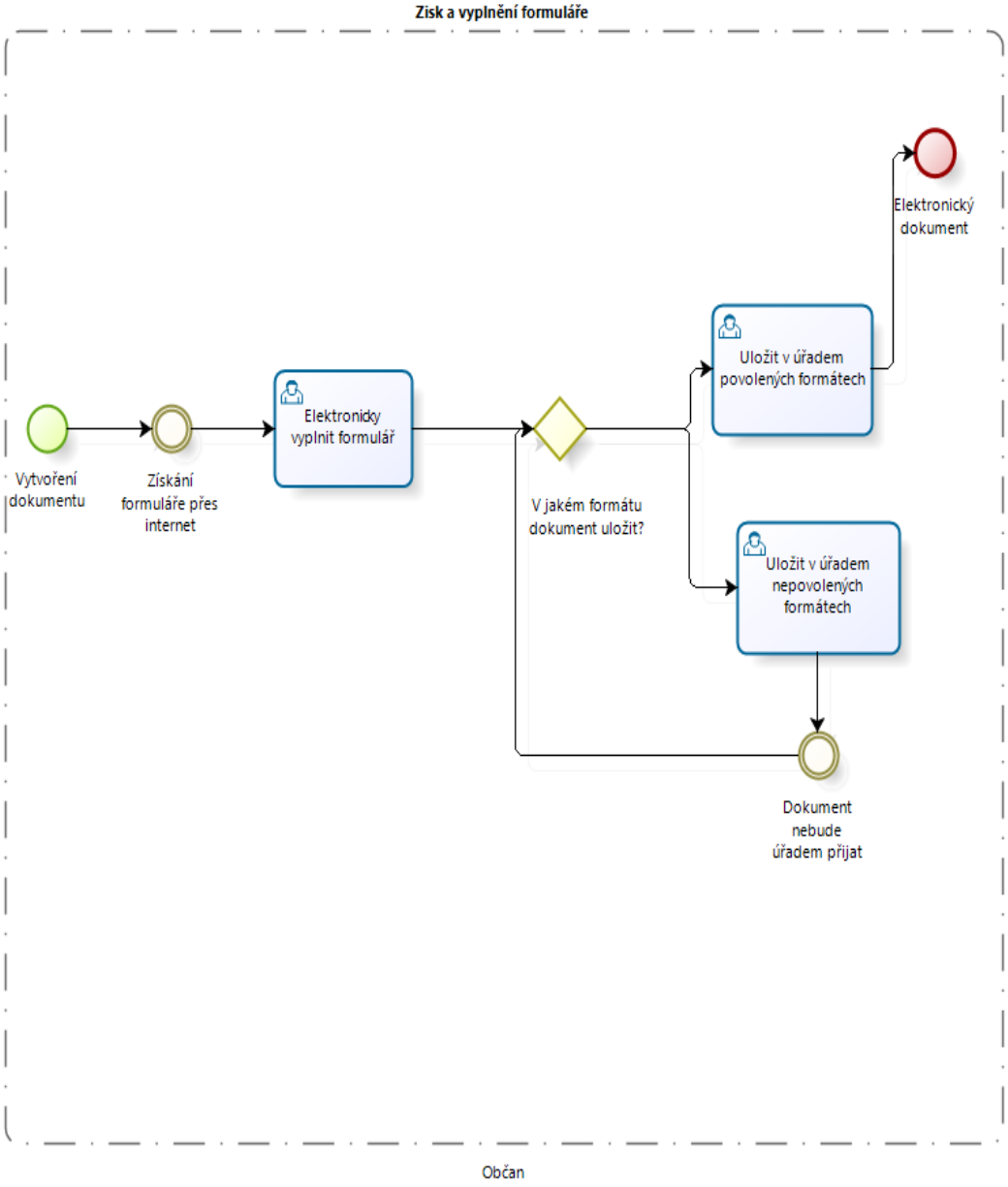
6.3.1. Zisk a vyplnění formuláře

Výchozí situace: Uživatel má povinnost vyplnit a odeslat formulář na patřičný úřad.

U analogového koloběhu dokumentu bylo možné kombinovat dokument tištěný i digitální. To v případě koloběhu využívající nařízení eIDAS možné není,

neboť celý proces se odehrává pouze na elektronické úrovni. Získání formuláře je možné pouze elektronicky přes internet.

Následuje elektronické vyplnění formuláře. Požadavkem je zcela nezbytně připojení k internetu a instalace příslušného software schopného s elektronickým formulářem pracovat (přečíst jej). Dokument musí být následně uložen ve formátu, který úřad přijímá (seznam akceptovatelných formátu by měl být uveden na webových stránkách konkrétního úřadu).



Obrázek 5 – Zisk a vyplnění formuláře, Lukáš Konvalina

6.3.2. Doručení dokumentu

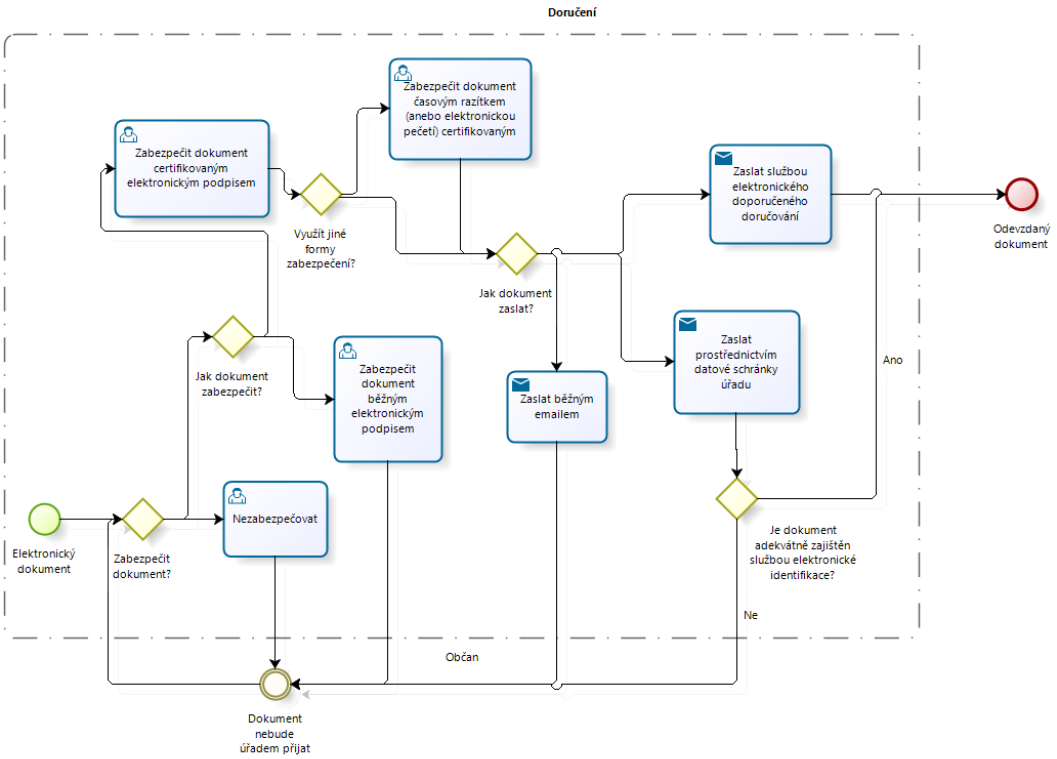
Vyplněný formulář je připravený na doručení na podatelnu úřadu. Pokud ale dokument nebude zajištěn žádnou ze služeb elektronické identifikace dle zákona, úřad jej nemusí (resp. nesmí) přijmout. Dokument tedy bude odmítnut a proces se vrátí zpět na počátek.

Pokud dokument bude zajištěn službou elektronické identifikace, je nutné zvolit její vhodný způsob, který bude odpovídat povaze dokumentu, citlivosti jeho obsahu a požadavkům úřadu. Například právnická osoba bude dokument pravděpodobně zabezpečovat i elektronickou pečetí. Elektronický dokument také musí mít takový formát, který úřad přijme. V případě, že dokument je zajištěn službami elektronické identifikace, ale je uložen v nevhodném formátu, může být dokument úřadem odmítnut a bude požadováno nové zaslání.

Zajištění dokumentu by mělo proběhnout minimálně elektronickým podpisem. Takový proces vyžaduje nákup certifikátu. Při zohlednění ceníku České pošty (nejběžnější poskytovatel certifikačních služeb v ČR) vychází osobní certifikát na 396 Kč (vč. DPH) na jeden rok.[31] Dalším možným způsobem zajištění dokumentu je časové razítko, čímž bude zajištěna shodnost dat od orazítkování po dobu platnosti razítka.

Další využitou službou může být datová schránka, ale ta nemusí být za všech okolností dostatečná. Například při posílání ze zahraničí je v rámci celoevropského eIDAS možná pouze služba elektronického doporučeného doručování (dle nařízení eIDAS), která zajišťuje jistotu akceptování přijetí dokumentu institucí v členském státě EU se zavedeným eIDASem.

[31] Kvalifikované certifikáty. *Česká pošta* [online]. [cit. 2018-04-10]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/kvalifikovane-certifikaty

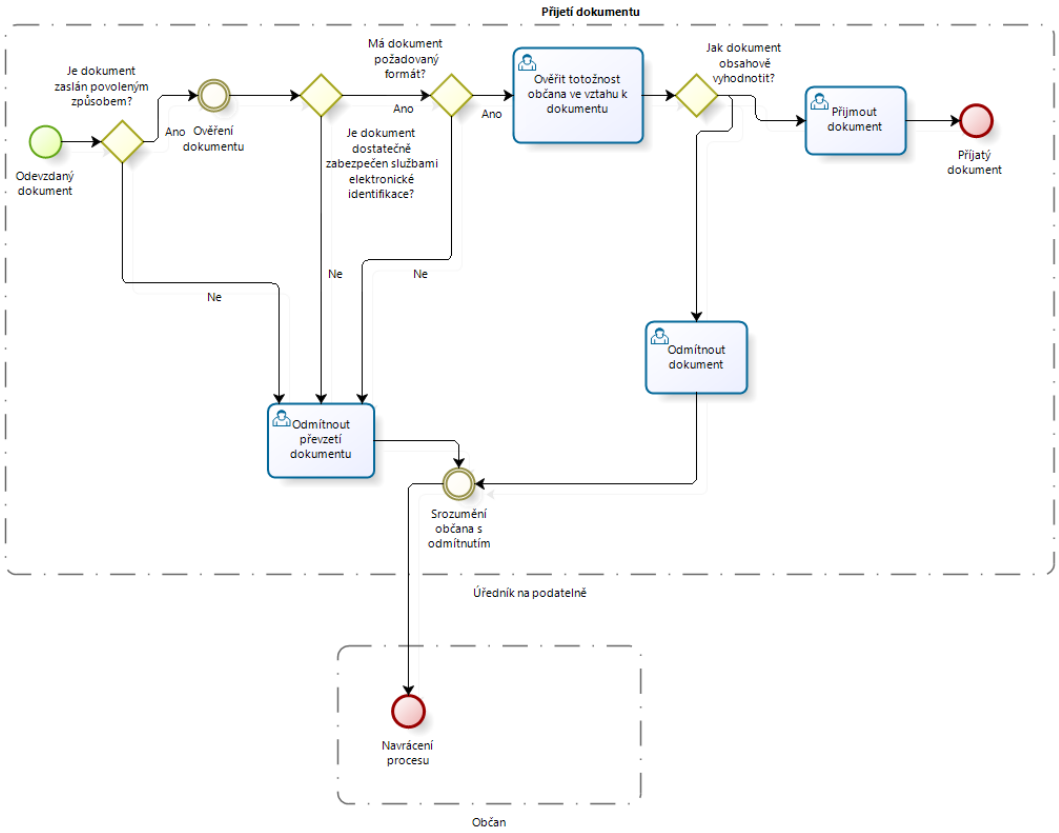


Obrázek 6 - Doručení, Lukáš Konvalina

6.3.3. Přijetí dokumentu

Protože digitální dokument je opatřený certifikovaným elektronickým podpisem (popř. dalšími službami), je jeho právní hodnota stejná jako v případě analogového ručně podepsaného dokumentu. Dokument proto musí být úřadem přijat. V případě, že dokument nesplňuje některou náležitost, bude jeho přijetí zamítnuto a odesílatel bude o procesu odmítnutí informován.

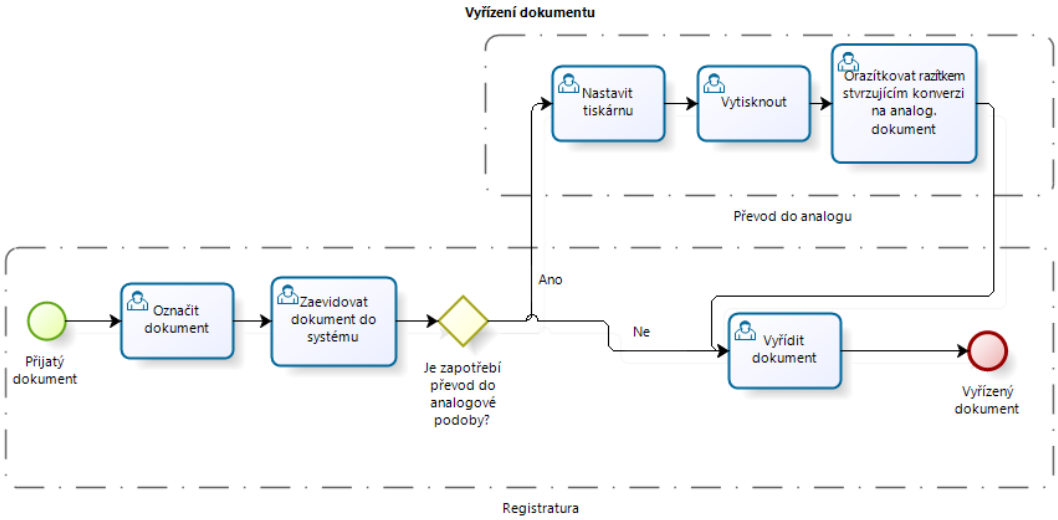
Oproti doručování před eIDAS (tedy u analogového dokumentu) má tento proces mnohem více podmínek, které mohou vést k odmítnutí přijetí dokumentu. Rovněž zde neexistuje možnost přímé komunikace s úředníkem na podatelně a tedy možnosti opravení chyb. Výstupním bodem této fáze procesu je přijetí správně vyplněného dokumentu obsahujícího všechny náležitosti.



Obrázek 7 – Přijetí dokumentu, Lukáš Konvalina

6.3.4. Vyřízení dokumentu

Správně vyplněný dokument byl podatelnou přijat a v rámci spisové služby úřadu s ním musí být patřičně naloženo, dle obecných požadavků a kritérií. Označení dokumentu a zaevidování přijetí dokumentu od občana do příslušné evidence a následné předání dokumentu do kanceláře (registratury). V případě potřeby konverze digitálního dokumentu do analogové podoby, je nutné stvrzení obsahu razítkem tak aby bylo zajištěno, že jak původní elektronický, tak i nově vzniklý digitální, mají stejný obsah a stejnou právní hodnotu. Vyhotovení dokumentu, uložení a jeho archivace



Obrázek 8 – Vyřízení dokumentu, Lukáš Konvalina

7. Výhody a nevýhody eIDAS

Nové možnosti zavedené systémem eIDAS se v běžném procesu koloběhu dokumentu vztahují především k otázce identifikace. Zákon 250/2017 vyžaduje postavení elektronických dokumentů s certifikovaným podpisem na stejnou právní úroveň jakou má listinný podepsaný dokument. Využití služeb elektronické identifikace má nesporné výhody v otázce dostupnosti, rychlosti a flexibility. Je však finančně mnohem náročnější a rovněž vyžaduje dostatečné znalosti. Mluvíme tu nejen o znalostech práce s dokumentem, jeho zajištění službami elektronické identifikace, ale též o pochopení samotného procesu, který dokumentu zajišťuje zabezpečení.

7.1. eIDAS z pohledu občana

Jestliže občan nechce riskovat možnosti zneužití, či podvodu, je zcela nezbytné, aby proces zabezpečení chápal po technické stránce tak dobře jako proces vlastnoručního podepsání listinného dokumentu. V opačném případě se vzhledem ke složitosti zabezpečení může stát obětí podvodu nebo se dopustit chyby.

Využití eIDAS se stává nespornou výhodou pro větší firmy s dostatečným obratem a kvalifikovanými zaměstnanci, pro které je finanční náročnost identifikačních služeb zcela eliminována ušetřením času díky rychlosti a flexibilnosti. Možnost komunikace s úřadem bez osobní účasti je rovněž nespornou výhodou.

Pro jednotlivce, či malé firmy je však využívání služeb eIDAS stále nevýhodné. Aby se toto změnilo, není řešením znesnadnit občanům doručování listinných dokumentů nebo dokonce zavést přímé nařízení nutnosti využívání elektronických dokumentů, nýbrž zlehčení ekonomické náročnosti a též osvěta společnosti v otázkách eIDAS. Lidé mohou začít důvěřovat jen tomu, co dobře znají.

7.2. eIDAS z pohledu instituce

Pro instituce znamená nařízení eIDAS navýšení rozpočtu (obecně vzato). Technické zázemí musí být schopné přijímat elektronické dokumenty a v případě potřeby je převádět do požadovaných formátů. Protože některé druhy dokumentů jsou vyžadovány i v listinné podobě, je počet jednotlivých dokumentů výrazně vyšší. Samozřejmostí je potřebná kvalifikace pracovníků, tedy případné přeškolování stávajících zaměstnanců, aby byli schopni s dokumenty pracovat a též přijímání zaměstnanců nových.

7.3. Vztah SOA Hradec Králové k nařízení eIDAS v rámci předarchivní péče a spisové služby

V rámci případové studie bylo vedení státního okresního archivu Hradec Králové položeno několik otázek. Jednalo se o otázky vztahující se ke změnám, které archivu přineslo nařízení eIDAS.

Na otázky odpovídal vedoucí archivu Mgr. Radek Pokorný, dne 30. 4. 2018.

1) Co znamenalo nařízení eIDAS pro archiv? K jakým změnám muselo dojít v rámci spisové služby?

V rámci projektu úpravy spisové služby došlo mimo jiné i k realizaci zavedení nových kvalifikovaných podpisů, časových razítek a pečetí. Používaný systém spisové služby musel být upraven tak, aby dokázal identifikovat certifikáty vydané všemi evropskými certifikačními autoritami v souladu s eIDAS a používat nové certifikáty.

2) K jakým změnám muselo dojít v rámci procesů předarchivní péče? Byly vyžadované změny výhodné pro chod archivu?

Žádné změny v procesech předarchivní péče v souvislosti s Nařízením jsme nezaznamenali. Výběr archiválií ve skartačním řízení elektronickou formou je v současnosti předáván buď informačním systémem datových schránek, nebo na technických nosičích. V případě datových schránek se průvodní dokumenty podepisují a přílohy nově opatřují elektronickou pečetí. V souvislosti s přípravou

na platnost Nařízení více původců začalo ve skutečnosti využívat časová razítka, což však byla de iure jejich povinnost i dle starší platné české legislativy.

3) Jaký byl alespoň hrubý časový horizont, od kdy SOA začal provádět kroky, aby vyhověl nařízení eIDAS, tedy hlavně zákonu 297/2016.

V našem konkrétním případu byl přechod součástí projektu úpravy spisové služby, která se musí přizpůsobit podmínkám aktualizovaného znění Národního standardu pro elektronické spisové služby z roku 2017, které vejde v úplnou účinnost od července 2018. Tento projekt běží od července loňského roku.

4) Bylo nutné měnit personál nebo pracovní místa? Přijímat nové zaměstnance? Školit? Nové pracovní pozice?

Potřeba pracovních míst nevznikla. V rámci přípravy rozšíření digitálního úřadování (např. oběh elektronických faktur) byl rozšířen okruh uživatelů kvalifikovaného elektronického podpisu. Dále byl pro každý spisovenský uzel organizace pořízena elektronická pečeť (elektronické razítko náš archiv v minulosti nevyužíval). Bylo tak nutné vyškolit uživatele na používání elektronického podpisu umístěného na tokenu (kvalifikovaném prostředku pro vytváření elektronických podpisů) v souladu s eIDAS a používání pečeti v rámci spisové služby.

5) Je o služby elektronické identifikace v otázce transakcí mezi původci a archivem zájem? Roste počet využití služeb eIDAS v posledních letech? Jsou v otázce transakcí nějaké komplikace?

Výhradní formou elektronické identifikace mezi původci a archivem je v současnosti elektronický podpis, pečeť a časové razítko používané ve vzájemné komunikaci. Jejich použití (místo pečeti razítko) bylo teoreticky stejné před i po eIDAS. Dle Nařízení je jasnější užití pečeti - jen pro ty dokumenty, které nejsou podepsány. V reálném provozu se ukazuje, že původci, kteří měli stejné povinnosti již dříve, ale nepostupovali zcela správně (např. používali jen elektronické podpisy), v souvislosti s blížícím se koncem přechodového období a povinností používat výhradně kvalifikovaný podpis, více obecně plní své povinnosti v této oblasti, např. více se začaly používat časová razítka. Jedná se však jen o pocit z korespondence s nimi, naše kontroly v oblasti spisové služby

neprobíhají v takových počtech a nejsou primárně zaměřeny na tuto oblast, abychom z nich mohli usuzovat více.

6) Byl eIDAS nákladný? Co bylo největším problémem po ekonomické stránce?

Konkrétní výdaje generovaly nové tokeny pro každého uživatele a školení uživatelů. Dále pak elektronické pečeti, rozšířený počet uživatelů el. podpisu. Systém elektronické spisové služby se musel upravit tak, aby byl schopen identifikovat Naše výdaje byly spojeny i s dalšími úpravami ve spisové službě a není lehké je přesně určit, pohybovaly se celkově v řádech desítek tisíc korun. Fixní výdaje by neměly být odlišné od těch, které měly organizace plně respektující platnou českou legislativu již před platností Nařízení. V praxi bude nárůst ročních výdajů především u původců, kteří platnou legislativu dříve nedodržovali, zejména v oblasti nevyužívání časových razítek.

7) Jaká rizika může nařízení eIDAS mít pro instituce i původce?

Pokutu za nedodržování stanovených pravidel. Tlak na úpravu spisové služby či vnitřních procesů, potřebu proškolení všech dotčených pracovníků.

8. Analýza rizik eIDAS

Pro analýzu možných úskalí zavedení eIDAS, je vycházeno z jednoduché tabulky, která tvoří průnik mezi dvěma faktory – faktorem předpokládané vážnosti hrozby a faktorem předpokládané ovlivnitelnosti hrozby občanem. Protože zdrojem pro analýzu nejsou žádná konkrétní data, nýbrž jednotlivá úskalí vycházející z výše popsaných a znázorněných situací, není cílem této analýzy poukázat na aktuální problémy, ale na problémy možné (bez ohledu na jejich četnost v praxi).

Faktor hrozby	Obecný popis situace
Úroveň 1	Nízké ohrožení občana s minimálním dopadem na jeho bezpečnost.
Úroveň 2	Střední ohrožení. Běžné ohrožení, které může občanovi způsobit potíže.
Úroveň 3	Vysoké ohrožení. Ohrožení, které může mít pro občana velmi vážné důsledky, může přivodit ohrožení jeho citlivých údajů.
Úroveň 4	Extrémní ohrožení. Průlom bezpečnostními opatřeními, v důsledku kterého jsou údaje občana již přímo zneužity pro podvodnou činnost.
Faktor ovlivnitelnosti	**Obecný popis situace**
Úroveň A	Vysoká. Občan může svými kroky snadno a bez obtíží předejít hrozbě.
Úroveň B	Průměrná. Občan může předejít hrozbě s využitím vysokých stupňů zabezpečení a ochrany, což vyžaduje pokročilé znalosti.
Úroveň C	Nízká. Občan i s velmi vysokými znalostmi může předejít hrozbě pouze částečně.
Úroveň D	Žádná. Občan nemůže předejít hrozbě.

Tabulka 2 – Hrozby, Lukáš Konvalina

8.1. Stanovení rizik

Tabulka stanovuje 30 rizikových situací, k nimž teoreticky může při využívání eIDAS dojít a které mohou mít bezpečnostní dopad na uživatele. Takovýchto situací může být jistě mnohem více, ale pro potřeby této analýzy, jež se vztahuje na rizika související s občanem jakožto uživatelem, je počet rizik dostatečný.

Vyhodnocení míry rizik je sice podřízené pohledu autora této práce, nicméně je zpracováváno objektivně, ve vztahu k informacím uvedeným v práci a rovněž z pohledu občana jakožto uživatele.

Situace	Riziko
Nedostatečný počet zaměstnanců v institucích využívající eIDAS.	2-D
Nedostatečná kvalifikovanost zaměstnanců institucí v otázkách eIDAS.	3-D
Nedostatečná znalost občana v otázkách eIDAS	4-B
Zneužití osobních údajů občana poskytovatelem certifikačních služeb.	4-D
Zneužití osobních údajů institucí stojící nad poskytovatelem certifikačních služeb (ministerstvo, stát...)	4-D
Nedostatečné šifrování klíčů u služeb elektronické identifikace, provozované institucí.	3-D
Nedostatečné zabezpečení při přesunu dokumentu od občana do cílové datové schránky.	3-D
Ztráta soukromých klíčů (občanem)	3-A
Ztráta veřejných klíčů (třetí stranou)	3-D
Selhání HW / SW instituce a nemožnost momentálního využití služeb eIDAS.	2-D
Selhání HW občana a nemožnost využití služeb eIDAS.	2-B
Výpadek elektřiny.	1-D
Nedostatečné pokrytí internetu v oblasti občana	2-B
Nedostatečné zabezpečení HW a SW občana vůči virům	2-C
Omezená doba platnosti certifikátů u služeb eIDAS	2-A
Přílišná cena služeb eIDAS	3-D
Nedostatečná analýza rizik poskytovatele služeb vytvářejících důvěru a následný nárůst potenciálního ohrožení uživatelů.	3-D
Nedostatečná flexibilita poskytovatele vůči úpravám zákonů.	3-D
Nedostatečně poskytnuté informace pro občana ohledně principů zabezpečení a správnosti využití služeb elektronické identifikace.	3-D
Včasné řešení bezpečnostních průlomů a jiných incidentů poskytovatelem (zabránění úniku dat).	3-D
Pomalé řešení bezpečnostních průlomů a jiných incidentů poskytovatelem.	4-D
Zatajování informací o bezpečnostních průlomech hackery.	4-D
Zneužití osobních dat a certifikací uživatelů hackery	4-D
Porušení zákona poskytovatelem a riskování odebrání certifikačních služeb.	3-D
Ztráta povolení k poskytování certifikačních služeb.	4-D
Poškození reputace poskytovatele služeb.	3-D
Nedostatečné zabezpečení dat uživatelů poskytovatelem.	3-D

Výpadky serverů, či jiné dočasné znemožnění využití poskytovaných služeb	1-D
Cenzura (či jiné omezení) komunikace s poskytovatelem služeb třetí stranou.	3-D
Nedostatečné prokazování vlastnictví certifikace poskytovatelem služeb eIDAS	1-D

Tabulka 3 – Situace, Lukáš Konvalina

8.2. Vyhodnocení rizik

	Hrozba 1	Hrozba 2	Hrozba 3	Hrozba 4
Ovlivnitelnost A	0	1	1	0
Ovlivnitelnost B	0	2	0	1
Ovlivnitelnost C	0	1	0	0
Ovlivnitelnost D	3	2	13	6

Tabulka 4 – Vyhodnocení rizik, Lukáš Konvalina

Výsledek analýzy potencionálních hrozeb dokazuje, že velmi velké množství situací (více než 70%) nemůže sám občan, jakožto uživatel služeb eIDAS ovlivnit. Velké procento z těchto prakticky neovlivnitelných situací navíc představuje velkou hrozbu v otázce zabezpečení dat vůči jejich zneužití. S využíváním služeb eIDAS tedy občan může na teoretické úrovni velmi riskovat.

Nyní by samozřejmě bylo možné zaměřit se na třetí faktor a tím by byla četnost těchto situací v reálné praxi. Tedy jak velká je pravděpodobnost, zda k dané situaci skutečně dojde. Z toho důvodu výpovědní hodnota této tabulky spočívá především ve sloupci Ovlivnitelnosti.

Závěr

Proces elektronické identifikace prostřednictvím nařízení eIDAS v současnosti vrcholí. Přesto se domnívám, že práce dokázala, že nařízení eIDAS obsahuje mnoho úzkých míst, které ani násilné zavedení nemůže vyřešit. Nejedná se jen a pouze o potíže s rychlostí zaváděním eIDASu, nebo nedostatkem kvalifikovaných pracovníků (věřím, že to vše postupem doby vyřeší faktor času), ale především lze úskalí vnímat v základních stavebních prvcích, včetně poněkud ironické skutečnosti, kdy uživatel přestává mít možnosti identifikace své i svých dokumentů ve vlastních rukou.

Přestože zde stojí dvě zdánlivě samostatné barikády, jedna v podobě občanů, druhá v podobě institucí, nachází se zde několik shodných kritických míst. Ekonomická situace a finanční náročnost služeb elektronické identifikace je prvním z nich a jedná se výraznou komplikací jak pro ekonomicky slabší občany, tak i pro menší úřady, jejichž rozpočet zavedení eIDASu postihuje a vyčerpává. Nařízení eIDAS pro ně znamená výdaje. Pro občany zatím nepovinné, ale pro státní úřady již brzy ano a lze si jen domýšlet, jak dlouho potrvá, než i občan nebude stát před otázkou, zda zaslat veledůležitý dokument na podatelnu úřadu osobně či elektronicky, nýbrž jakého poskytovatele certifikátů vybrat, aby se náklady na doručení dokumentu co nejvíce blížily době, kdy ještě bylo možné doručovat dokumenty v listinné podobě.

Provedená analýza rizik eIDAS byla zaměřena na vytyčení možných rizikových situací, jejich potenciální vážnost a především jejich možnou ovlivnitelnost občanem, tedy uživatelem služeb eIDAS. Analýza i přes svoji omezenou velikost dokázala, že existuje množství potenciálních bezpečnostních hrozeb, přičemž mnoho z nich může mít fatální dopady na bezpečnost dat a zároveň jen velmi malé procento z nich, může občan jakožto uživatel služeb eIDAS přímo ovlivnit. Bezpečnost citlivých osobních údajů i přenášených dat se tak přesouvá k třetím stranám a občan alias uživatel je nucen důvěřovat jak těmto stranám, tak i institucím, které stojí nad nimi a které plní kupříkladu funkci dohlížitele. Samozřejmě lze namítnout, že některé potenciální kritické situace uvedené v analýze jsou z hlediska pravděpodobnosti téměř vyloučené. Tento fakt

ale stále nic nemění na jejich možné existenci, přičemž otázka pravděpodobnosti skutečného výskytu je vzhledem ke stále ještě velké čerstvosti nařízení eIDAS těžko zodpověditelná.

Tato práce by mohla pomoci nalézt určitá riziková místa v problematice eIDAS a zároveň by se mohla stát jakousi základnou, či odrazovým můstkem pro práci jinou, která by se kupříkladu mohla zabývat zkoumáním rizikových situací v reálné praxi a nacházením vhodných řešení jak těmto situacím předejít.

Použité zdroje a literatura

GALVAS, Miroslav. Datové schránky. *Epravo.cz* [online]. 13. července 2017 [cit. 2018-04-11]. Dostupné z: https://www.epravo.cz/top/clanky/datove-schranky-106059.html

KAPUCIÁNOVÁ, Aneta. Služba Spolužáci.cz na konci srpna končí. *Seznam.cz: Sblog* [online]. 4. dubna 2018 [cit. 2018-04-11]. Dostupné z: https://blog.seznam.cz/2018/04/sluzba-spoluzaci-cz-na-konci-srpna-skonci/

Kvalifikované certifikáty. *Česká pošta* [online]. [cit. 2018-04-10]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/kvalifikovane-certifikaty

LECHNER, Tomáš. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013, 256 s. ISBN 978-80-87576-41-0.

Nařízení Evropského parlamentu a rady EU 2016/679. *EUR-Lex: Přístup k právu evropské unie* [online]. 27. dubna 2016 [cit. 2018-04-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:32016R0679

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014. *EUR-lex* [online]. 2014, 23. července 2014 [cit. 2018-01-06]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN

Ondřej Felix. Cíle a oblasti regulace eIDAS (Ondřej Felix). In: *Youtube* [online]. 15. 6. 2016 [cit. 2018-03-15]. Dostupné z: https://www.youtube.com/watch?v=loLkgFpzVUk

PETERKA, Jiří. *Báječný svět elektronického podpisu* [online]. Autorská verze. Praha: CZ.NIC, 2011 [cit. 2018-01-18]. ISBN 978-80-904248-3-8.

PETERKA, Jiří. Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. *Lupa.cz: Server o českém internetu* [online]. 20. září 2011 [cit. 2018-03-25]. Dostupné z: https://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/

Petr Kuchař. Plány MV (Petr Kuchař - hlavní architekt eGovernmentu MV). In: *Youtube* [online]. 20. 4. 2017 [cit. 2018-03-15]. Dostupné z: https://www.youtube.com/watch?v=Z-fPkOC9tM4

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ: Digitální agenda pro Evropu. *EUR-Lex* [online]. 26. srpna, 2010 [cit. 2018-04-15]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52010DC0245R(01)&from=EN

VAŠÍČEK, Petr. Úvod do BPMN. *BPM prakticky* [online]. 2018 [cit. 2018-04-11]. Dostupné z: http://bpm-sme.blogspot.cz/2008/03/3-uvod-do-bpmn.html

Vyhláška č. 259/2012 Sb.: Vyhláška o podrobnostech výkonu spisové služby. *Zákony pro lidi* [online]. 2015 [cit. 2018-01-06]. Dostupné z: https://zakonyprolidi.cz/cs/2012-259/zneni-20150101

Základní příručka. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-04-06]. Dostupné z: https://www.uoou.cz/zakladni%2Dprirucka/ds-4744/p1=4744

Zákon č. 250/2017 Sb.: Zákon o elektronické identifikaci. *Zákony pro lidi* [online]. 2017 [cit. 2018-01-08]. Dostupné z: https://zakonyprolidi.cz/cs/2017-250/zneni-20180701

Zákon č. 297/2016 Sb.: Zákon o službách vytvářejících důvěru pro elektronické transakce. *Zákony pro lidi* [online]. 2016 [cit. 2018-02-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297