VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IMPLEMENTACE DYNAMICKÉHO BIOMETRICKÉHO PODPISU V PODNIKU PO NABYTÍ ÚČINNOSTI NAŘÍZENÍ EIDAS

IMPLEMENTATION OF DYNAMIC BIOMETRIC SIGNATURE IN THE COMPANY AFTER THE ENTRY INTO FORCE OF THE REGULATION EIDAS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Pavla Jelečková**
AUTHOR

VEDOUCÍ PRÁCE — **prof. Ing. Vladimír Smejkal, CSc.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Pavla Jelečková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**prof. Ing. Vladimír Smejkal, CSc.**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Implementace dynamického biometrického podpisu v podniku po nabytí účinnosti nařízení eIDAS

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Vytvoření obecně použitelné metodiky pro implementaci dynamického biometrického podpisu v podniku po nabytí účinnosti nařízení eIDAS a s přihlédnutím k dalším právním předpisům a technickým normám.

Základní literární prameny:

DAWSON, M., D. R. KISKU, P. GUPTA, J. K. SING a W. LI. Developing next-generation countermeasures for homeland security threat prevention. Hershey PA: IGI Global, 2017. 428 s. ISBN 978-1522-50-7031.

MATES, P. a V. SMEJKAL. E-government v České republice: Právní a technologické aspekty. 2. vyd. Praha: Leges, 2012. 464 s. ISBN 978-80-87576-36-6.

SMEJKAL, V., J. KODL a M. UŘIČAŘ. Elektronický podpis podle nařízení eIDAS. Revue pro právo a technologie, VI., 2015. č. 11, s. 189-235. ISSN 1805-2797.

SMEJKAL, V. a K. RAIS. Řízení rizik ve firmách a jiných organizacích. 4. vyd. Praha: Grada, 2013. 488 s. ISBN 978-80-247-4644-9.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

L. S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

B. Půža

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Diplomová práce se zaměřuje na problematikou elektronického podepisování v České republice po nabytí účinnosti nařízení eIDAS. Specifikuje klíčové pojmy z této oblasti, pojednává o alternativách elektronického podepisování v rámci podniku, srovnává vlastnosti kryptografického elektronického podpisu a dynamického biometrického podpisu. V rámci hlavního cíle práce, kterým je implementace dynamického biometrického podpisu v podniku, je navrženo řešení procesu schvalování daňových dokladů podniku. V závěru je provedeno ekonomické porovnání papírového a elektronického řešení.

Klíčová slova

dynamický biometrický podpis, zaručený elektronický podpis, nařízení eIDAS, kvalifikované služby vytvářející důvěru

Abstract

The diploma thesis focuses on the problematics of elektronic signing in the Czech Republic after the Entry into Force of Regulation eIDAS. It specifies the key words in this area, compares the properties of cryptographic electronic signature and dynamic biometric signature. Within the main objective of the work, which is the implementation of dynamic biometric signature in the company, a solution is proposed to the process of approving business tax forms. At the end, an economic comparison of paper and electronic solutions is made.

Key words

dynamic biometric signature, advanced elektronic signature, regulation eIDAS, qualified trust services

Bibliografická citace

JELEČKOVÁ, P. *Implementace dynamického biometrického podpisu v podniku po nabytí účinnosti nařízení eIDAS*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 86 s. Vedoucí diplomové práce prof. Ing. Vladimír Smejkal, CSc.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašují, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským, ve znění pozdějších předpisů).

V Brně dne 21. května 2017

……

Poděkování

Ráda bych poděkovala svému vedoucímu diplomové práce prof. Ing. Vladimíru Smejkalovi, CSc. za odborné rady a připomínky při zpracování této diplomové práce.

OBSAH

1 ÚVOD

V našem každodenním životě se setkáváme se situacemi vyžadujícími ověření naší identity. Tento proces ověření totožnosti je známý pod pojmem autentizace. Totožnost můžeme prokazovat nejrůznějšími způsoby, přičemž lze zmínit tři základní metody:

- „Co vím“ – metoda založená na znalosti tajné informace, která je známá pouze oprávněné osobě. Příkladem může být znalost hesla či PINu.
- „Co mám“ – metoda založená na vlastnictví nějakého předmětu, například tokenu, kterým prokážeme svoji identitu, či čipové karty apod.
- „Co jsem“ – metoda, při které probíhá ověření totožnosti na základě biometrických charakteristik jedince. Jako příklad lze uvést sken oční rohovky či dynamiku podpisu.

V případě, že výše uvedené tři metody kombinujeme, mluvíme o tzv. vícefaktorové autentizaci, jejímž účelem je využít výhody jednotlivých metod, a naopak eliminaci jejich nevýhod.

Autentizaci definujeme jako ověření daných entit pomocí předmětů (průkazy, karty), projevy osobní povahy (hlas, podpis), osobními vlastnostmi (oční duhovka) nebo znalostmi (PIN, heslo). V současné době je v případě listiny prostředkem k autentizaci mj. vlastnoruční podpis, pečeť či razítko. U elektronického dokumentu jsou autentizačními prostředky elektronické podpisy a elektronické pečetě. V případě podpisu se může jednat o podpis vlastnoruční, elektronický analogový (obrázek) nebo digitální (kryptografický), či dynamický biometrický, přičemž poslední z nich je kombinací vlastnoručního a elektronického podpisu.

V této diplomové práci se zaměřuji na biometrické metody, konkrétně na implementaci dynamického biometrického podpisu, a to v rámci právního stavu po nabytí účinnosti Nařízení EU o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (dále také jen Nařízení eIDAS nebo Nařízení)[1], které vstoupilo v platnost 1. července 2016. Aktuálně se nacházíme ve dvouletém přechodném období

[1] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

od nabytí účinnosti Nařízení, kdy členské státy EU mají čas na to, aby se vypořádali s částmi, které Nařízení nechává k řešení na národní úrovni, a začali se jím plně řídit. To se v ČR stalo v rámci zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, který vstoupil v platnost dnem vyhlášení, tj. 19. září 2016.

Teoretická část této práce je rozdělena na dvě části – první se týká legislativy kolem elektronického podepisování, druhá porovnáním kryptografického elektronického podpisu s dynamickým biometrickým podpisem z hlediska technologického.

Další část práce, tvoří analýza současného stavu podniku, v němž bude implementován dynamický biometrický podpis do procesu schvalování faktur (daňových dokladů). Začátek této části je věnován popisu stávajících procesů a jejich zhodnocení.

Návrhová část je popisuje navrhované řešení z hlediska funkčního, procesního, hardwarového a softwarového či bezpečnostního. Poslední část této kapitoly je věnována finančnímu zhodnocení návrhu, porovnání nákladů na původní papírové řešení s novým elektronickým řešení a porovnání dynamického biometrického podpisu s podpisem vlastnoručním z hlediska bezpečnostních aspektů.

2 CÍL PRÁCE A METODIKA

Cílem této diplomové práce je vytvoření obecně použitelné metodiky pro implementaci dynamického biometrického podpisu v podniku po nabytí účinnosti nařízení eIDAS, s přihlédnutím k dalším právním předpisům a technickým normám. Dílčími cíli je shrnout novou platnou legislativu týkající se elektronického podpisování v České republice a porovnat kryptografický elektronický podpis s dynamickým biometrickým podpisem z hlediska technologického a bezpečnostního. Na základně analýzy současného stavu procesů v podniku bude formulován návrh implementace biometrického podpisu do procesu.

Vzhledem k tomu, že množství procesů, které probíhá v podnicích, je značné a jednotlivé procesy se jak po stránce obsahové, tak organizační a začleněním do existujících informačních systémů značně odlišují, po dohodě s vedoucím práce jsem se soustředila na jednu z nejčastějších oblastí podnikových procesů, a to implementaci dynamického biometrického podpisu (dále také jen DBP) do procesu schvalování faktur (daňových dokladů).

3 TEORETICKÁ VÝCHODISKA PRÁCE

Teoretická část práce je rozdělena na dvě části, z nichž první se zabývá legislativou související s elektronickými podpisy. Druhá část popisuje principy kryptografického elektronického podpisu a dynamického biometrického podpisu.

3.1 Legislativa upravující elektronický podpis

Legislativa týkající se elektronického podpisu zahrnuje nařízení eIDAS, a tzv. adaptační zákony navazující na nařízení – z. č. 297/2016 Sb. a z. č. 298/2016 Sb.

3.1.1 Nařízení eIDAS

Tato část se týká samotného nařízení eIDAS. Je rozdělená na úvod a působnosti Nařízení, jeho cíle a definice pojmů dle tohoto Nařízení.

3.1.1.1 Úvod a oblast působnosti Nařízení

Právní úprava týkající se elektronického podpisu v České republice pochází již z roku 2000. Byla vytvořena zákonem č. 227/2000 Sb., o elektronickém podpisu, který vycházel ze směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy a bez problémů byla mj. začleněna do nového občanského zákoníku z. č. 89/2012 Sb. (dále jen NOZ). [3, s. 189]

Ke změnám v legislativě dochází v roce **2016**, kdy **1. července** roku 2016 nabývá účinnosti Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu a o zrušení směrnice 1999/93/ES, známé pod názvem eIDAS, neboli Regulation on **elektronic identification and trust services for electronic transactions** in the internal market. Nařízení eIDAS upravuje vícero oblastí, jako je elektronická identifikace, elektronické podpisy a pečetě, služby vytvářející důvěru či autentizaci internetových stránek. S ohledem na Nařízení bylo přijato prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rad (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. [6, s. 8]

Článek 1 Nařízení eIDAS říká, že cílem je *zajistit řádné fungování vnitřního trhu a současně usilovat o odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru.* [5]

Nařízení stanoví:

a) *„Podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu;*
b) *Pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí; a*
c) *Stanoví právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.“*[2]

Článek 2 Nařízení eIDAS vymezuje oblast působnosti, podle kterého se Nařízení vztahuje na systémy elektronické identifikace oznámené členskými státy, taktéž na poskytovatele služeb vytvářejících důvěru usazené v EU. Nevztahuje se na poskytování služeb vytvářejících důvěru, které jsou používány výhradně v uzavřených systémech vyplývajících z vnitrostátního práva nebo z dohod mezi stanoveným okruhem účastníků. Nařízením není dotčeno vnitrostátní právo ani právo EU týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy. [5]

Nařízení by mělo být **z hlediska technologického neutrální** a **otevřené inovacím** vzhledem k tempu technologických změn. Nařízení je skutečně nařízením, ne směrnicí, proto **je bezprostředně závazné pro všechny členské státy EU** a nevyžaduje žádné implementace v národní legislativě, takže se neprovádí jeho transpozice do národního práva. Jestliže Nařízení stanovuje něco jiného než národní právní předpis členského státu, musí být postupováno dle Nařízení. [5]

[2] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES čl. 1. písm. a) až c).

Místo transpozičního zákona byly proto vytvořeny tzv. **adaptační zákony**, a to č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, a č. 298/2016 Sb., zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, které mají adaptovat již existující právní úpravu České republiky na dopady přímo účinného Nařízení. Taktéž mají dořešit otázky, které nařízení ponechává na národní úrovni. Změnový zákon novelizuje 65 zákonů a navrhuje podstatné změny v zákoně č. 328/1999 Sb., o občanských průkazech, a v z. č. 111/2009 Sb., o základních registrech. Díky těmto změnám bude vytvořen prostor pro zavedení a využívání tzv. elektronických občanských průkazů (dále eOP). Na kontaktní elektronický čip těchto eOP lze zapsat data pro vytváření elektronických podpisů spolu s kvalifikovaným certifikátem pro elektronický podpis, ale také identifikační certifikát, který umožní využívat rozličné typy služeb. [6, s. 8–10]

Zákon č. 297/2016 ruší:

- Z. č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- Vyhlášku č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek
- Vyhlášku č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného certifikátu a kvalifikovaného časového razítka

Uvedené zákony upravují:

- Některé postupy poskytovatele služeb vytvářejících důvěru
- Některé požadavky na službu vytvářející důvěru
- Působnost Ministerstva vnitra v oblasti služeb vytvářejících důvěru
- Sankce za porušení povinností v oblasti služeb vytvářejících důvěru

- Obsahují změny v zákonech, kterých se eIDAS dotýká, například změny v trestním řádu, občanském soudním řádu, změny v zákoně o občanských průkazech, o cestovních dokladech, autorského zákona, soudního řádu správního, v zákoně o archivnictví a spisové službě ale i změny v zákoně o zeměměřictví, státní sociální podpoře a mnoho dalších. [7]

3.1.1.2 Cíle Nařízení eIDAS

Hlavní cíle Nařízení jsou shrnuty v preambuli. Podle ní má **budování důvěryhodnosti** on-line prostředí klíčový význam pro hospodářský a sociální rozvoj. Dle bodu 2 poskytne Nařízení **společný základ pro bezpečnou elektronickou komunikaci** mezi občany, podniky, orgány veřejné moci, tím posílí efektivnost veřejných a soukromých online služeb, elektronického podnikání a elektronického obchodu v EU. Očekávaným výsledkem je **zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu**. [5]

Dalším z cílů je odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, z toho vyplývá **sjednotit elektronickou identifikaci** a **autentizaci a její vzájemné uznávání** ve členských státech EU. Členské státy mají možnost zavést a používat prostředky pro účely elektronické identifikace pro přístup k on-line službám a včetně povinnosti je uznávat. Zásada vzájemného uznávání by se měla použít, pokud systém elektronické identifikace oznamujícího členského státu splňuje podmínky pro oznámení a toto oznámení bylo zveřejněné v Úředním věstníku EU. Při určování totožnosti osob, by měly úrovně záruky vyjadřovat míru spolehlivosti prostředků pro elektronickou identifikaci a taktéž to, že osoba deklarující konkrétní totožnost je skutečně osobou, s níž je tato totožnost spojena. [5]

Cílem v oblasti služeb vytvářejících důvěru je **harmonizace**, v oblasti elektronické identifikace tzv. **interoperabilita**. Rovněž stanovení obecného právního rámce pro využívání služeb vytvářejících důvěru a zároveň umožnit, aby mohly být využívány jako důkaz v soudním či správním řízení ve všech členských státech. Rámec interoperability musí být z hlediska technologického neutrální, řídí se evropskými a mezinárodními normami, usnadňuje aplikaci zásady ochrany osobních údajů a zajišťuje, aby byly tyto

údaje zpracovány v souladu se směrnici 95/46/ES[3]. Co se týče poskytovatelů služeb vytvářejících důvěru, je stanoven cíl zavedení režimu dohledu pro všechny poskytovatele (za různých podmínek jak pro nekvalifikované, tak pro kvalifikované poskytovatele), včetně stanovení odpovědnosti pro všechny poskytovatele služeb vytvářejících důvěru. [5]

Další cíl je zajištění soudržného rámce, který by zabezpečil vysokou úroveň bezpečnosti a právní jistotu, vedení důvěryhodných seznamů, které budou udávat stav kvalifikace poskytovatele služeb, či udělování značky důvěry EU, která bude označovat kvalifikované služby vytvářející důvěru poskytované kvalifikovanými poskytovateli služeb. [5]

Elektronickému podpisu nesmí být upírány právní účinky na základě skutečnosti, že je v elektronické podobě. Kvalifikovaný elektronický podpis má stejný právní účinek jako podpis vlastnoruční. Nařízení by mělo stanovit požadavky na kvalifikované prostředky pro vytváření elektronických podpisů, které mají zajistit jejich funkčnost. Nově zavedené elektronické pečetě by měly sloužit jako důkaz toho, že byl elektronický dokument vydaný určitou právnickou osobou a poskytovat integritu a jistotu o původu dokumentu. Nechybí zajištění dlouhodobého uchovávání informací, aby byla zajištěna dlouhodobá platnost elektronických pečetí a podpisů, a možnost jejich ověření bez ohledu na budoucí technologické pokroky. [5]

Nezbytně nutné je stanovit právní rámec pro usnadnění uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy. To s sebou přináší možnost nové tržní příležitosti nabízení nové panevropské služby elektronického doporučeného doručování pro poskytovatele služeb vytvářejících důvěru z EU. [5]

V oblasti internetových stránek se jedná o stanovení minimální povinnosti v oblasti bezpečnosti a odpovědnosti pro služby autentizace. Díky službám autentizace internetových stránek se může návštěvník určitých internetových stránek ujistit, že tyto

[3] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

stránky reprezentují legitimní subjekt. To povede ke zvýšení důvěryhodnosti a důvěry v on-line obchodování. [5]

A jak vyplývá z názvu Nařízení, **ruší směrnici 1999/93/ES.** [5]

3.1.1.3 Definice pojmů dle Nařízení eIDAS

V Nařízení dochází ke změně některých pojmů, některé změny jsou zásadní, jiné mají upřesňující charakter. Pokud je změna významná oproti původní legislativě (dosavadní právní úpravě), bude uvedena pro porovnání i legislativa v ČR před eIDAS. Uvedeny jsou pouze pojmy vztahující se k problematice elektronického podepisování. Diplomová práce cituje nikoliv doslovně, ale v odpovídajícím kontextu.

Podepisující osoba je podle Nařízení fyzická osoba (FO), která elektronický podpis vytváří. [5]

Elektronický podpis jsou data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a **která používá podepisující se osoba k podepsání.** V původním právním předpise[4] se definice elektronického podpisu lišila v poslední části věty, byla definována takto: *„a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*“. [5] Díky této definici dochází k chápání podpisu dle jeho primární funkce, a to jak k doložení skutečnosti, že jeho použitím určitá osoba projevila svoji vůli, či že se v určitý čas nacházela na určitém místě, případně, že ním stvrzuje platnost určitého dokumentu. Dochází tedy k položení rovnítka mezi elektronický podpis a data, která jsou použita k podepsání. [3, s. 217]

Zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje požadavky ve článku 26 Nařízení, a to:

a) je jednoznačně spojen s podepisující se osobou
b) umožňuje její identifikaci

[4] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

c) je vytvořen pomocí dat pro vytváření elektronických podpisů, jež může podepisující se osoba **s vysokou úrovní důvěry** použít pod svojí kontrolou
d) je k datům, která jsou jím podepsána, připojen tak, že je možné zjistit jejich jakoukoliv následnou změnu [5]

Kvalifikovaný elektronický podpis je zaručený elektronický podpis, který byl vytvořen kvalifikovaných prostředkem pro vytváření elektronických podpisů a je založen na kvalifikovaném certifikátu pro elektronické podpisy. V původním zákoně[5] není výslovně definován. [5]

Data pro vytváření elektronických podpisů jsou jedinečná data, která používá podepisující se osoba k vytváření elektronických podpisů. [5]

Certifikát pro elektronický podpis je elektronické potvrzení, jež spojuje data pro ověřování platnosti elektronických podpisů s určitou FO a **potvrzuje** u této osoby alespoň její **jméno nebo pseudonym.** [5] V původním změní, dle zákona o elektronickém podpisu, spojuje data pro ověření elektronických podpisů s podepisující osobou a umožňuje tak, ověřit její identitu. [8]

Kvalifikovaný certifikát pro elektronický podpis je certifikát pro elektronický podpis, který je vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky uvedené v příloze I Nařízení, tedy:

a) označení, že byl certifikát vydaný jako kvalifikovaný certifikát pro elektronický podpis, alespoň ve formě vhodné pro automatické zpracování
b) soubor dat, který umožní jednoznačně identifikovat kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně uvedení členského státu, v němž je poskytoval služeb usazen, a
- v případě právnické osoby (PO) – název a případné registrační číslo, jež je uvedené v úředních záznamech
- v případě FO – její jméno

[5] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

c) alespoň jméno či pseudonym podepisující se osoby; pokud se uvádí pseudonym, musí být jasně vyznačeno, že se jedná o pseudonym
d) data pro ověřování platnosti elektronických podpisů odpovídající datům pro vytváření elektronických podpisů
e) označení jak začátku, tak konce doby platnosti certifikátu
f) identifikační číslo certifikátu, které musí být jedinečné pro určitého kvalifikovaného poskytovatele služeb vytvářejících důvěru
g) zaručenou elektronickou pečeť nebo zaručený elektronický podpis poskytovatele služeb vytvářejících důvěru, jež certifikát vydal
h) údaj o místu, kde je bezpečně k dispozici certifikát, na němž je založena zaručená elektronická pečeť či zaručený elektronický podpis podle písmene g)
i) údaj o umístění služeb, které lze využít pro ověření platnosti kvalifikovaného certifikátu
j) příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování, pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů

Přičemž body h) a j) jsou nové a zásadní. [3, s. 200–202]

Služba vytvářející důvěru přestavuje nový pojem, jedná se o elektronickou službu, která je poskytována zpravidla za úplatu a spočívá:

a) ve vytváření, ověřování shody a platnosti elektronických podpisů, elektronických pečetí či elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů, jež souvisejí s těmito službami nebo
b) ve vytváření, ověřování schody a platnosti certifikátů pro autentizaci internetových webových stránek nebo
c) v uchovávání elektronických podpisů, pečetí nebo certifikátů, jež souvisejí s těmito službami [5]

Kvalifikovaná služba vytvářející důvěru je služba, která vytváří důvěru a splňuje použitelné požadavky stanovené v Nařízení. [5]

Poskytovatel služeb vytvářejících důvěru je FO či PO, která poskytuje jednu či několik služeb vytvářejících důvěru jako kvalifikovaný nebo nekvalifikovaný poskytovatel služeb vytvářejících důvěru. [5]

Kvalifikovaný poskytovatel služeb vytvářejících důvěru je poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či několik služeb vytvářejících důvěru a kterému byl orgánem dohledu **udělen status kvalifikovaný poskytovatel**. [5] V původní legislativě [6] pojem označoval kvalifikovaného poskytovatele certifikačních služeb, který poskytuje certifikační služby, vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů a splnil ohlašovací povinnost dle §6. [3, s. 203]

Produktem se rozumí programové vybavení nebo technické zařízení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru. [5] V zákoně o elektronickém podpisu se taková obecná definice nenachází, což je v souladu s širším zaměřením Nařízení eIDAS oproti původní Směrnici 1999/93/ES, z níž zákon vycházel. [8]

Prostředkem pro vytváření elektronických podpisů se rozumí konfigurované programové vybavení nebo technické zařízení pomocí, které se využívá k vytváření elektronických podpisů. [5]

Kvalifikovaný prostředek pro vytváření elektronických podpisů je prostředek pro vytváření elektronických podpisů, který splňuje požadavky z přílohy II, a to:

1. kvalifikované prostředky pro vytváření elektronických podpisů vhodnými postupy a technickými prostředky zajistí přinejmenším, aby:
   a) byla přiměřeně zajištěna důvěrnost dat, která byla použita pro vytvoření elektronického podpisu,
   b) data, která byla použitá pro vytváření elektronického podpisu, se mohla prakticky vyskytnout pouze jednou,

[6]., o elektronickém podpisu.

c) bylo přiměřeně zajištěno, že data, která byla použitá při vytváření elektronického podpisu nelze odvodit, a že je elektronický podpis spolehlivě chráněn proti padělání v současnosti dostupnými technickými prostředky,
d) oprávněná podepisující osoba měla možnost data, která jsou použitá pro vytváření elektronických podpisů, spolehlivě chránit před jejich zneužití třetí osobou,

2. kvalifikované prostředky pro vytváření elektronických podpisů nesmějí bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsání a ani nesmějí měnit podepisovaná data,
3. data pro vytváření elektronických podpisů může jménem podepisující osoby spravovat nebo vytvářet pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru,
4. aniž by byl dotčen bod 1 písmeno d), kvalifikovaní poskytovatelé služeb vytvářejících důvěru, jež spravují data pro vytváření el podpisů jménem podepisující osoby, mohou kopírovat data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky:
   a) bezpečnost zkopírovaných dat je na stejné úrovni jako bezpečnost u původních dat,
   b) počet zkopírovaných dat nepřesáhne minimum potřebné pro zajištění kontinuity služby. [5]

Výše uvedené požadavky jsou obecné, resp. nezávislé na použité technologii pro elektronický podpis. Lze jim tedy při vhodné implementaci vyhovět jak v případě kryptografického, tak dynamického biometrického podpisu.

Elektronické časové razítko jsou data v elektronické podobě, jež spojují jiná data v elektronické podobě s určitým okamžikem a tím **prokazují, že tato jiná data existovala v daném okamžiku.** [5]

Kvalifikované elektronické časové razítko, elektronické časové razítko, které splňuje požadavky ze článku 42, tedy:

1. kvalifikované elektronické razítko musí splňovat tyto uvedené požadavky:

a) spojuje čas a datum s daty takovým způsobem, aby byla možnost nezjistitelné změny dat přiměřeně zamezena
b) je založeno na přesném zdroji času spojeným s koordinovaným světovým časem
c) je podepsáno pomocí zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovala služeb vytvářejících důvěru či označeno jinou rovnocennou metodou [5]

V původní legislativě ČR bylo kvalifikované časové razítko definované jako datová zpráva vydaná kvalifikovaným poskytovatelem certifikačních služeb, a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a tak zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem. [8] Nařízení odstraňuje ne příliš vhodnou část původní definice, kdy se dalo diskutovat o tom, jak dlouho daná data existovala před časovým okamžikem. Nová definice dle eIDAS tento problém odstraňuje. [3, s. 213–214]

Elektronický dokument je jakýkoli obsah, jenž je uchovávaný v elektronické podobě, jako text či zvuková, vizuální či audiovizuální nahrávka. [5]

V tomto případě by se dalo diskutovat o vhodném překladu z anglického jazyka slova „recording“ jako nahrávka. Přičemž v německém verzi se hovoří o „Aufzeichnung“, čili záznam. Roli audiovizuálního záznamu může plnit i pouhý vizuální záznam bez přítomnosti zvuku, na rozdíl od audiovizuální nahrávky, která musí zvukovou složku obsahovat. V zákoně č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů je dle §2 písm. e) dokumentem každá zvuková, obrazová, písemná či jiná zaznamenaná informace, ve formě analogové či digitální. Což odpovídá spíše pojmu záznam než nahrávka. [16]

Daty pro ověřování platnosti se rozumí data, jež se používají k ověření platnosti elektronické pečeti či elektronického podpisu. [5]

Ověřování platnosti představuje postup ověřující shodu a potvrzení platnosti elektronické pečeti či elektronického podpisu. [5]

3.1.2 Rozbor vybraných pojmů

V této části budou podrobněji rozebrané kvalifikované služby vytvářející důvěru, elektronický podpis, ověřování platnosti kvalifikovaných elektronických podpisů, elektronické pečeti, elektronická časová razítka.

3.1.2.1 Kvalifikované služby vytvářející důvěru

Dle eIDAS čl. 20 odst. 1 se kvalifikovaní poskytovatelé služeb vytvářejících důvěru musí alespoň jednou za 24 měsíců na vlastní náklady podrobit auditu ze strany subjektu posuzování shody. Tento audit potvrzuje, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru včetně jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky dle Nařízení. Dle odst. 2, aniž by byl dotčen odst. 1, může orgán dohledu u kvalifikovaných poskytovatelů služeb vytvářejících důvěru na jejich náklady kdykoli provést audit, či požádat subjekt posuzování shody o provedení posouzení shody.

Odst. 3 se věnuje **odejmutí statusu kvalifikovaného poskytovatele,** resp. **služby** poskytovatelům a jimi poskytovaným službám. Jestliže orgán dohledu požaduje, aby kvalifikovaný poskytovatel služeb vytvářejících důvěru napravil neplnění požadavků dle eIDAS, a daný poskytovatel tak ve lhůtě stanové orgánem dohledu neučiní, může mu orgán dohledu odebrat s přihlédnutím k rozsahu, délce trvání a důsledkům neplnění status kvalifikovaného poskytovatele či kvalifikované služby. Tuto informaci je nutné sdělit subjektu, který aktualizuje důvěryhodné seznamy podle čl. 22 odst. 1 (viz. níže). [5, čl. 20 odst. 1 až 3] V České republice je tímto subjektem Ministerstvo vnitra České republiky, které provozuje a spravuje aplikaci **CertIQ**[7] pro ověřování certifikátů vůči důvěryhodným seznamům podle eIDAS. [9]

Článek 21 se zabývá zahájením poskytování kvalifikované služby vytvářející důvěru. Pokud chtějí poskytovatelé služeb vytvářejících důvěru bez statusu kvalifikovaného poskytovatele poskytovat kvalifikované služby, předloží orgánu dohledu oznámení o tomto úmyslu společně s posouzením shody vydaným subjektem posuzování shody. Orgán dohledu ověří, že žadatel o status kvalifikovaného poskytovatele či služeb splňuje požadavky dle eIDAS. Pokud dojde k závěru, že jsou požadavky splněny, **udělí orgán**

[7] Dostupná z: https://tsl.gov.cz/tsl_cr.html.

dohledu tomuto žadateli status kvalifikovaného poskytovatele či **kvalifikované služby** a vyrozumí o tom subjekt, který aktualizuje důvěryhodné seznamy. Naopak pokud dojde orgán dohledu k závěru, že nejsou požadavky splněny, či není ověření dokončeno do tří měsíců od oznámení, vyrozumí o tom žadatele a uvede důvody prodlení a dobu, během níž bude ověření dokončeno. Poskytovatelé, jimž byl přidělen status kvalifikovaného poskytovatele služeb, mohou danou kvalifikovanou službu vytvářející důvěru poskytovat poté, co byl tento status vyznačen v důvěryhodných seznamech. Samotné požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru jsou obsahem článku 24 Nařízení eIDAS. [5, čl. 21 odst. 1 až 3]

Důvěryhodné seznamy jsou upraveny ve čl. 22, podle kterého každý členský stát zřizuje, udržuje a zveřejňuje důvěryhodné seznamy, jež obsahují informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru spolu s informacemi o jimi poskytovaných kvalifikovaných službách vytvářejících důvěru. Tyto seznamy se zřizují ve formě vhodné pro automatické zpracování a jsou opatřeny elektronickým podpisem či elektronickou pečetí. Členské státy jsou povinny bez zbytečného odkladu sdělit Komisi informaci o subjektu, který bude odpovědný za zřízení, udržování a zveřejnění vnitrostátních důvěryhodných seznamů včetně informací o místě zveřejnění těchto seznamů, o certifikátech, jež budou použity k opatření důvěryhodných seznamů elektronickým podpisem či pečetí a či o jejich případných změnách. Tyto získané informace Komise bezpečnou cestou zpřístupní veřejnosti taktéž ve formě vhodné pro automatické zpracování a opatřené elektronických podpisem či pečetí. [5, čl. 22 odst. 1 až 4]

Dle čl. 23 mohou kvalifikovaní poskytovatelé služeb vytvářejících důvěru jednoduchým, rozpoznatelným a jasným způsobem označovat jimi poskytované kvalifikované služby vytvářející důvěru pomocí **značky důvěry EU**. [5, čl. 23]

Obr. č. 1: Značka důvěry EU pro kvalifikované služby vytvářející důvěru v barevném a černobílém provedení (Převzato z: [10, příloha I a příloha II])

3.1.2.2 Elektronický podpis dle eIDAS

Elektronickému podpisu je věnován oddíl 4 Nařízení. Článek 25 upravuje právní účinky elektronických podpisů, kdy odst. 1 říká, že **elektronickému podpisu nesmí být upírány právní účinky a nesmí být odmítán jako důkaz** v řízení jen proto, že má elektronickou podobu nebo proto, že nesplňuje požadavky na kvalifikovaný elektronický podpis. Dle odst. 2 má **kvalifikovaný elektronický podpis stejné právní účinek jako vlastnoruční podpis**. Odst. 3 upravuje uznávání ve členských státech, kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě je uznávaný jako podpis se stejnou výši důvěry (tedy jako kvalifikovaný elektronický podpis) ve všech členských státech. K podepisování lze využít elektronický podpis od libovolné certifikační autority v rámci EU, nelze vyžadovat pouze národní podpisy. [5, čl. 22 odst. 1 až 4]

Jak již bylo uvedeno výše, je elektronický podpis dle eIDAS definován jako „*data v elektronické podobě, který jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání*“ [5, čl. 3 bod 10]. Díky této definici dochází k chápání podpisu dle jeho primární funkce, a to jak k doložení skutečnosti, že jeho použitím určitá osoba projevila svoji vůli, či že se v určitý čas nacházela na určitém místě, případně, že ním stvrzuje platnost určitého dokumentu. Dochází tedy k položení rovnítka mezi elektronický podpis a data, která jsou použita k podepsání. [3, s. 217]

Díky současným technologickým možnostem a pokrokům přichází v úvahu řada různých variant provedení elektronického podpisu. Dle článku 3 bod 13 Nařízení eIDAS se daty pro vytváření elektronických podpisů rozumí jedinečná data, která používá podepisující se osoba k vytváření elektronických podpisů. Pokud využijeme metodu asymetrické kryptografie, bude tato jedinečná data představovat soukromý klíč. Pokud se znovu vrátíme k definici elektronického podpisu dle eIDAS, která říká, že elektronický podpis jsou jakákoliv data v elektronické podobě, která mohou být připojena k jiným datům v elektronické podobě, pak těmito daty může být v podstatě cokoliv, co dokážeme zdigitalizovat. Tedy jakýkoliv digitální záznam v podobě jedniček a nul, ať nejrůznější

obrázky, heslo, PIN či hlas apod., který bude připojen k podepisovaném dokumentu. [3, s. 218]

Nová definice elektronického podpisu dle autorů článku „Elektronický podpis podle Nařízení eIDAS“ posiluje postavení dynamického biometrického podpisu v legislativě EU a ČR a taktéž vytváří možnost přijetí dalších metod pro elektronické podepisování v budoucnosti. [3, s. 220]

Nařízení nepřináší žádnou změnu v tom, že jak kryptografický elektronický podpis, tak dynamický biometrický podpis jsou vlastnoručním podpisem, vyhovují požadavkům na písemnost ve smyslu ust. §562 ost. 1 NOZ. Toto bylo v legislativě ČR uvedeno obdobně již v předchozím občanském zákoníku, z. č. 40/1964 Sb. Oba byly taktéž elektronickým podpisem dle z. č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů a rovněž jsou elektronickým podpisem dle Nařízení eIDAS. Vyplývá to nejen z výše uvedených definic dle eIDAS, ale i z principů, které se týkají přijímání elektronických podpisů s nižší zárukou bezpečnosti (těch, které nesplňují požadavky na kvalifikovaný elektronický podpis). [3, s. 222] V eIDAS je toto definované ve článku 25 odst. 1: *„Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“* [5, čl. 25 odst. 1]

Dle nařízení eIDAS se elektronickým podpisem rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která používá podepisující se osoba k podepsání. Zaručený elektronický podpis dle eIDAS je jednoznačně spojen s podepisující osobou, umožňuje její identifikaci, je vytvořen pomocí dat pro vytváření elektronických podpisů, která může podepisující se osoba s vysokou úrovní důvěry použít pod svojí kontrolou a je k podepsaným datům připojen tak, aby bylo možné zjistit jejich jakoukoliv následnou změnu. Dynamický biometrický podpis tyto dvě definice splňuje, řadí se tedy na úroveň elektronického podpisu i zaručeného elektronického podpisu dle eIDAS. [3, 199]

Článek 26 upravuje požadavky na zaručené elektronické podpisy, ty jsou již shrnuty v kapitole s pojmy výše. Dle čl. 27 odst. 3 mimo jiné nesmějí členské státy v případě přeshraničního využívání on-line služeb poskytovaných subjekty veřejného sektoru vyžadovat elektronický podpis s vyšší zárukou, než je kvalifikovaný elektronický podpis. Článek 28 pojednává o kvalifikovaných certifikátech pro elektronické podpisy – především musí splňovat požadavky z přílohy I, tyto požadavky byly stejně jako v předchozím případě již uvedeny v kapitole výše. Mimo jiné upravuje zneplatnění či dočasné pozastavení platnosti kvalifikovaných certifikátů pro elektronický podpis. Čl. 29 odkazuje na přílohu II s požadavky na kvalifikované prostředky pro vytváření elektronických podpisů. Následující dva články tohoto oddílu upravují certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů či zveřejňovací povinnost týkající se seznamu certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů. Certifikací se rozumí postup posouzení bezpečnosti, který byl proveden v souladu s některou z norem pro posuzování bezpečnosti produktů IT, či jiný postup za podmínky, že používá srovnatelné úrovně bezpečnosti. [5, čl. 26 až 31]

3.1.2.3 Ověřování platnosti kvalifikovaných elektronických podpisů

Dle článku 32 je potvrzena platnost kvalifikovaného elektronického podpisu, když:

a) certifikát, na kterém je založen podpis, jenž je v souladu s přílohou I, byl kvalifikovaným certifikátem pro elektronický podpis v okamžiku podpisu
b) kvalifikovaný certifikát byl vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru a současně byl platný v okamžiku podpisu
c) data pro ověřování podpisů odpovídají datům, která byla poskytnuta spoléhající straně
d) spoléhající se straně je řádné poskytnut jedinečný soubor dat, který identifikuje podepisující se osobu v certifikátu
e) byl-li v okamžiku podpisu použit pseudonym, je toto jeho použití jednoznačně sděleno spoléhající se straně
f) elektronický podpis byl vytvořený pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů
g) integrita podepsaných dat nebyla omezena

h) v okamžiku podpisu byly splněny požadavky, které jsou stanoveny ve článku 26 (požadavky na zaručené elektronické podpisy) [5, čl. 32]

Dle dikce písmena b) je podstatné, že certifikát byl platný v okamžiku podpisu, je tedy možné ověřovat kvalifikovaný elektronický podpis i po vypršení platnosti certifikátu. Nabízí se otázky, jak bude možné určit bez časového razítka, kdy byl podpis vytvořen. V některých případech lze časový okamžik odvodit z kontextu obsahu dokumentu, nicméně protože tento okamžik může být např. antedatován, jedinou objektivní informací je časový údaj, který je získán z měřidla důvěryhodného času a je kryptograficky zabezpečen ve formě tzv. časového razítka. Toto měřidlo času je synchronizováno s důvěryhodným zdrojem koordinovaného světového času (Coordinated Universal Time, dále jen UTC). UTC je celosvětový časový standard, který je založen na tzv. atomových hodinách, jednotlivá časová pásma jsou definována svými odchylkami od UTC. Získaný časový údaj je vkládán do časových razítek a poskytuje platné a kontrolované informace pro případ sporů mezi poskytovatelem časových razítek a klienty. [3, s. 214]

Článek 33 a 34 Nařízení zavádí pojmy jako kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů, či kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů, přičemž obě služby může poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru. První pojem, **kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů**, zajišťuje ověřování platnosti v souladu se článkem 32 a umožňuje, aby spoléhající se strany získaly výsledek postupu ověřování platnosti způsobem automatizovaným, spolehlivým, účinným a který je opatřený zaručeným elektronickým podpisem, resp. pečetí poskytovatele kvalifikované služby ověřování platnosti. Druhý pojem, **kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů**, vysvětluje jako službu, kterou taktéž poskytuje pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, a který využívá technologie a postupy, jež jsou schopny zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí jeho technické doby planosti. V obou případech může Komise prostřednictvím prováděcích aktů určit referenční čísla norem pro tyto služby. [5, čl. 33 a 34]

3.1.2.4 Elektronická časová razítka

Od roku 2004, kdy nabyla účinnosti novela zákona o elektronickém podpisu, byl v české legislativě zaveden pojem časové razítko ale pouze s přívlastkem kvalifikované. Základní stupeň časového razítka nebyl definován. [8] Nařízení eIDAS obsahuje jak úroveň základní časového razítka, tak kvalifikovanou, podrobněji výše v kapitole Definice pojmů dle Nařízení. Ve článku 41 Nařízení je zdůrazněno podobně jako u podpisu, že *„Elektronickému časovému razítku nesmějí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko.“* [5, čl. 41 odst. 1]

Dle odst. 2 platí u **kvalifikovaného elektronického časového razítka domněnka správnosti času a data**, které udává, a **integrity dat**, s nimiž jsou tento čas a datum spojeny. Výslovněji je toto uvedené v definici pojmů, kdy se elektronické časové razítko považuje za data v elektronické podobě, jež spojují jiná data v elektronické podobě s určitým okamžikem a tím prokazují, že tato jiná data existovala v daném časovém okamžiku. Třetí odstavec, se týká uznávání kvalifikovaných elektronických časových razítek ve členských státech a říká, že toto kvalifikované elektronické časové razítko vydané v jednom členském státě je uznáváno stejnou právní silou (tedy jako kvalifikované elektronické časové razítko) ve všech členských státech. [5, čl. 41 dost. 2 a 3]

3.1.3 Zákon č. 297/2016 Sb.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce upravuje některé postupy poskytovatelů služeb vytvářejících důvěru, požadavky na službu vytvářející důvěru, působnost Ministerstva vnitra v této oblasti a sankce za porušení povinností. [11]

Podepisování a pečetění dokumentu

Dle § 5 lze k podepisování použít pouze **kvalifikovaný elektronický podpis**, podepisuje-li se jím elektronický dokument, kterým právně jedná:

a) stát, územní samosprávný celek, PO zřízená zákonem, státem či založená státem, územním samosprávným celkem nebo PO zřízenou zákonem, nebo
b) při výkonu své působnosti osoba neuvedená v písmenu a) [11, §5]

Dle § 6 tohoto zákona lze v případě podepisování elektronického dokumentu, kterým se právně jedná vůči veřejnoprávní osobě či podepisujícímu v souvislosti s výkonem jejich působnosti, využít pouze **uznávaný elektronický podpis**. Tento uznávaný elektronický podpis reprezentuje zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis. Dle §7 lze k podepisování použít zaručený elektronický podpis, uznávaný elektronický podpis, či jiný typ elektronického podpisu, v případě, že se právně jedná jiným způsobem než uvedeným v §5, resp. 6. [11, §6 a 7]

Z výše uvedeného vyplývá, že pro právní jednání státních orgánů a samospráv nebo právnických osob zřízených zákonem či vykonávající veřejnou správu, jakož i pro právní jednání vůči nim má být používán pouze uznávaný elektronický podpis, který má účinky vlastnoručního podpisu. V obou možných variantách se jedná o podpis využívající kvalifikovaný certifikát; v tomto případě je použití DBP tedy zatím vyloučeno. (Nelze ovšem vyloučit, že bude implementována taková verze DBP, který bude pracovat i s biometrikou i s kvalifikovaným certifikátem; pak ovšem výhody snadného používání DBP budou značně potlačeny.)

Naproti tomu pro použití mimo oblast veřejné správy se toto omezení neuplatní (viz dikce §7). *Jde tedy o dokumenty, respektive právní jednání jiných subjektů, než jsou ty uvedené v § 5, adresované subjektům uvedeným v § 5 v jiném než vrchnostenském postavení nebo adresované jiným subjektům než uvedeným v § 5. V případě těchto právních jednání je možné použít všechny typy elektronických podpisů, které nařízení eIDAS zná, tj. elektronický podpis, zaručený elektronický podpis, zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis. Zákon tak rozšiřuje paritu s vlastnoručním podpisem i na tyto typy elektronických podpisů.* [20]

Podle §8 veřejnoprávní podepisující osoba či jiná PO využívá k zapečetění dokumentu v elektronické podobě při výkonu své působnosti **kvalifikovanou elektronickou pečeť**, nestanoví-li jiný právní předpis jinak či to nevyplývá z povahy právního jednání. Další použití elektronických pečetí obsažené § 9 resp. §10, je shodné s §6 resp. §7, pouze je zde pojem elektronický podpis nahrazen elektronickou pečetí. [11, §8 až 10]

Pro soukromoprávní jednání je tedy možné v souladu s ust. § 10 zákona použít zaručenou elektronickou pečeť, uznávanou elektronickou pečeť, případně jiný typ elektronické pečeti, pečetí-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 8 nebo § 9 odst. 1.

Použití kvalifikovaného elektronického časového razítka

Dle §11 veřejnoprávní podepisující, jež podepisují elektronický dokument, jímž právně jednají dle §5, opatří podepsaný elektronický dokument **kvalifikovaným elektronickým časovým razítkem.** To stejné platí pro osobu, která podepsala elektronický dokument, jímž právně jedná při výkonu své působnosti podle § 5. Veřejnoprávní podepisující, jež zapečetili elektronický dokument, jímž právně jednají dle §8, opatří zapečetěný elektronický dokument **kvalifikovaným elektronickým časovým razítkem**. To stejné platí pro osobu, která podepsala elektronický dokument, jímž právně jedná při výkonu své působnosti podle § 8. [11, §11]

Co se týká používání časového razítka pro soukromoprávní jednání, toto zákon neupravuje vůbec. Je tedy možné používat jak „obyčejné“ časové razítko (čl. 3 bod 33 Nařízení), tak kvalifikované časové razítko (bod 34).

Ověřování platnosti zaručené elektronické pečetě a zaručeného elektronického podpisu

Dle § 12 se pro ověřování platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis a na ověřování platnosti zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě obdobně použije čl. 32 odst. 1 písm. a) až e), g) a h) dle nařízení eIDAS. [11, §12]

Působnost ministerstva

Paragraf 13 pojednává o působnosti Ministerstva vnitra, jež plní úkoly dohledu podle Nařízení eIDAS a tohoto zákona. Přiděluje mu povinnost vést či zveřejňovat důvěryhodné seznamy, či právo udělit pokyn pro zneplatnění kvalifikovaných certifikátů v případě, stanovených podmínek apod. § 14 upravuje poskytování služeb vytvářejících důvěru Správou základních registrů, stanovuje nutné atributy při evidenci FO, PO, certifikátu a dalších údajů či to, že údaje o certifikátech jsou dálkovým přístupem veřejně dostupné. V případě neoprávněného použití značky důvěry EU hrozí FO sankce do výše 2 000 000 Kč (§16). Pro PO či podnikající FO jsou sankce rozděleny do tří pásem, podle toho, o jaký správní delikt se jedná. Maximální výše sankce je taktéž 2 000 000 Kč dle §17. Výše pokuty se odvíjí od závažnosti správního deliktu, způsobu jeho spáchání, následkům a k okolnostem, za kterých byl spáchán. Delikty dle tohoto zákona projednává v prvním stupni ministerstvo. Výnosy z pokut jsou příjmem do státního rozpočtu. [11, § 13 až 18]

Poslední dva paragrafy obsahují **přechodná** a **zrušovací ustanovení**. Definují používání podpisů a pečetí po dobu 2 let ode dne nabytí účinnosti zákona, tedy od 19. září 2016. Po dobu 2 let od nabytí účinnosti tohoto zákona lze k podepisování podle §5 použít taktéž zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis. Na místo zaručené elektronické pečetě založené na kvalifikovaném certifikátu použít pro elektronickou pečeť nebo místo kvalifikované elektronické pečeti použít elektronickou značku[8] založenou na systémovém certifikátu vydaném osobou, jež byla akreditovaným poskytovatelem certifikačních služeb (před nabytím účinnosti tohoto zákona) a jež je kvalifikovaným poskytovatelem služeb vytvářejících důvěru, či zaručenou elektronickou pečeť založenou na certifikátu pro elektronickou pečeť, který byl vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Namísto kvalifikovaného elektronického časového razítka dle §11, lze použít elektronické časové razítko vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Tento zákon ruší z. č. 227/2000 Sb., z. č. 440/2004 Sb., vyhlášku č. 378/2006 Sb., vyhlášku č. 212/2012 Sb. a ruší další části nejrůznějších zákonů, jako například zákonu o trestním řízení soudním, o správních poplatcích, o archivnictví a spisové službě atd. [11, §19 a 20]

[8] Podle z. č. 227/2000 Sb. ve změní účinném před nabytím účinnosti tohoto zákona 297/2016 Sb.

3.1.4 Zákon č. 298/2016 Sb.

Další úpravy či změny v české legislativě související s eIDAS jsou obsahem zákona č. 298/2000 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Tento zákon **obsahuje 67 částí**, z nichž každá specifikuje změny v dosavadní legislativě. **Změny** se týkají **širokého spektra zákonů**, a to nejen těch, co se týkají archivnictví a spisové služby, občanských průkazů, cestovních dokladů či trestního řádu, ale i daně z hazardních her, obchodu s reprodukčním materiálem lesních dřevin či ochrany veřejného zdraví. [7]

3.2 Porovnání elektronického podpisu a DBP z technologického hlediska

V této kapitole budou porovnány dva druhy podpisů, a to kryptografický elektronický podpis a dynamický biometrický podpis z hlediska technologického.

3.2.1 Elektronický podpis

Elektronický (digitální) podpis lze obecně chápat jako posloupnost jedniček a nul (bitů). Jinou otázkou však je, jak je vytvořen. Definice podle čl. 3 odst. 10 Nařízení říká pouze velice obecně, že „elektronickým podpisem rozumíme data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“. V zásadě dnes můžeme rozlišovat dva druhy elektronických podpisů: 1. kryptografické, 2. ostatní.

Jak již název napovídá, kryptografické elektronické podpisy určitým způsobem využívají šifrování. Obecně platí, že šifrovací algoritmus převádí data v otevřené podobě na data v podobě zašifrované a naopak. Pro zašifrování se použije klíč pro zašifrování, pro odšifrování klíč pro odšifrování. Pokud jsou klíče stejné, jde o kryptografii symetrickou. O asymetrické kryptografii hovoříme tehdy, jsou-li tyto klíče různé. Podpis na bázi kryptografických metod využívá tzv. **asymetrické kryptografie**, která používá soukromý a veřejný klíč. Při šifrování i při realizaci podpisu je nutné dávat pozor na

použití privátního a veřejného klíče. Při podepisování se data zašifrují privátním klíčem, následné ověření využívá klíč veřejný, zatímco v případě šifrování dat jsou klíče využívány naopak. Šifruje se veřejným klíčem příjemce a dešifruje jeho privátním klíčem. [2, s. 283–286]

Hash funkce neboli otisk

Významnou úlohu v procesu vytváření kryptografických elektronických podpisů hraje hash neboli, jak se také říká v češtině, otisk podepisovaného dokumentu. Hash reprezentuje obsah celého dokumentu, aniž by prozrazoval něco o jeho skutečném obsahu. Používá se matematicko-kryptografická metoda, kdy je pomocí jednosměrné funkce převeden obsah dokumentu na jednoznačné číslo o pevné délce. Hashovací funkce splňuje tyto podmínky:

a) pro daný hash H je obtížné vypočítat takové a, pro které by platilo
   h(a) = H (hashovací funkce je tedy jednosměrná)
b) pro daný vstup a je obtížné najít druhý vstup b, aby platilo H(a) = H(b)
c) je málo pravděpodobné najít rozdílné vstupy a, b, pro které by platilo H(a) = H(b)

Mezi nejznámější hashovací funkce patří SHA1, ripemd-160, SHA224, 256, 384, 512, whirlpool, SHA3. [2, s. 286-287]

Národní bezpečnostní úřad ve svém prohlášení doporučuje nadále nepoužívat hashovací funkce, které mají výstup menší než 160 bitů, například MD4, MD5,ripemd-160, haval-128 atd. Doporučuje zahájit přípravu na přechod od hashovací funkce SHA-1 na vyšší generaci, například SHA-2, SHA-224, SHA-256, SHA-384 a SHA 512, a to v horizontu 3-5 let. Zároveň doporučuje prozkoumat bezpečnostní aplikace a kryptografické prostředky využívající hashovací funkce a odborně posoudit jejich bezpečnost s ohledem na nejnovější kryptoanalytické útoky. [12]

Elektronické podepisování na bázi kryptografického elektronického podpisu

Při procesu podepisování digitálního dokumentu kryptografickým elektronickým podpisem budeme vycházet z existence asymetrického šifrovacího algoritmu, resp. možnosti využití veřejného a privátního klíče, který reprezentuje naši schopnost vytvořit elektronický podpis. Podepisovaný digitální dokument je reprezentován hashem.

Složitým matematickým spojením založeným na asymetrické kryptografii, které je schopen provést pouze počítač, vznikne z hashe digitálního dokumentu a privátního klíče nový řetězec bitů, který reprezentuje elektronický podpis. Vzniklý elektronický podpis má tyto vlastnosti:

- podepisovaný dokument se podpisem nijak nezměnil, resp. nebyl nijak změněn jeho obsah,
- podpis je možné elektronicky přenášet mimo dokument či jej uložit, nelze jej ale přenést na jiný dokument, je totiž funkcí obsahu samotného podepisovaného dokumentu (hashe) a soukromého podepisovacího klíče. Pokud bychom podepsali dva digitální dokumenty odlišné v jediném bitu, byly by výsledné podpisy těchto dokumentů odlišné. Tuto vlastnost zaručí právě matematické operace spojující hash digitálního dokumentu s privátním klíčem. [2, s. 289–290]

Následující text se zabývá používáním a ověřováním kryptografických elektronických podpisů, aby bylo zřejmé, jak odlišný je způsob nakládání s dynamickým biometrickým podpisem.

Ověření elektronického podpisu a certifikátu

Ověření pravosti elektronického podpisu probíhá pomocí veřejného klíče. Tento **veřejný klíč** je pevně **svázán se soukromým, „privátním“ klíčem**. Veřejný klíč neumožňuje možnost podepisovat, slouží pouze k ověření. Za samotným ověřování stojí opět matematická operace, která je prováděna počítačem a jejím výsledkem je informace o tom, zda byl dokument skutečně podepsán osobou, která se za podepisující osobu vydává a zda dokument nebyl změněn po jeho podepsání. Aby byla zajištěna vyšší jistota toho, že veřejný klíč patří té osobě, které to tvrdí, existují tzv. **certifikáty**. Jedná se o digitální dokument, který obsahuje informace týkající se certifikátu, identifikační údaje příslušné osoby a veřejný klíč. Tento digitální dokument je **podepsaný vydavatelskou certifikační autoritou**. A dle principu přenosu důvěry můžeme důvěřovat neznámému certifikátu, který je podepsaný důvěryhodnou certifikační autoritou. [2, s. 292–293]

Certifikát dle X.509

V rámci série doporučení ITU[9] X.500 je v rámci X.509 definovaný certifikát, který je používán pro digitální podpisy založené na bázi asymetrické kryptografie. Na bázi X.509 systém vytváří **hierarchickou strukturu důvěrnosti certifikátů**, kdy na vrcholu stojí tzv. kořenová certifikační autorita (lze říci nejdůvěryhodnější). Certifikát obsahuje informace, jako jsou verze, sériové číslo, identifikátor algoritmu, název vystavitele certifikátu, dobu platnosti, označení subjektu (držitele soukromého klíče), informace o veřejném klíči, volitelné položky a podpis certifikační autority (hash všech položek podepsaný soukromým klíčem certifikační autority). Poskytovatelé služeb vytvářejících důvěru vydávají tzv. **seznam revokovaných certifikátů** (CRL), který obsahuje datum vydání, seznam certifikátů, jež byly revokovány včetně důvodu a času. To vše je podepsáno podpisem poskytovatele. [17, 18, 2, s. 293–298]

Postup ověřování v případě komunikace mezi dvěma komunikujícími stranami:
Nejdříve si komunikující strany ověří podpis druhé komunikující strany pomocí jeho veřejného klíče. Následně ověří autentičnost tohoto veřejného klíče pomocí veřejného klíče certifikační autority. Požadavek na důvěryhodnost je k vztažen v certifikační autoritě. [2, s. 301]

V úvahu přichází dvojí postup a to: Ověřující strana obdrží podepsanou zprávu a současně s ní certifikát. Tento certifikát je chráněn podpisem poskytovatele služeb vytvářejících důvěru. V případě druhé varianty obdrží ověřující strana pouze adresu serveru poskytovatele certifikačních služeb, na kterém se nachází certifikát. Při validaci se jedna komunikující strana dotazuje poskytovatele certifikačních služeb (důvěryhodné třetí strany) na platnost certifikátu druhé komunikující strany. Systém ověřování může být řešen přímým online dotazem na aktuální stav certifikátu nebo je postaven na tzv. CRL(certificate revocation list) seznamech, kdy se porovnává, zda nebyl certifikát revokován. [2, s. 302]

[9] ITU, dříve CCITT je International Telecommunication Union, jejíž sekce ITU Telecommunication Standardization Sector (ITU-T) vydává standardy se vztahem k telekomunikacím. Viz www.itu.int/.

Obr. č. 2: Ověření pravosti podpisu a certifikátu (Zpracování vlastní dle: [2, s. 302])

3.2.2 Dynamický biometrický podpis

Dynamický biometrický podpis (DBP) představuje **nejpokročilejší variantu biometrického podpisu**, který využívá elektronických prostředků pro snímání dynamických charakteristik podpisu a je tedy použitelný jak pro podepisování, tak pro verifikaci (autentizaci) podepisující se osoby. V dnešní době jsou již známy i další pokusy používat k podpisu jiné dynamické projevy, například snímání krevního řečiště nebo gest prováděných například mobilním telefonem. [2, s. 315–316]

Při vzniku lidského podpisu vzniká primární impuls v centrálním nervovém systému, mozku. Nervový systém následně aktivuje příslušné svalstvo. Výsledkem uvolňování a stahování svalů je pohyb pera po papíře, které zanechává stopu hrotu psacího nástroje. Biomechanický proces vzniku podpisu tedy není jednoduchý. [2, s. 316]

Verifikaci podepisující se osoby rozlišujeme na dva typy, a to off-line a on-line systémy. V případě **off-line systémů** se verifikovaná osoba podepíše na papír klasickým způsobem. Tento podpis je poté prostřednictvím skeneru či kamery digitalizován. Následně se pomocí aplikace určuje shodnost podpisu osoby se vzorkem. Toto srovnání se provádí na základě srovnání celkového obrazu podpisu, jde tedy v podstatě o dosavadní ověřování pomocí podpisového vzoru bez přítomnosti údajů o dynamice podpisu. V případě **on-line** jsou srovnávací charakteristiky podpisu získávány v reálném čase, a to pomocí speciálního snímacího hardwaru, specializovaného tabletu či speciálně

upraveného pera. [1, s. 170–171] Tyto technologie zachycují jak statické, tak dynamické charakteristiky podpisu během vzniku samotného podpisu. Pouze tedy v případě on-line systému se tedy jedná o zachycování dynamického biometrického podpisu. [2, s. 317]

Podpis je tvořen dvěma částmi:

a) **Viditelné informace** – grafická podoba, která je znázorněna na dokumentu (viditelná na tabletu či pracovní stanici). Grafická forma podpisu je zobrazena především proto, aby podepisující se osoba viděla výsledek svého podepisování, má pouze informační hodnotu.
b) **Neviditelné informace** – informace, jež jsou výsledkem biometrického podpisu, jsou vloženy do elektronického dokumentu a k jejich zobrazení je třeba využít software (např. Acrobat Reader) či klienta pro speciální aplikace DBP. [4, s. 402]

Podpis je určen **charakteristickými vlastnostmi** (parametry). Mezi tyto vlastnosti patří čas trvání podpisu, křivky a body, tlak pera na podložku, velikost podpisu, jeho forma a tvar, úhel a délka čar, oblouků, počet smyček či rychlost, zrychlení, resp. zpomalení při jednotlivých tazích. [4, s. 402] Parametry bývají obvykle vyjádřeny jako vektor charakteristik, které jsou extrahovány během celého procesu podepisování. Tyto charakteristiky jsou například maximální a průměrná rychlost psaní, poměr krátkých a dlouhých tahů, jejich zakřivení atd. Charakteristiky dynamické jsou vyjádřeny **časovou funkcí**, ta charakterizuje podpis v každém okamžiku jeho vzniku. Tyto časové funkce popisují souřadnicové pozice hrotu psacího nástroje x(t) a y(t), tlak hrotu na podepisovací podložku p(t), rychlost v(t), zrychlení a(t), časové intervaly mezi jednotlivými částmi podpisu atd. Je možné využít i dalších charakteristik jako je například dynamický zdvih, tzn. celkový pohyb psacího nástroje (tedy i pohyb nad tabletem), kdy je tento pohyb zaznamenáván ve 3D prostoru. Tento dynamický zdvih je taktéž jedinečný pro podepisující se osobu, a proto napomáhá k vyšší přesnosti verifikace. [1, s. 171]

Vlastnoruční podpis je zaznamenáván pomocí speciálního pera a digitalizačního tabletu. Tyto tablety získají z podpisu data, která umožňují analyzovat jak statické, tak dynamické vlastnosti samotného podpisu, díky kterým jsou spojeny s podepisující se osobou. [2, s. 318] Parametry výše uvedené tvoří tzv. **biometrický vzorek**, který odráží znaky, návyky

a projev chování podepisující se osoby. [4, s. 402] Samotné vytvoření tohoto vzorku vychází z matematického aparátu neuronových sítí a jedná se o proprietární řešení tvůrce. Podepisující pera jednotlivých výrobců jsou odlišné velikostí vektoru biometrických informací. **Dynamický biometrický podpis není vytvářen ze samotného obsahu podepisovaného dokumentu, je do něj integrován**. [2, s. 330]

V případě, že je **dynamický biometrický podpis** využit **pro autentizaci podpisu, resp. osoby, která podpis učinila**, probíhá získávání podpisu dvoufázově a to:

a) Podepisující se několikrát (cca 3krát – 10krát) podepíše na podepisovací tablet. Z těchto podpisů je vytvořen základní biometrický vzorek.
b) Ověření podpisu spočívá v určení shody biometrického vzorku získaného z fáze a) a z porovnávaného podpisu.

Získaný biometrický vzorek je přenesen do databáze, kdy je při verifikaci vznesen dotaz do této databáze. Dotaz prohledává databázi na shodu s některým z uložených vzorků nebo dle ID, jež přísluší k porovnávanému podpisu, dojde k jeho srovnání s odpovídajícím vzorkem. Tato porovnání jsou řešena na bázi heuristických a statistických metod a představují proprietární řešení dodavatele systému. [2, s. 328]

Při autentizaci osoby se obecně pohybujeme v modelu 1:N, tj. porovnáváme sejmutý záznam se všemi záznamy o osobách v databázi. Nevýhodou je vyšší riziko chybného přijetí identifikace a vysoké nároky na výpočetní výkon systému. Tento problém odstraníme předchozím identifikačním krokem (zadáním identifikačního údaje typu jméno, číslo, ID apod.), což je možné uskutečnit jak v případě autentizace obecným záznamem, tak v případě ověřování podpisu. Tím se dostaneme do varianty 1:1 s vyšší přesností a nižší náročností na zpracování. Mezi důležité parametry tohoto podpisu patří **FRR**[10] neboli četnost nesprávného odmítnutí, známá jako chyba typu 1, a **FAR**[11] neboli četnost chybného přijetí, tzv. chyba typu 2, ale i vnitřní nastavení systému pro ověřování dynamického biometrického podpisu. [1, s. 174] Toto vnitřní nastavení stanovuje výrobce řešení, nastavuje tak požadovanou úroveň shody všech porovnávaných charakteristik

[10] False rejection rate
[11] False acceptance rate

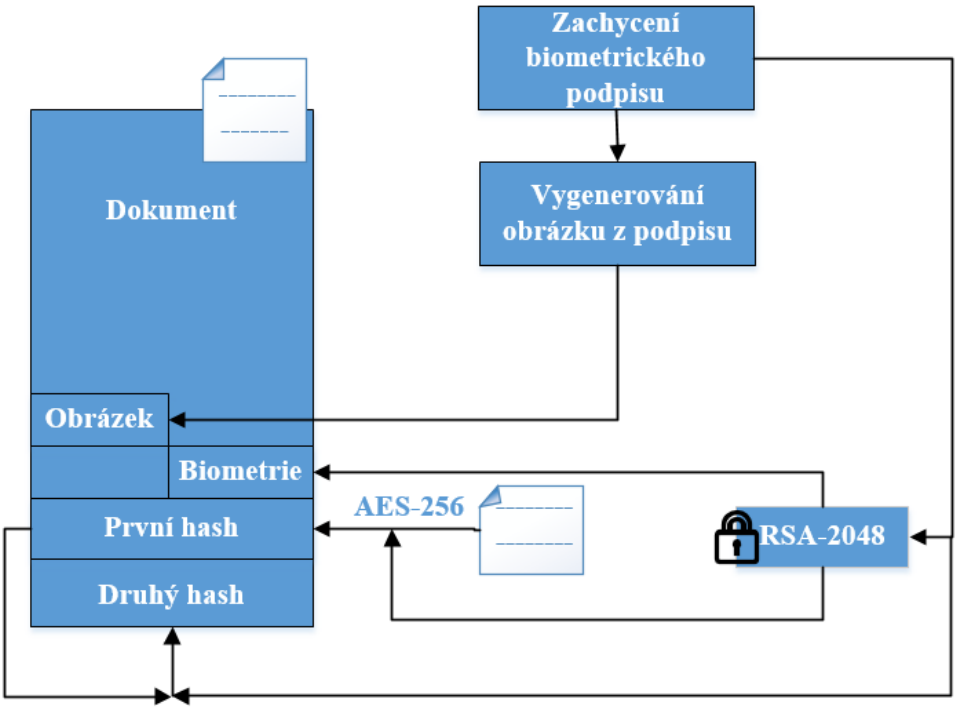
(např. 78%-ní úroveň shody všech charakteristik znamená kladné ověření osoby). [2, s. 327]

Základní postup podepsání elektronického podpisu ve formátu PDF

1. Vytvořen hash z podepisovaného PDF dokumentu.
2. Vytvořen hash z dat dynamického biometrického podpisu.
3. Vytvoření souboru tzv. servisních dat (výrobní číslo snímacího tabletu apod.).
4. Získané servisní data a hashe se zašifrují – lze využít symetrické šifry pro uzavřené systémy, či asymetrické šifry. V případě asymetrické šifry má certifikát provozovatel a dešifrování se provede soukromým klíčem, který spravuje.
5. Vzniká záznam, jež obsahuje jak podpis dokumentu, tak spojení dynamického biometrického podpisu s dokumentem. Dokument je chráněn proti porušení integrity jak obsahu, tak samotného dynamického biometrického podpisu. [2, s. 318–319]

K podepisování elektronických dokumentů ve formátu PDF lze využít například řešení společnosti SignoSoft a Adobe, SOFTPRO apod. Adobe Acrobat zpracovává podpisy pomocí tzv. podpisových modulů, které zajišťují integraci podpisu do elektronického dokumentu. Konkrétní řešení integrace podpisu do elektronického dokumentu ve formátu PDF je závislé na dodaném externím podpisovém modulu. [2, s. 320]

Při šifrování a zachovávání integrity dokumentu provádí níže popsané řešení SignoSoft kroky, které zachycuje následující obrázek.

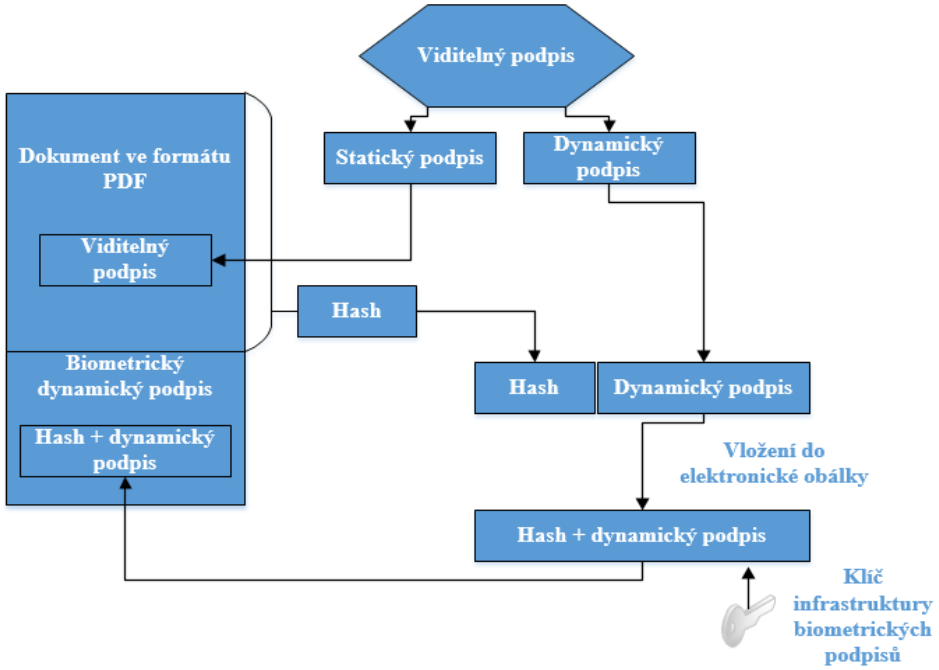


Obr. č. 3: Kroky při zpracování vloženého podpisu (Zpracování vlastní dle: [2, s. 321])

1. S využitím zařízení pro snímání podpisu je zachycen podpis (jak viditelná složka – obrázek, tak neviditelná – biometrická data), a ten je dále zpracován aplikací.
2. Ze získaného podpisu je vygenerován obrázek, který je vložen do podepisovaného dokumentu.
3. Biometrická data podpisu jsou zašifrována pomocí asymetrického algoritmu RSA-2048 (lze až 4096) a jsou taktéž uložena do podepisovaného dokumentu.
4. Obsah podepisovaného dokumentu je zašifrován pomocí symetrického algoritmu AES 256 a následně použit v dalším kroku pro výpočet hashe SHA-256.
5. První otisk (hash) SHA-256, lze i RIPEMD-160/320, se získá ze šifrovaných biometrických dat a šifrovaného obsahu dokumentu a je uložen do podepisovaného dokumentu. Slouží k zajištění integrity dokumentu a zašifrovaných biometrických dat. Je podepsán veřejným klíčem.
6. Druhý otisk (hash) se získá z prvního otisku a zachycených biometrických dat a je taktéž uložen do podepisovaného dokumentu. Zajišťuje spojení dokumentu a biometrického podpisu.
7. Dokument je uložen. [2, s. 321]

Zajištění integrity dokumentu

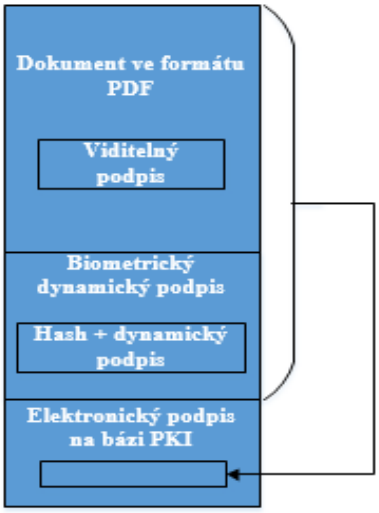
Princip pro zajištění integrity PDF dokumentu s využitím hashe a dynamického biometrického podpisu zachycuje následující obrázek.



Obr. č. 4: Princip zajištění integrity PDF dokumentu s využitím hashe a dynamického biometrické podpisu (Zpracování vlastní dle: [2, s. 329])

Podepisující osoba se podepíše na podpisový tablet. Tablet podpis nasnímá a vytvoří statický podpis a dynamický podpis. Ke statickému podpisu se doplní údaje (jako například čas podpisu, důvod atd.) a následně se vloží do PDF dokumentu jako viditelný podpis. Dynamický podpis se spojí s hashem PDF dokumentu a tím vznikne základ pro dynamický elektronický podpis. Před vložením do dokumentu se vloží do elektronické obálky (zašifruje se). Poté je vložen do PDF dokumentu. [2, s. 329]

V některých případech se dynamický biometrický podpis doplňuje o další zaručené elektronické podpisy nebo elektronické pečetě. Především v uzavřených systémech, kdy je jednou stranou provozován celý systém včetně PKI. Pracovník společnosti může vytvářet podpis na bázi PKI, je vybaven například čipovou kartou. Jako první podpis je zachycen dynamický biometrický podpis klienta a jako druhý následuje PKI podpis pracovníka společnosti, následně může dojít ještě k doplnění časovým razítkem. [2, s. 329] Tento princip zachycuje následující obrázek.



Obr. č. 5: Princip zajištění integrity PDF dokumentu s využitím hashe, dynamického biometrické podpisu a elektronického podpisu na bázi PKI (Zpracování vlastní dle: [2, s. 330])

Normy pro DBP

Mezi základní normy patří:

- ISO/IEC 19794-7: Information technology – Biometric data interchange formats Part 7: Signature/sign time series data
- ISO/IEC 19794-11: Information technology – Biometric data interchange formats Part 11: Signature/sign processed dynamic data
- ISO/IEC 29109-7: Conformance Testing Methodology for Biometric Data Interchange formats defined in ISO/IEC 19794 – Part 7: Signature/sign series data
- ISO/IEC 29109-11: Conformance Testing Methodology for Biometric Data Interchange formats defined in ISO/IEC 19794 – Part 11: Signature/sign processed dynamic data [2, s. 332]

Tyto normy byly vydány jako české technické normy:

- ČSN ISO/IEC 19794-1 Informační technologie – formáty výměny biometrických dat – Část 1: Struktura
- ČSN ISO/IEC 19794-7 Informační technologie – formáty výměny biometrických dat – Část 7: data podpisových řad podpisu/značky [2]

ČSN ISO/IEC 19794-1

Norma říká, že *„pro ochranu autenticity, integrity a důvěrnosti uložených a přenášených biometrických dat se doporučuje použít kryptografické techniky“*. Dle části normy

Stárnutí a trvání použití je nutno specifikovat základní periodu použití biometrických referenčních dat, a to z důvodu změn řady biometrických charakteristik s rostoucím věkem osoby. [2, s. 333]

ČSN ISO/IEC 19794-7

Definuje strukturu výstupních dat vznikajících během procesu podepisování v tabletu. Dle této normy jsou zachytávány následující charakteristiky ve formě časových řad. Tyto parametry zachycuje následující tabulka, přičemž použití charakteristik X a Y je povinné, dále je nutné zahrnout T nebo DT nebo musí být indikované rovnoměrné vzorkování. Zahrnutí dalších charakteristik je volitelné, je nutné zmínit, že počet analyzovaných charakteristik ovlivňuje spolehlivost a jednoznačnost autentizace podepisující se osoby. [2, s. 335–336]

Tab. č. 1: Zaznamenávané charakteristiky (Zpracování vlastní dle: [2, s. 335])

Název charakteristiky	**Popis charakteristiky**
X	Souřadnice x – horizontální poloha pera
Y	Souřadnice y – vertikální poloha pera
Z	Souřadnice z – výška pera nad psací plochou
T	Čas
DT	Časový rozdíl
AX	Zrychlení ve směru x
AY	Zrychlení ve směru y
VX	Rychlost ve směru x
VY	Rychlost ve směru y
F	Tlak na hrot pera
S	Stav hrotu – dotyk / nedotyk hrotu psací plochy
TX	Náklon podél osy x
TY	Náklon podél osy y
R	Rotace kolem osy pera
AZ	Uhel natočení pera
EI	Uhel úklonu pera

3.2.3 Shrnutí porovnání

Spojení hashe digitálního dokumentu biometrickými daty podpisu vytváří propojení mezi dynamickým podpisem a hashem digitálního dokumentu. Zašifrováním těchto vstupů vznikne ochrana proti zneužití vzniklého dokumentu, tato ochrana znemožňuje neoprávněné připojení dynamického biometrického podpisu k jinému dokumentu v případě dešifrování či prolomení šifry. U kryptografického elektronického podpisu na bázi kryptografických metod je podpis bezprostředně propojen s dokumentem. [2, s. 330]

Kryptografický **elektronický podpis je** tedy **výsledkem kryptografických operací provedených nad konkrétním textem (podepisovaným dokumentem) a soukromým klíčem**, zatímco **dynamický biometrický podpis je výsledkem činnosti podepisující se osoby a vložen do podepisovaného dokumentu**. S textem, který je uveden na podepisovaném dokumentu, nemá nic společného. [2, s. 330] Proto se pro dokumenty opatřené DBP používají další kryptografické operace, které umožňují ochránit DBP a integritu dokumentu, jak jsou popsány výše. Na rozdíl o kryptografického elektronického podpisu jde o operace, které nezávisí na klíčích a certifikátech uživatele, což činí proces podepisování a související organizační požadavky (uchovávání klíčů, obnova certifikátu apod.) pro něj daleko jednodušším.

3.3 Popis ochrany před padělaním DBP

Jako jeden z argumentů proti dynamickému biometrického podpisu jsou změny v podepisování. Zde je nutno zmínit skutečnost, že žádné dva podpisy nejsou zcela stejné, vždy existují určité odchylky od podpisů stejného jedince. Naopak dva zcela identické podpisy mohou nasvědčovat tomu, že se jedná o padělek. [19] Podepisující osoba má v procesu podepisování specifickou sadu pohybů, čímž vznikají tzv. markanty podpisu. Experimenty bylo ověřeno, že biometrická data získaná při vytváření podpisu poskytují takový soubor informací, který umožní při použití automatického vyhodnocování validačním programem odhalit jakýkoliv padělek DBP. Podrobnější popis je uveden v: [14]

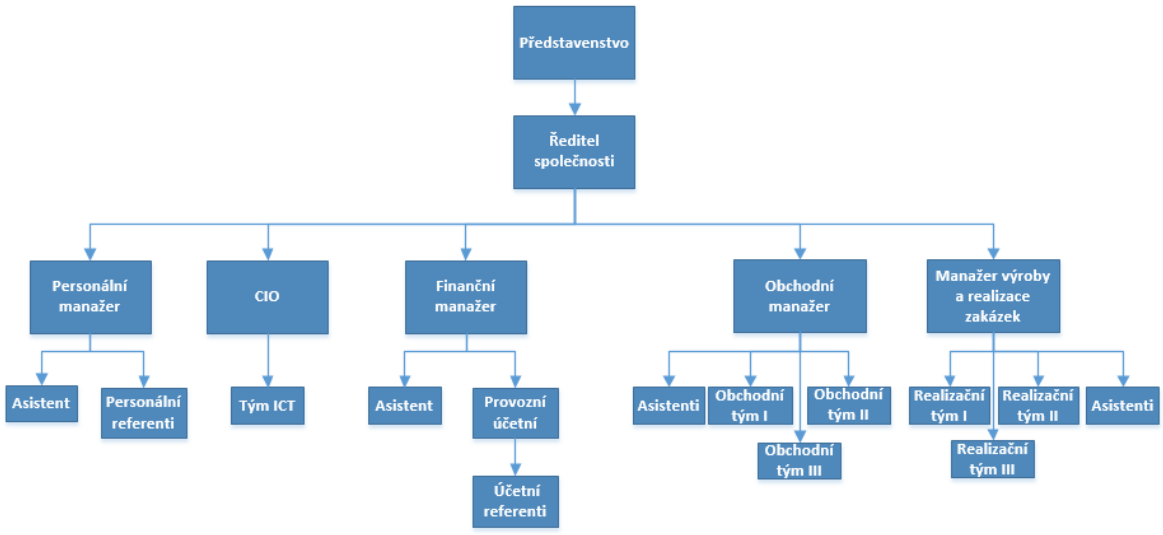
Výsledky výše uvedeného experimentu mluví ve prospěch důvěryhodnosti dynamických biometrických podpisů. Z experimentu též vyplývá, že služby písmoznalce je třeba využít až v krajních případech ověřování pravosti, tedy běžně postačí implementace validačního serveru. V případě on-line ověření dynamického biometrického podpisu je nutné vyřešit správu zabezpečené databáze podpisových vzorů, stejně tak i zabezpečit privátní klíč vydaný certifikační autoritou, a taktéž její kořenový certifikát. [14, s. 1 až 8]

4 ANALÝZA SOUČASNÉHO STAVU

V této části je popsána analýza současného stavu zpracování daňových dokladů v modelovém podniku.

4.1 Charakteristika modelové firmy

Jedná se o středně velký podnik, který poskytuje jak své služby, tak i výrobky a je plátcem DPH. Strukturu firmy zobrazuje následující organizační schéma. V čele modelové firmy stojí představenstvo, přímo podřízeným je ředitel společnosti. Na další úrovni jsou manažeři jednotlivých oddělní – CIO, finanční, personální, obchodní manažer a manažer výroby a realizace zakázek. Finanční manažer, jak již název napovídá, vede finanční oddělení. Toto oddělení tvoří asistent provozní účetní a účetní referenti. Obchodní oddělení a oddělení výroby a realizace zakázek, jsou tvořeny asistenty a jednotlivými týmy, v jejichž čele stojí vedoucí týmů. Pravomoc účastnit se procesu zpracování daňových dokladů má 25 osob – ředitel, manažeři, asistenti, vedoucí týmů, provozní účetní a referenti.



Obr. č. 6: Organizační struktura podniku

Dokumenty v podniku

V podniku se pracuje s nejrůznějšími dokumenty. Velká většina jich je v papírové (listinné) podobě, v elektronické podobě minimum. Nejvíce dokumentů představují doklady daňové (faktury). Během období jednoho roku jich firma zpracuje v průměru

5 240 ks. Daňové doklady jsou rozděleny na vystavené a přijaté, dle jejich podoby v elektronické či listinné. **Vystavené daňové doklady** jsou vytvořeny v ERP systému firmy – obsahují veškeré náležitosti dle zákona[12]. Tyto doklady prezentují pohledávky firmy. **Přijaté daňové doklady** jsou doručeny do firmy kanálem pošty či emailem od dodavatelů a představují závazky firmy.

Veškeré daňové doklady – vystavené i přijaté, jsou archivovány v listinné podobě, pouze elektronicky doručené dokumenty jsou uloženy zároveň ve file systému v odpovídajících složkách. Papírové složky pro evidenci daňových dokladů, jsou velice obsáhlé, často nepřehledné a jednoduše může dojít k jejich ztrátě či poškození. Papírovou evidenci je nutno skladovat ve vhodných podmínkách a její životnost je omezená.

Z výše uvedeného odstavce vyplývá, že papírová evidence není příliš šťastné řešení. A to nejen z důvodu nepřehlednosti, robustnosti, rizik spojených s jejich uchováváním (povodně, hlodavci apod.), ale taktéž nastává problém s vhodným uložením a archivováním. Neustálý vývoj informačních technologií a zároveň odpovídající legislativy umožňuje odstranit tyto nedostatky a využívat jiný způsob evidence a archivování. Výše zmíněné dokumenty má povinnost vést každý podnik, proto byla zvolena tato konkrétní problematika, vytvořenou metodiku bude tedy možné aplikovat s úpravami i na jiné podniky. Z popisů stávajících stavů procesů uvedených níže vyplývá, že vedení dokumentů především v listinné podobě, včetně jejich schvalování, resp. vyplňování pověřenými osobami, je nedokonale řešeno a nese s sebou zbytečný čas spojený s fyzickou distribucí a vyřízením těchto dokumentů. V tomto místě je tedy prostor pro jejich zlepšení.

Zlepšením se jeví přechod na elektronickou formu dokumentů s využitím elektronického podpisu, a to konkrétně dynamického biometrického podpisu. Tento způsob podepisování byl zvolen z důvodu uživatelské přívětivosti, neboť jeho vytvoření je jednoduché a zároveň není potřeba zvláštních dovedností pro jeho vytvoření. V případě podepisování dynamickým biometrickým podpisem se uživatel podepíše pomocí speciálního pera na podpisový pad a podpis je hotový. V případě vytváření kryptografického elektronického

[12] Dle ustanovení § 29 z. č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

podpisu musí být certifikát nainstalovaný na daném zařízení, ze kterého se chce podepisující podepsat, či je nutno využít připojené zařízení k počítači v případě uložení certifikátu na čipové kartě, k podepsání lze využít software, například Adobe Acrobat Reader DC, a v panelu Nástroje – Certifikáty pomocí funkcionality Digitálně podepsat jej označit podpisem. Při podepisování PDF dokumentu kryptografickým elektronickým podpisem je nutno, aby podepisující zadal heslo či PIN umožňující přístup k jeho privátnímu klíči; uživatelé si tedy musí pamatovat heslo a při každém podepsání jej zadávat. Při uložení privátního klíče na nějakém tokenu ještě jej mít fyzicky k dispozici. Nutnost zadání hesla v případě podepisování dokumentu dynamickým biometrickým podpisem odpadá. Taktéž oproti kryptografickému elektronickému podpisu odpadá nutnost obnovy certifikátu po uplynutí doby platnosti. Pro implementaci dynamického biometrického podpisu taktéž hovoří výsledky experimentu zabývajícího se paděláním, který je uveden v kapitole výše[13], neboť je z praxe známo, že podepisovací tokeny jsou často svěřovány k podepisování jiným osobám, typicky asistentům/kám.

4.2 Popis stávajícího stavu procesů

V této části jsou popsány aktuální stavy procesů v modelovém podniku – procesy zpracování přijatého / vystaveného daňového dokladu.

4.2.1 Proces zpracování přijatého daňového dokladu

Proces zpracování přijatého daňového dokladu emailem je následující. Elektronické daňové doklady jsou přijaty prostřednictvím emailu, kanál datových schránek není využíván. Daňové doklady jsou předány na účetní oddělení, kde jsou provozní účetní vytištěny, zaevidovány a je zkontrolovaná jejich úplnost a formální správnost. V případě nalezení chyby je daňový doklad vrácen dodavateli. Proběhne-li korektně ověření správnosti, je vytvořena tzv. košilka – dokument, který se přikládá ke každému daňovému dokladu, obsahuje jeho základní identifikační údaje a jsou na něm uvedeni jeho schvalovatelé.

Následně určí provozní účetní dle podnikového podpisového řádu osobu, příp. osoby, jež budou odpovědny za schválení. Výběr odpovědných osob je proveden na základě dvou

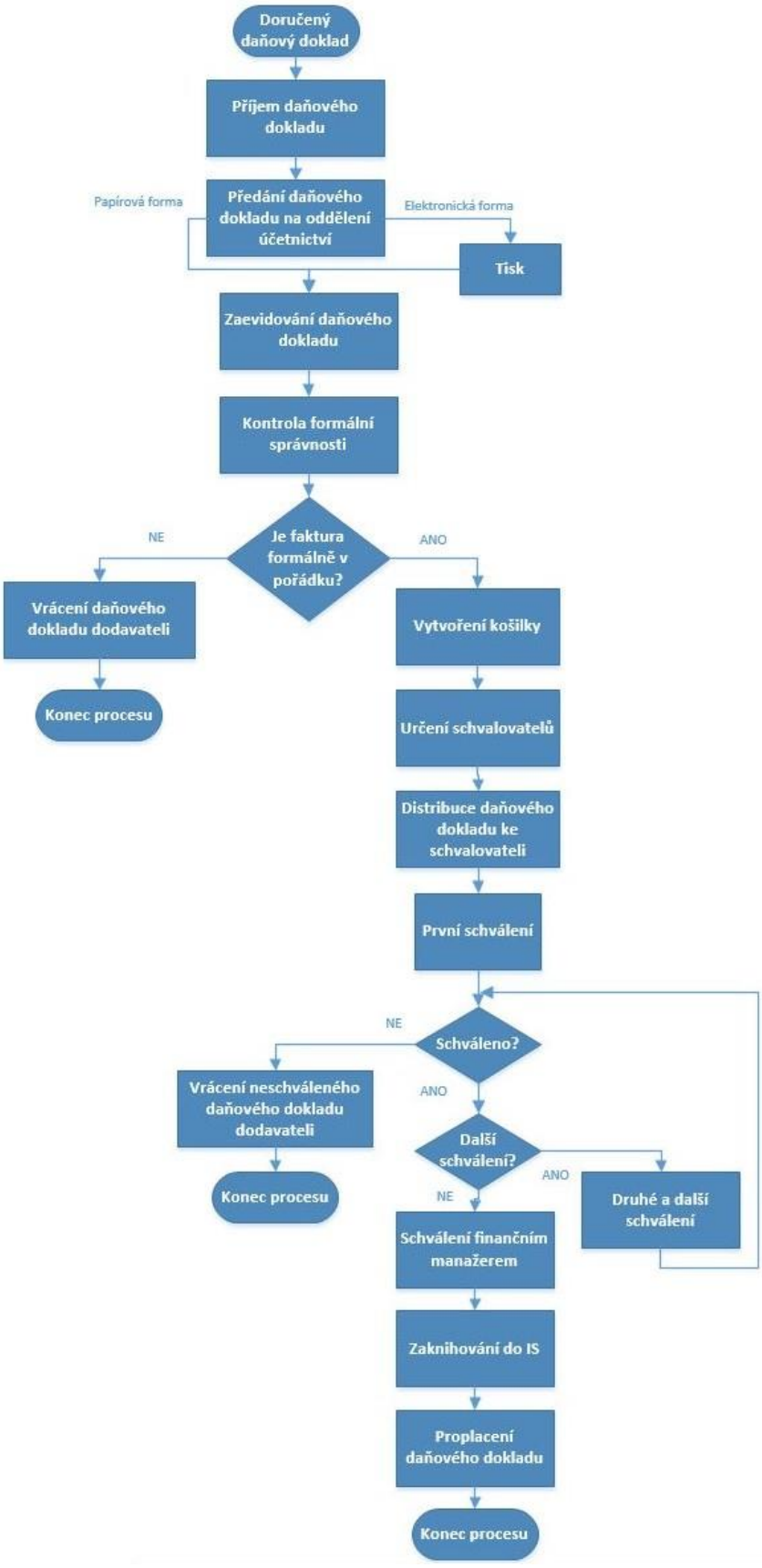
[13] Popis ochrany před paděláním.

kritérií, a to textu položky na daňovém dokladu a celkové částky na faktuře. Tito schvalovatelé jsou uvedeni na košilce a svými podpisy schvalují proplacení uvedené částky, případně výši uvedené částky. Takto připravené daňové doklady jsou distribuovány v listinné podobě schvalovatelům. Schvalovatel stvrzuje svým podpisem na košilce, že fakturovaná částka či služby odpovídají skutečnosti. Poté připojí k daňovému dokladu objednávku a vrátí zpět provozní účetní či ji v případě nutnosti předá dalšímu schvalovateli ke schválení. V případě, že daňový doklad obsahuje věcné chyby, je tato skutečnost zaznamenána na košilku a je vrácen provozní účetní.

Pokud daňový doklad schvalují další schvalovatelé, například proto, že je fakturovaná částka vyšší nebo se na ní nachází více oblastí nákladů, je distribuován dále. Proces schvalování je stejný jako v předchozím případě.

Po schvalovacím kolečku je daňový doklad provozní účetní předán finančnímu manažerovi k poslednímu podpisu. Takto schválený daňový doklad se ručně knihuje do informačního systému firmy, tedy dochází k jeho ručnímu zaúčtování, zápisu do účetních knih vedených v ERP systému podniku, a poté je předán k proplacení.

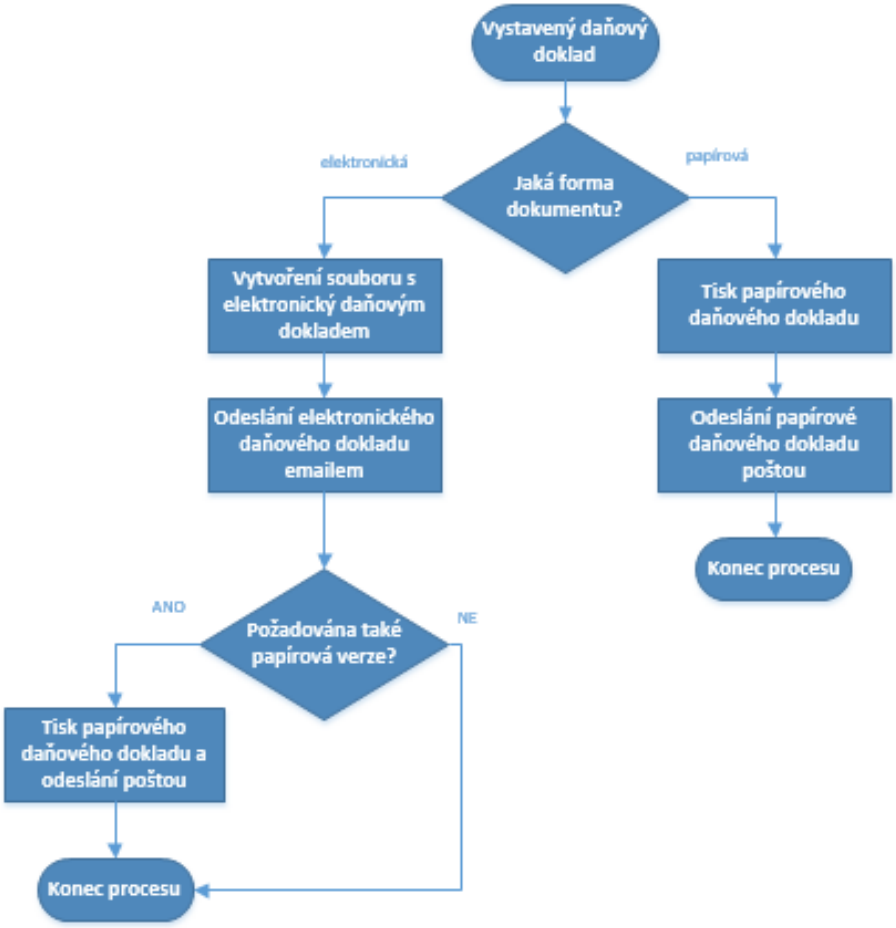
Proces zpracování přijatých daňových dokladů v listinné podobě je stejný jako v podobě elektronické, pouze je vynechán krok tisku.



Obr. č. 7: Proces zpracování přijatého daňového dokladu

4.2.2 Proces zpracování vystaveného daňového dokladu

Vystavené daňové doklady v informačním systému jsou odeslány odběrateli elektronicky ve formátu pdf, či vytištěny a odeslány v listinné podobě. Pokud jsou daňové doklady odesílané elektronicky a odběratel požaduje taktéž listinnou podobu, ačkoliv to dnes již naprosto není nutné, je elektronický daňový doklad vytištěn a odeslán poštou. S odběrateli, kterým jsou odesílány daňové doklady v elektronické podobě, je zajištěn souhlas s tímto způsobem zasílání a zpracování[14]. Daňové doklady zaslané emailem nejsou opatřeny elektronickým či jiným podpisem, PDF daňový doklad je platným dokladem, stejně jako daňový doklad v papírové podobě.



Obr. č. 8: Proces zpracování vystaveného daňového dokladu

[14] Dle ustanovení § 26 odst. 3 z. č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

4.3 Zhodnocení stavu stávajících procesů

Z výše uvedených procesních diagramů lze vidět, že schvalování, resp. vyplňování dokumentů může probíhat i na více stupních. Veškerá související dokumentace nezbytná pro schválení, vyplnění dokumentů probíhá v listinné podobě, je tedy nutné tuto dokumentaci vždy tisknout a fyzicky distribuovat patřičným pozicím. To s sebou přináší vyšší náklady na tisk a delší čas potřebný pro vyřízení spojený s fyzickou distribucí dokumentů. Proto lze navrhnout, aby byly tyto procesy upraveny a dokumenty plně digitalizovány. Dokumenty budou vedeny v elektronické podobě, stejně tak i dále předávány. Vznikne nové workflow, dokumenty budou předávány v elektronické podobě ve formátu PDF. K jejich podepsání či vyplnění bude využit dynamický biometrický podpis, který bude snímán pomocí speciálního podpisového padu a pera. Konkrétní návrh řešení je uveden v kapitolách níže.

5 NÁVRH ŘEŠENÍ

5.1 Popis procesu zpracování dokladů po zavedení dynamického biometrického podepisování

V případě zavedení dynamického biometrického podpisu do procesu zpracování daňových dokladů budou všechny doklady soustředěny v elektronické podobě (listinné převedeny skenováním) a následně budou tyto doklady v elektronické podobě podepsány biometrickým podpisem. Tím bude zaručena věrohodnost původu dokladů, neporušenost obsahu a jeho čitelnost. V elektronické podobě budou doklady taktéž uchovávány pro případnou další potřebu. To s sebou přinese lepší přehlednost v evidenci, urychlení procesů (včetně možnosti snadného vyhledávání) či snížení nákladů na tisk a skladování. Uložení dokladů v tomto případě zabezpečí elektronické úložiště. Toto úložiště je ochrání před jejich zneužitím, poškozením, zničením, neoprávněnou změnou, ztrátou či odcizením. Podstatné je rovněž to, že elektronické úložiště se může vyskytovat ve více exemplářích, tj. být vytvářeny repliky v reálném čase, a to i na geograficky vzdáleném místě, což výrazně zvýší ochranu dokumentů před většinou rizik.

5.2 Hlavní přínosy řešení

Implementace dynamického biometrického podpisu s sebou přináší mnoho přínosů, přičemž lze jmenovat:

- zjednodušená a zrychlená práce s doklady v Document Management System (dále jen DMS)
- uchovávání podepsaných dokladů pouze v elektronické podobě
- s předchozím bodem související snížení nákladů na zpracování, tisk a uchovávání (finanční vyjádření v závěru diplomové práce)
- uspořádané a přehledné uložení dokladů s možností prakticky libovolného vyhledávání a dataminingu
- zabezpečené uložení citlivých dokladů s omezeným přístupem
- notifikace v případě vzniku workflow, jeho vykonání, ukončení apod.
- jednoduchá autentizace uživatelů s využitím adresářových služeb LDAP (Active Directory, dále AD)
- snížení chybovosti při ručním přepisu dat do informačního systému

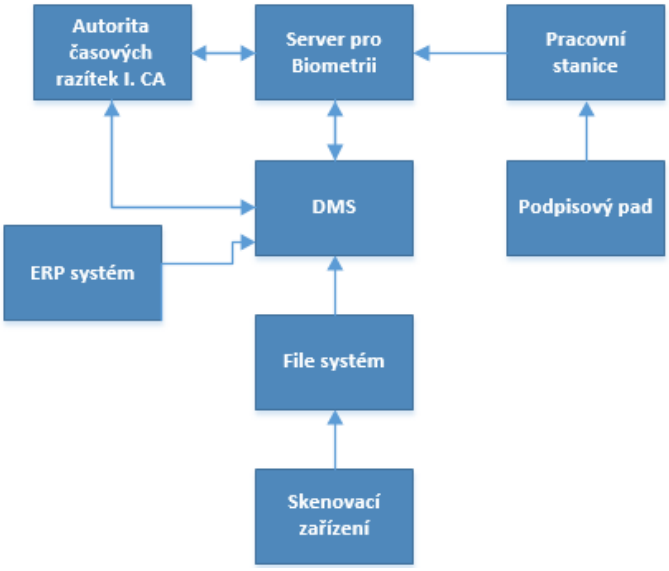
- snížení rizika ztráty či zničení papírového dokladu (listiny).

5.3 Funkční návrh

5.3.1 Základní schéma řešení

Veškeré listinné doklady budou skenovány a v elektronické podobě ve formátu PDF spravovány v DMS systému s napojením na zabezpečené úložiště. Do DMS budou importovány komponentou z file systému. Pro biometrické podepisování budou využity podpisové pady a dostupná aplikace pro biometrické podepisování dokumentů. Jakmile bude zahájeno schvalovací (podpisové) workflow, dojde k odeslání notifikace příslušných osobám pomocí emailu a v DMS se uloží vstupní verze dokumentu – bez podpisů.

Po posledním podpisu se vstupní verze přeuloží „obrazem“ podepsaného dokumentu – s podpisy, ale bez biometrických údajů. „Obraz“ bude dostupný ke čtení pro běžné uživatele v DMS. Podepsaný dokument s biometrickými daty bude označen časovým razítkem autority časových razítek (poskytovatelem služeb vytvářejících důvěru) a uložen do zabezpečeného archivu DMS do zvláštních složek, k nimž bude mít přístup pouze specifikovaný okruh osob, pro ostatní uživatele nebude tato verze dostupná. Taktéž bude zajištěno napojení na Active Directory (AD) pro autentifikaci uživatelů z ERP systému firmy a pro import dokladů do DMS. DMS a server pro biometrii budou napojeny na autoritu časových razítek – I.CA. Základní schéma řešení zobrazuje následující obrázek.



Obr. č. 9: Základní schéma řešení

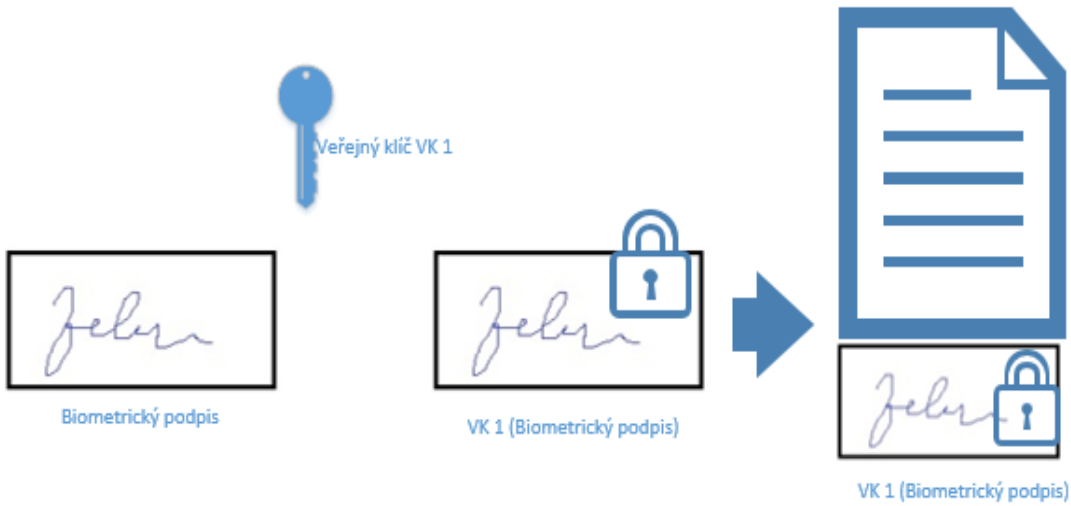
5.3.2 Popis podepsání dokumentu a označení časovým razítkem

Pro zabezpečení biometrických dokumentů budou použity tyto prvky:

Tab. č. 2: Prvky použité pro zabezpečení biometrických dokumentů

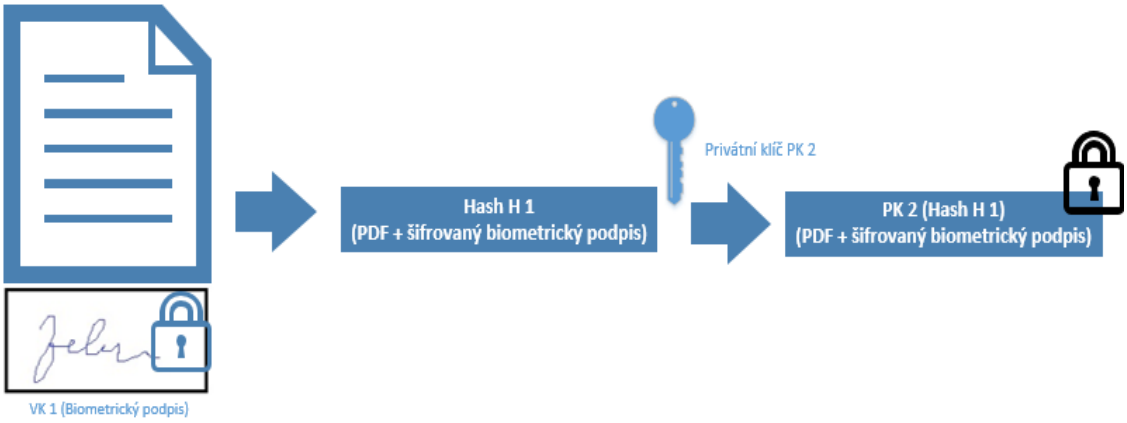
Označení	Algoritmus	Popis prvku
PK 1	RSA-3072	Privátní klíč, používá se pouze v případech soudních sporů pro dešifrování biometrických dat, kdy dojde za předem stanovených podmínek k dešifrování u konkrétního biometrického podpisu u certifikační autority. Je bezpečně uložený u certifikační autority.
VK 1	RSA-3072	Veřejný klíč, který je pevně svázán s PK 1, slouží k finálnímu šifrování biometrických dat. Je uložen na biometrickém serveru.
PK 2	RSA-2048	Privátní klíč, který slouží k elektronickému podepsání PDF a je uložen v zabezpečené formě na biometrickém serveru.
VK 2	RSA-1024	Veřejný klíč, který je pevně svázán s VK 2, slouží k ověření elektronického podpisu. Je ukládán do PDF dokumentu jako součást elektronického podpisu.
H 1	RIPEMD-160/320	Hash dokumentu, který obsahuje šifrovaná biometrická data, je určený pro vytvoření elektronického podpisu.
H 2	SHA-256	Hash dokumentu, který obsahuje čitelná biometrická data.

Biometrická data v šifrované podobě jsou přijata na server a dochází k jejich dešifrování. Následně se data v čitelné podobě zašifrují asymetrickým algoritmem RSA-3072 pomocí veřejného klíče VK 1. Šifrovaný podpis je následně vložen do dokumentu PDF.



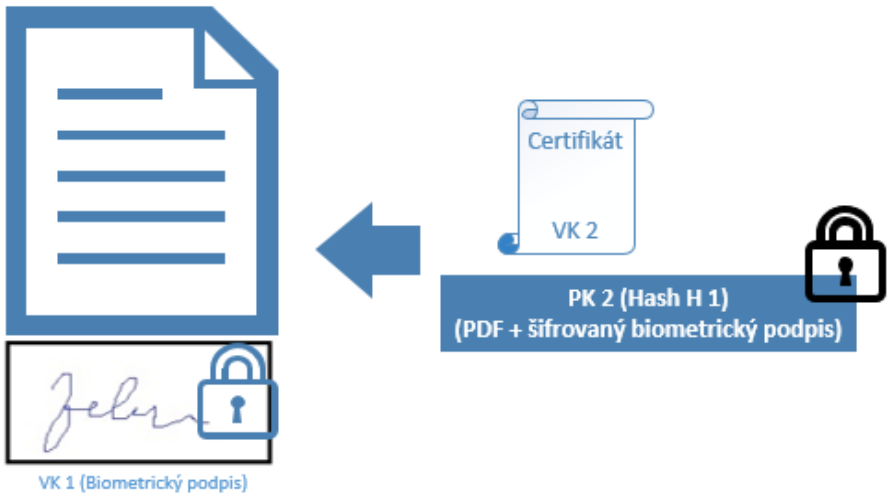
Obr. č. 10: Šifrování podpisu a jeho následné vložení do dokumentu

Proces elektronického podepsání dokumentu probíhá takto: Dojde k výpočtu hashe H 1. Tento hash se podepíše privátním klíčem PK 2.



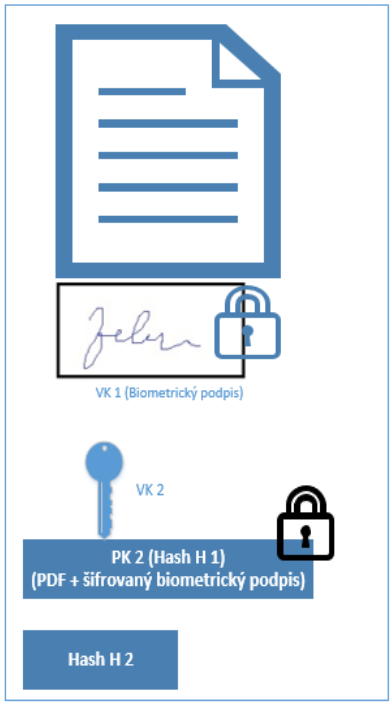
Obr. č. 11: Výpočet hashe H 1 a jeho podepsání privátním klíčem

Takto podepsaný hash H 1 se společně s veřejným klíčem VK 2 (certifikátem) vloží do PDF dokumentu.



Obr. č. 12: Vložení hashe do dokumentu

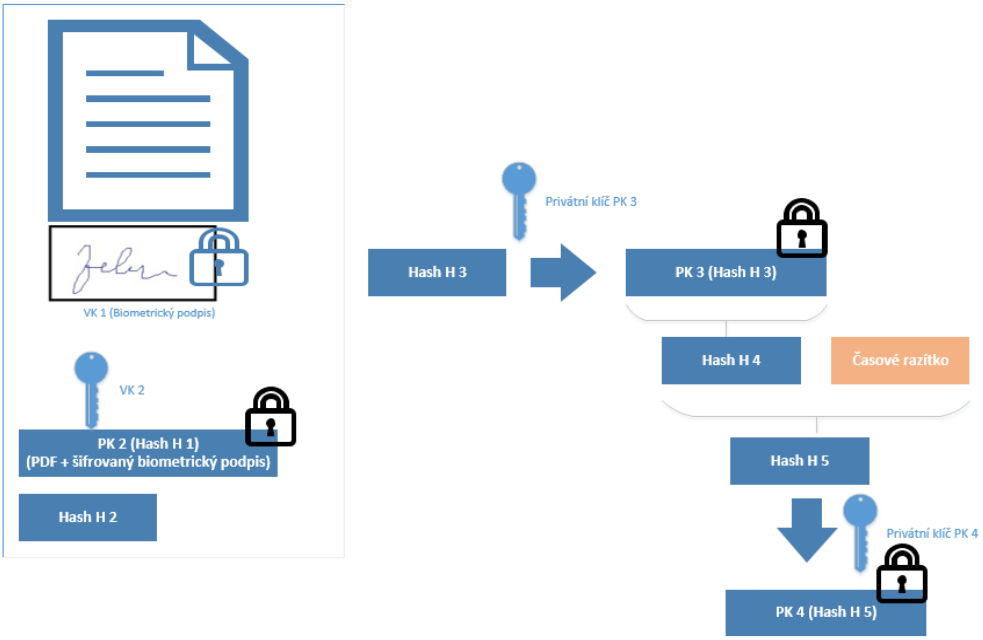
Dokument, který je podepsaný jedním podpisem, má tedy tuto strukturu.



Obr. č. 13: Struktura dokumentu s jedním podpisem

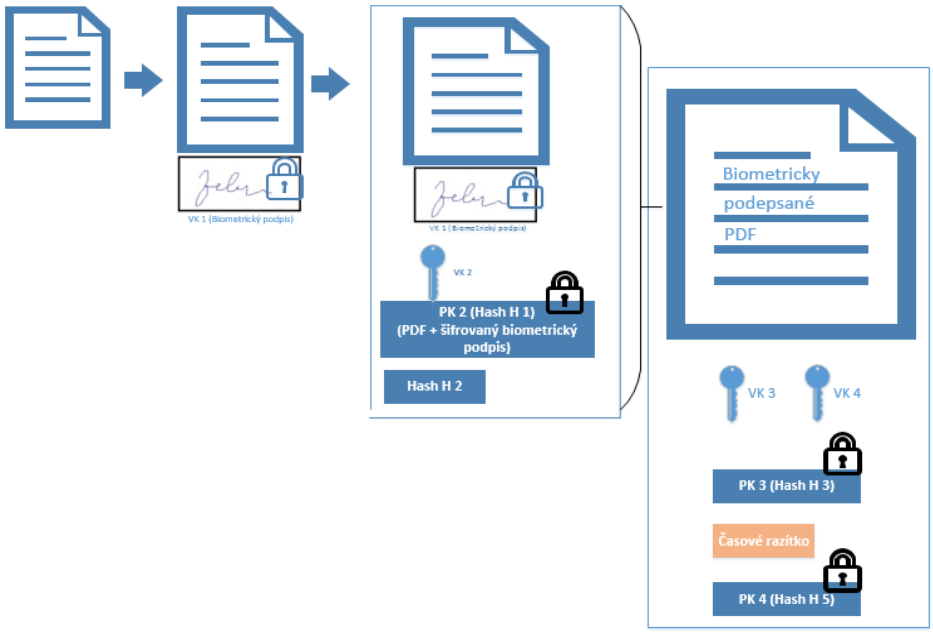
Při dalším podpisu se celý proces opakuje. Po posledním podpisu je vytvořen hash, na obr. č. 14 H 3, ten je zaslán na server autority časových razítek (poskytovatele služeb vytvářejících důvěru). Na serveru autority dojde k vytvoření časového razítka a jeho předání zpět na biometrický server podniku. Na biometrickém serveru je vložen do PDF.

Časové razítko se využívá pro účel prodloužení časové kontinuity a tedy garance, že daný dokument existoval v daném čase.



Obr. č. 14: Připojení časového razítka

Všechny změny původního PDF během procesu podepisování a razítkování zachycuje přehledně následující obrázek č. 15.



Obr. č. 15: Struktura podepsaného dokumentu s přidaným časovým razítkem

5.3.3 Ověření dokumentu

Při ověřování bude možné ověřit elektronické podpisy či ověřit biometrické podpisy.

5.3.3.1 Ověření elektronických podpisů

Pomocí veřejného klíče VK 2 dojde k dešifrování elektronického podpisu, tím získáme hash dokumentu H 1. Zde platí předpoklad důvěry certifikátu obsahujícího veřejný klíč VK 2. Výpočtem hashe a jeho porovnání s dešifrovanou podobou dojde k prokázání, zda bylo manipulováno s dokumentem či nikoliv.

5.3.3.2 Ověření biometrických podpisů

Privátní klíč PK 1, který je potřeba k ověření biometrických podpisů je dostupný u certifikační autority, proto je možné ověření provést pouze u ní. Pomocí tohoto klíče dojde k dešifrování biometrických dat. Následuje druhá část, kdy písmoznalec pomocí patřičných nástrojů ověří pravost podpisu.

5.4 Návrh procesní

5.4.1 Proces zpracování přijatého daňového dokladu

K přijímání daňových dokladů bude i nadále využíván kanál emailu, pro elektronickou formu, a pošty či osobní předání pro listinnou formu. Doklady doručené v listinné podobě budou skenovacím zařízením naskenovány a dočasně uloženy ve stávajícím file systému.

Pomocí OCR technologie dojde k vytěžení textu, kdy OCR systém převede vstupní informace na obraz a z tohoto obrazu následně automaticky rozpozná znaky. Tato technologie pracuje na principu klíčových slov, kdy se naučí klíčová slova a poté je hledá v dokumentech, pokud klíčové slovo najde, hledá kolem něj hodnotu, která by měla být s tímto klíčovým slovem svázána. Další princip, na kterém technologie funguje, je princip šablony, kdy je pro dodavatele tvořící největší objem dokladů vytvořena šablona, která má definované umístění vytěžovaných informací.

Kvalita a kompletnost vytěženého textu záleží na kvalitě vstupního obrazu. V případě vytěžování informací z faktur bude vytěžováno co nejvíce informací. Jsou určeny povinné atributy, které se musí pomocí OCR technologie vytěžit – identifikační údaje FO,

PO, DIČ v případě plátce DPH, základ, sazbu a výši DPH, cenu bez DPH a případné slevy. Dojde-li k vytěžení minimálně těchto povinných atributů, je dokument připraven k importu. Pokud nedojde k vytěžení těchto povinných atributů, je informován pracovník, který vytěžené informace zkontroluje a potřebné chybějící údaje doplní. Pokud systém vyhodnotí, že je kvalita vstupního obrazu nedostačující a nelze z něj vytěžit, je taktéž předán k ručnímu zpracování. Pokud bude určeno, že se nejedná o daňový doklad, bude tento doklad označen jako „ostatní“, k jeho importu nedojde.

Následně budou dokumenty v dávkách importovány z file systému do DMS. Doklady přijaté emailem budou po přijetí rovnou importovány do DMS, pokud mají strukturovanou podobu. Pokud mají nestrukturovanou podobu, dojde také k vytěžení textu. Při importu dochází ke klasifikaci dat, jejímž cílem je identifikovat daňové doklady, přičemž ty, které jimi nejsou, je třeba vyřadit z procesu zpracování a předat je odpovědné osobě ke zpracování. Importní nástroj taktéž zajišťuje automatickou tvorbu knihy došlých faktur. Zároveň je nastartované workflow a daňový doklad je odeslán ke zpracování. S každým vygenerovaným úkolem, či zpracovaným úkolem ve workflow jsou odesílány emailem notifikace o nově vzniklém úkolu.

Prvním krokem workflow je kontrola formálních náležitostí. Elektronicky přijímané doklady nemusí být dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů opatřeny podpisem, není tedy dodavatelů vyžadován podepsaný daňový doklad. V případě, že je přesto daňový doklad podepsán elektronickým podpisem, či elektronickou značkou (podle Nařízení elektronickou pečetí) ověří se platnost certifikátu, na němž je založen. Toto ověření je zajištěno spojením DMS s certifikační autoritou (kvalifikovaným poskytovatelem služeb vytvářejících důvěru[15]), která vydala certifikát, a automatizovaným způsobem dojde k jeho ověření či porovnání vydaných RCL, jehož výsledkem je informace o platnosti, resp. neplatnosti certifikátu. Pokud není certifikát platný, bude doklad předán do kroku vrácení dodavateli a proces workflow je ukončen. Pomocí VK dojde k dešifrování a získání hashe. Tento hash je porovnán s vypočítaným hashem a jejich porovnáním dojde k prokázání, zda bylo s dokumentem manipulováno či nikoliv. Pokud bude přijatý dokument podepsán dynamickým

[15] Poskytující poskytuje kvalifikovanou službu ověřování platnosti dle Nařízení eIDAS §33 res. §40.

biometrickým podpisem, bude docházet pomocí veřejného klíče k dešifrování elektronického podpisu a získaný hash, bude porovnán s hashem vypočítaným, tak dojde jako v přechozím případě k prokázání, zda bylo s dokumentem manipulováno. K ověření biometrických podpisů bude docházet pouze v případě soudních sporů a bude prováděno u certifikační autority.

Proces vrácení dokladu dodavateli je následující: Workflow doklad distribuuje pracovníkovi, který je odpovědný za jeho vrácení – provozní účetní, je nastartován úkol vrácení dokladu. Tento pracovník v DMS vybere odpovídající šablony zprávy v MS Word, do které DMS doplní informace o vráceném dokladu, důvod vrácení, kontakt na odpovědného pracovníka a datum vrácení. Odpovědný pracovník ke zprávě připojí doklad a odešle ji zpět dodavateli. Pracovník poté označí úkol v DMS jako vyřízený.

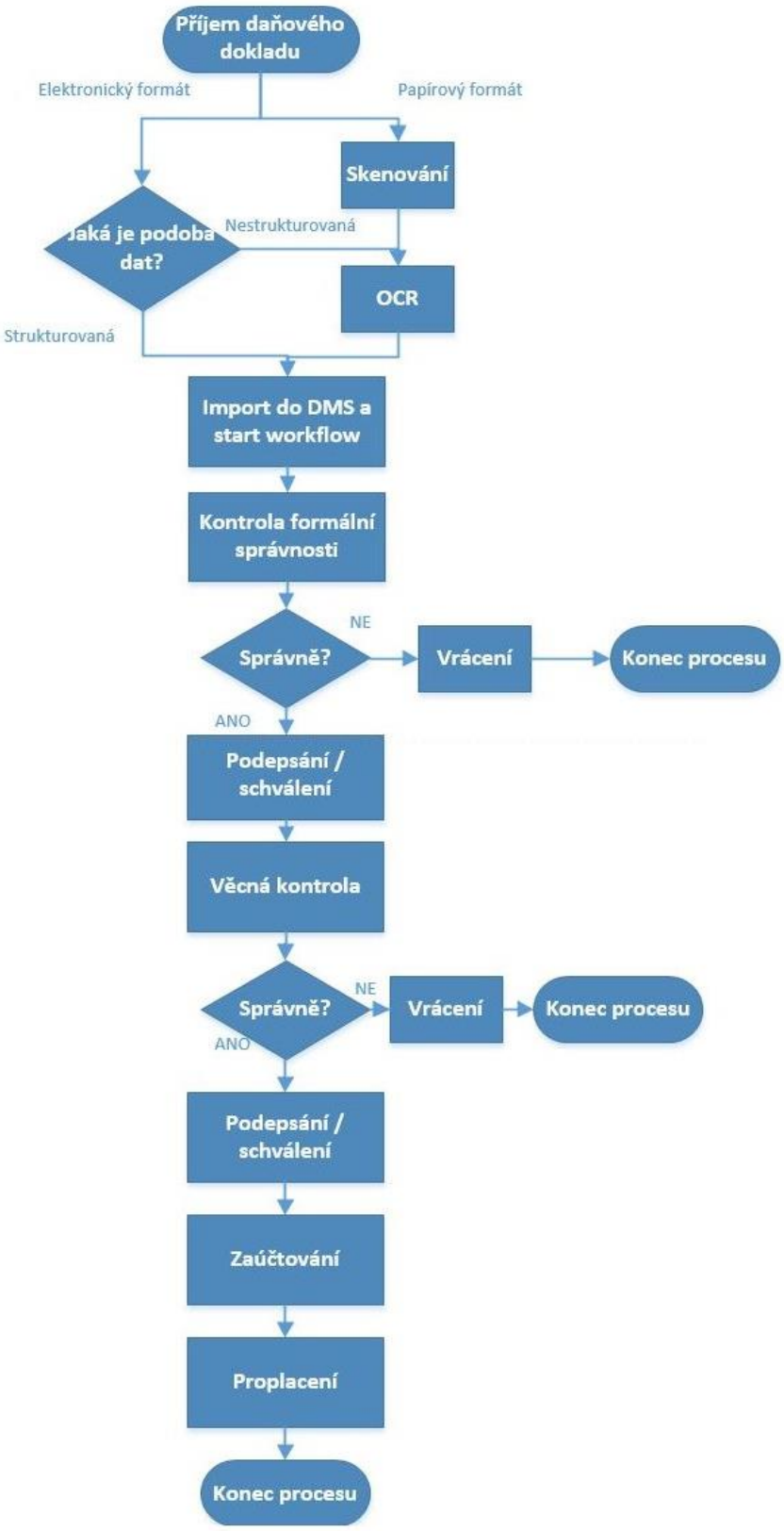
V případě bezproblémové kontroly formálních náležitostí dochází následně k věcné kontrole tedy, že fakturované plnění bylo dodané. Schvalovatelé věcného plnění jsou zaměstnanci, kteří plnění přijali či odpovídají za oblast, které se plnění týká. Schvalování může probíhat víceúrovňově. Schvalovatel si zobrazí úkol v DMS. Ověří věcnou správnost a v případě shody jej pomocí podpisového padu opatří svým podpisem – viz níže. Je-li vyžadované další schválení, předá jej dál. Pokud není příslušným schvalovatelem, vrátí doklad vlastníkovi procesu zpracování daňových dokladů – tedy provozní účetní, případně jej předá na správného schvalovatele. V případě, že věcné plnění neodpovídá, vyplní důvod neschválení a následuje krok vrácení dokladu dodavateli.

Po posledním potřebném schválení může dojít k zaúčtování. To provádí účetní v ERP systému. Jakmile zaúčtování provede, je tento výsledek předán z ERP do DMS systému včetně data zaúčtování. Pokud k zaúčtování nedojde, je z ERP do DMS předán výsledek nezaúčtováno, včetně důvodu, DMS následně zašle doklad pracovníkovi odpovědnému za řešení této situace.

Posledním krokem je samotné proplacení dokladu na základě jeho schválení k proplacení. Toto schvalování provádí finanční manažer. Ověří, zda je možné doklad proplatit. Pokud

ano, podepíše doklad pomocí podpisového padu a označí jej jako proplatitelný. Pokud ne, označí jej jako neproplatitelný a DMS zašle doklad pracovníkovi odpovědnému za řešení této situace – provozní účetní. Po schválení dokladu k proplacení předá DMS systém do ERP, že je možné provést platbu a ERP ji provede. Do DMS dojde k zaznamenání informace, kdy byla faktura proplacena.

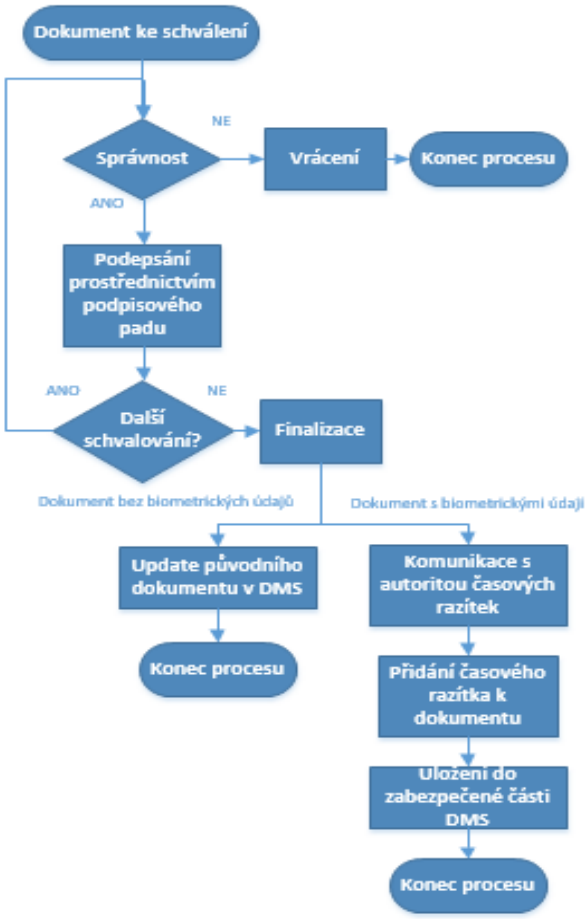
Tento proces zobrazuje následující procesní diagram.



Obr. č. 16: Upravený proces zpracování přijatého daňového dokladu

Proces schvalování – podepisování pomocí podpisového padu

Schvalovatel obdrží notifikační email se vznikem nového úkolu. V DMS systému si otevře dokument v PDF, který je potřeba schválit. Po provedení patřičných kontrol dokumentu jej schválí – biometricky podepíše. Podpis bude zachycen pomocí podpisového padu a vložen do pole pro podpisy. V případě, že dokument neschválí, vyplní důvod neschválení a pomocí funkce Vrátit jej vrátí, tím je proces ukončen, k podpisování dokladu v tomto případě nedochází. V případě, kdy je třeba dalších schvalovatelů dokument po schválení pomocí funkce Předat dál předá dalšímu schvalovateli. Po posledním podpisu následuje uložení dokumentu. Verze dokumentu s obrazem podpisu, ale bez biometrických údajů, „přeuloží" původní verzi v DMS. Při ukládání verze s biometrickými údaji dochází ke komunikaci s autoritou časových razítek (poskytovatelem služeb vytvářejících důvěru), dokument bude opatřen časovým razítkem a uložen do zabezpečeného archivu DMS. Po dokončení úkolu je odesílána notifikace zadavateli úkolu s informací o dokončení.



Obr. č. 17: Proces schvalování přijatého dokladu

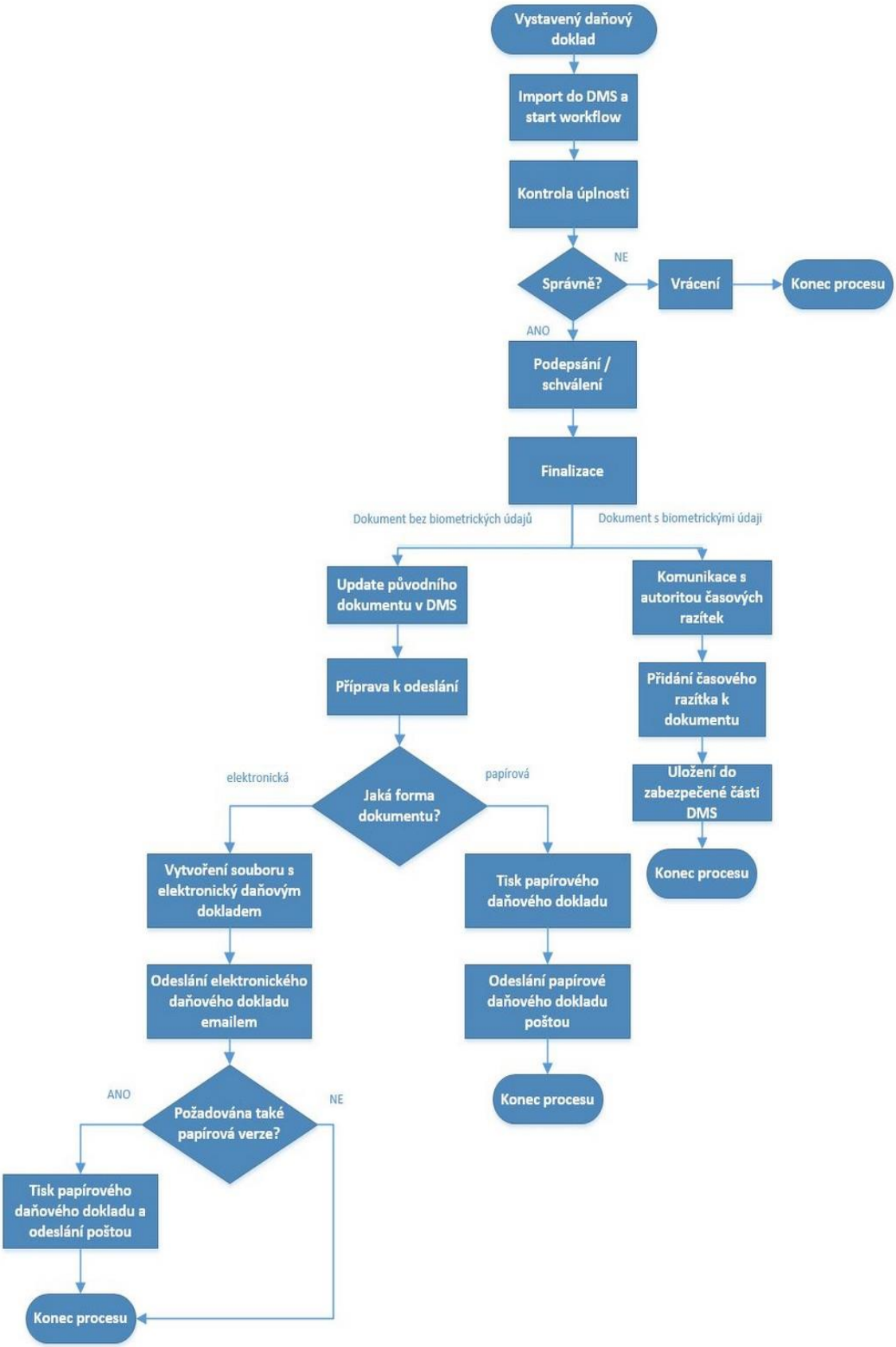
5.4.2 Proces zpracování vystaveného daňového dokladu

Vystavené daňové doklady budou nově odesílány podepsané, přičemž odesílána bude verze dokladu bez biometrických informací s obrazem dynamického podpisu. Dle zákona č. 235/2004 Sb., ve znění pozdějších předpisů nemusí odchozí elektronické doklady obsahovat elektronický podpis.

V ERP systému vzniká vystavený daňový doklad v elektronické strukturované podobě. Následuje krok importu dokladu do DMS systému a začátku workflow, doklad je tedy odeslán k podpisu zodpovědné osobě. Zodpovědná osoba obdrží emailovou notifikaci s novým úkolem podpisu. V DMS systému otevře dokument v PDF, provede kontrolu všech náležitostí daňového dokladu a proběhne-li kontrola v pořádku, dokument biometricky podepíše. V případě, že dokladu chybí povinné údaje, vrátí jej pomocí funkce Vrátit vystaviteli, tím je workflow ukončeno.

Po podepsání dokumentu dojde k jeho uložení, stejně jako v procesu schvalování přijatého dokumentu, se uloží dvě verze. První verze bez biometrických údajů obsahující obraz podpisu přeuloží původní verzi v DMS. V případě druhé verze s biometrickými údaji dochází ke komunikaci s autoritou časových razítek (poskytovatelem služeb vytvářejících důvěru), dokument je opatřen časovým razítkem a uložen v zabezpečeném archivu DMS. Verze bez biometrických údajů bude odeslána odběrateli buď elektronicky emailem, v listinné podobě poštou či předána osobně. Je-li kromě elektronické podoby požadována i listinná podoba, je doklad vytištěn a odeslán v obou podobách.

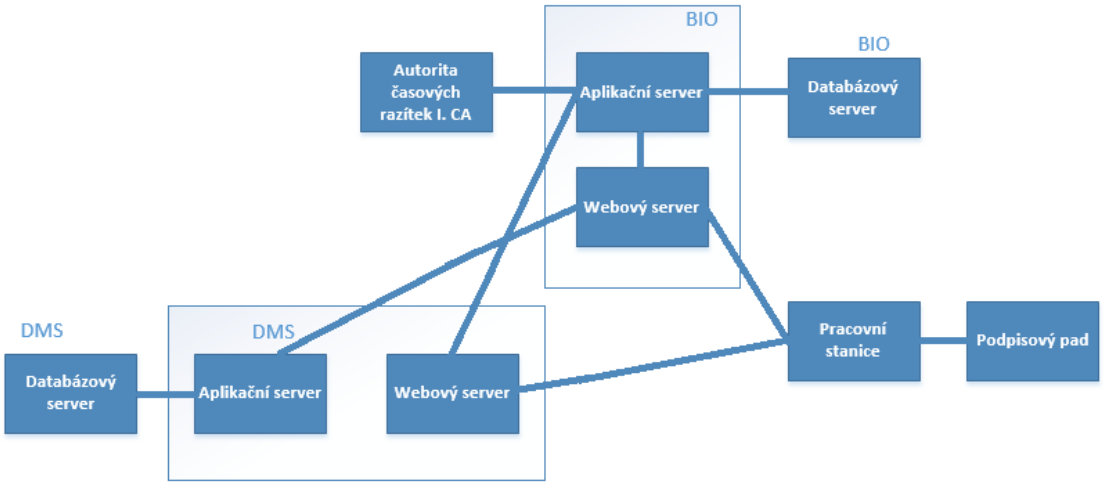
Popsaný proces přehledně popisuje následující diagram.



Obr. č. 18: Proces schvalování vystaveného dokladu

5.5 Návrh hardwarový a softwarový

Architektura navrhovaného řešení je klient-server. Podnik využívá platformy Windows, tedy i řešení bude postaveno na této platformě. Jako DMS bylo zvoleno řešení INOVIO[16], jako biometrické řešení SignoSoft client-server[17]. INOVIO představuje pokročilý DMS pro střední podniky s inteligentní možností workflow. Toto řešení zprostředkovává elektronický oběh dokumentů včetně schvalovacích procedur, zároveň je cenově dostupné pro střední podniky.



Obr. č. 19: Schéma komunikace mezi komponentami

Webové a aplikační servery budou virtuální a provozovány na stejném stroji. Databázové servery budou provozovány samostatně z důvodu lepšího výkonu a zabezpečení. Biometrický databázový server bude zaznamenávat statusové informace a logy biometrického serveru, veškeré dokumenty budou ukládány do DMS. Webové servery jsou odpovědny za přijímání požadavků od klientů (pracovních stanic), z důvodu bezpečnosti budou zprostředkovávat komunikaci s aplikačními servery, které se starají o provoz aplikací. Aplikační servery budou komunikovat s databázovými servery, přičemž biometrický aplikační server bude navíc komunikovat s autoritou časových razítek. Vzájemnou komunikaci mezi biometrickým systémem a DMS budou zajišťovat jejich webové a aplikační servery.

[16] http://inovio.cz/.
[17] http://www.signosoft.cz/biometrickepodpisy.php.

Vzhledem k požadavkům firmy na proces, průměrnému počtu zpracovaných dokladů za rok[18] a zvolenému řešení jsou požadavky na infrastrukturu následující.

Tab. č. 3: Požadavky na infrastrukturu

	DMS	**BIO**
Aplikační server		
Operační systém	Windows Server 2008 a vyšší x64	Windows Server 2008 a vyšší x64
Procesor	4 CPU	2 CPU
Paměť	8 GB RAM	6 GB RAM
Java Runtime environment / Memory	Java 9 x64 / 3096 MB	Java 9 x64 / 2048 MB
J2EE AS	Apache Tomcat 9.0.0	ApacheTomcat 9.0.0
Databázový server (DS)	Windows Server 2008 a vyšší x64, Microsoft SQL Server 2008 Standard a vyšší	Windows Server 2008 a vyšší x64, Microsoft SQL Server 2008 Standard a vyšší
Datový prostor	350 GB a více	15 GB a více
Procesor	4 CPU	2 CPU
Paměť	4 GB RAM	4 GB RAM
Webový server	Internet Information Services IIS 7.0 a vyšší	Internet Information Services IIS 7.0 a vyšší

Povolené porty

Komunikace bude probíhat přes povolené porty. Biometrický webový server, stejně tak i DMS webový server, mají otevřený port pro komunikaci s pracovní stanicí. Databázové servery mají otevřený taktéž po jednom portu pro komunikaci s aplikačními servery. Aplikační servery mají dostupné dva porty pro komunikaci s oběma webovými servery.

Podpora webových prohlížečů

Pro zobrazování PDF dokumentů z DMS je třeba mít na pracovní stanici nainstalovaný volně dostupný doplněk ve webovém prohlížeči (Google Chrome 25 nebo vyšší, Internet Explorer 10 a vyšší, Mozilla Firefox 4 nebo vyšší). Pro podepisovací aplikaci je taktéž

[18] Charakteristika modelové firmy

mít potřeba nainstalovaný doplněk v prohlížeči. Podporované jsou stejné prohlížeče, tedy je dostačující mít nainstalovaný jeden webový prohlížeč.

Podpisový pad

Podpis bude zachycován pomocí podpisových padů. Byly vybrány podpisové pady značky **Wacom STU-430**. Jedná se o plně vybavený podepisovací tablet v tenkém designu, je vybaven plochým povrchem pro snadnější podepisování. Je vysoce odolný proti škrábancům. Napájení je pomocí USB portu. Specifikace je uvedena v následující tabulce.

Tab. č. 4: Specifikace Wacom STU-430

Parametr	Hodnota
Tloušťka / výška / šířka	10,85 mm / 174,37 mm / 161,43 mm
Rozlišení displeje	320 x 200 pixelů
Povrch displeje	Tvrzené sklo, ochrana proti poškrábání a anti reflexní úprava
Aktivní plocha podpisu	95,98 mm x 59,98 mm
Úrovně tlaku	1 024
Rozlišení snímání	2,540 lpi
Technologie pera	Bezdrátové bezbateriové pero
Cena za 1 ks vč. DPH	5 900 Kč

Obr. č. 20: Wacom STU-430 (Převzato z: [13])

Podepisovací technologie

Jako software pro biometrický podpis je zvoleno řešení **SignoSoft Client/Server**. Jedná se o komplexní serverové podepisovací řešení, umožňuje možnost komplexní správy

systému a integraci do stávající infrastruktury. Řešení umožňuje napojení různých typů biometrických aplikací pro různé kanály, typy dokumentů či obchodní systémy. Umožňuje vložit do PDF dokumentu podpis zaznamenaný pomocí podpisového padu a tím vznikne vlastnoručně podepsaný a zabezpečený dokument. Proces je postaven na čtyřech základních krocích, a to příprava PDF dokumentu, vlastnoruční podepsání, uložení podpisu včetně uzamčení a následné sdílení dokumentu. Podrobnější popis podepisování a následného uložení podepsaného dokumentu je uveden v kapitolách výše.

Tab. č. 5: Cena řešení SignoSoft

Položka	**Celková cena za položku vč. DPH**
Licence SignoSoft 1ks	3 662 Kč
SignoSoft – konfigurace, integrace, implementace	173 000 Kč

Znalecké zkoumání řešení SignoSoft

Dle W. J. Flynna, jehož článek zabývající se znaleckým zkoumáním pravostí vlastnoručních podpisů byl publikován v odborném časopise Journal of American Society of Questioned Document Examiners, musí mít přednost zkoumání surových dat podpisu před jinými variantami. Z těchto surových dat lze získat nejen vizuální podpis s tvarovými charakteristikami, ale taktéž i data o dynamice a posloupnosti tahů či tempu psaní. Mgr. Jan Zimmer, znalec z oboru písmoznalectví, se zaměřil na ověření těchto Flynnových poznatků. Při experimentech pracoval s řešením SignoSoft a dospěl k výsledku, že lze získat pomocí tohoto řešení dostatečné a spolehlivé informace o tlaku na podepisovací pero, tempu psaní i tvarech podpisu. Díky těmto informacím je tedy znalecky možné zkoumat pravost podpisu. [15, s. 1-3] Jak již bylo uvedeno v kapitole Popis ochrany před paděláním DBP, je nutné poukázat na to, že znalecké řešení je nutné jen ve výjimečných případech, kdy pouze potvrdí vyhodnocení řešené podpisovou aplikací.

DMS

Elektronický oběh dokumentů bude zabezpečen pomocí pokročilého **DMS INOVIO**. Uložené doklady jsou mimo veřejné cloudy, jsou pod úplnou kontrolou firmy. Umožňuje nastavení oprávnění přístupu uživatelům. Nechybí podpora workflow pro elektronické schvalování faktur, přičemž toto workflow bude upraveno pro požadavky firmy. Do DMS

budou ukládány mimo jiné podepsané dokumenty. Dokument s biometrickými informacemi bude uložen do zabezpečené části DMS, kopie bez biometrických informací, pouze s obrazem podpisu, bude uložena v běžné dostupné části DMS.

Tab. č. 6: Cena řešení Inovio

Položka	Celková cena za položku vč. DPH
Licence Inovio 1 ks	5 896 Kč
Inovio – konfigurace, integrace, implementace	281 000 Kč

5.6 Návrh bezpečnostní a oprávnění přístupu

Bezpečnost je řešena na úrovní systémové – způsob ukládání a zabezpečení dat, komunikace mezi jednotlivými systémy, a aplikační – přístupy a oprávnění k aplikaci.

5.6.1 Systémové zabezpečení

Aplikace bude dostupná pouze pro oprávněné naimportované uživatele. Přihlášení uživatelů do aplikace bude umožněno pomocí uživatelského jména a hesla na úrovni DMS. Autentizovaným uživatelům budou přidělena oprávnění dle jejich role. Žádný z uživatelů nebude mít oprávnění provádět změny v kořenových složkách aplikace. Veškeré aktivity uživatelů budou sledovány a zaznamenány v logu tak, aby bylo možné zjistit, kdy a kým byla změna provedena. Tyto logy budou dostupné po dobu půl roku pro oprávněné uživatele, kteří je mohou kontrolovat, poté budou archivovány v DMS pro případnou nutnou kontrolu v budoucnosti.

Pro zachování integrity bude vytvoření tzv. snapshotu (snímku) aplikace a jeho aktualizace při každé schválené změně či aktualizace aplikace. Soubory aplikací budou chráněny před neoprávněnými změnami přicházejícími od jiných procesů. Při každém spuštění bude aplikace porovnávána s vytvořeným snapshotem a v případě odlišností, dojde k zastavení spouštění aplikace a k upozornění Správce systému na porušení integrity aplikace, který bude odpovědný za vyřešení tohoto incidentu.

Komunikační toky jsou z důvodu ochrany před zneužitím šifrované. Výjimku tvoří komunikace mezi aplikačním serverem, na kterém běží aplikace biometrického serveru,

s databázovým serverem, který zaznamenává pouze statusové informace biometrického serveru, jako například potvrzující a informační zprávy či chybová hlášení.

Biometrická data zachycena pomocí podpisového padu jsou hned v tomto v zařízení (podpisovém padu Wacom STU-430) šifrována, tedy odchází na biometrický server v šifrované podobě. Na biometrický server jsou doručena pomocí HTTPS – hypertextového přenosového protokolu, kdy jsou přenášená data kódována protokolem TLS poskytujícím možnost zabezpečené komunikace. Na biometrickém serveru jsou data šifrována pomocí algoritmu RSA-3072. Data v této podobě jsou vložena do PDF dokladu a dojde k podepsání certifikátem společnosti. Po posledním schválení – podpisu dochází ke komunikaci biometrického serveru s certifikační autoritou a do dokumentu je vloženo časové razítko. Dokument je poté uložen do zabezpečené části DMS.

Uložení dokumentů

Dokumenty budou ukládány do DMS. V průběhu zpracování je dokument uložen v tzv. pracovní verzi v pracovním úložišti DMS. Do této části nebude umožněn přístup žádnému uživateli. Po posledním podpisu, schválení, bude dokument obsahující biometrická data uložen v zabezpečené části DMS. Jeho verze bez biometrických dat bude uložena v přístupné části DMS, do této části již budou mít uživatelé přístup. Z pracovního úložiště budou pracovní verze odstraněny. Verze bez biometrických dat je dostupná k běžnému užívání. Verze s biometrickými daty bude archivována.

Uložení biometricky podepsaných dokladů

Doklady obsahující biometrické informace budou ukládány v zabezpečené části DMS se speciálním přístupem, na rozdíl do těch dokladů, které obsahují pouze obraz biometrického podpisu bez biometrických informací. Ty budou ukládány taktéž v DMS ale v části, do které lze přistupovat, a budou dostupné uživatelům pro čtení.

Verze dokladů s biometrickými informacemi budou opatřeny časových razítkem, pomocí kterého lze dokázat existenci dokumentu v archivu. Budou uloženy do zvláštních složek, do kterých bude umožněn přístup pouze správci biometrických dokladů a vlastníkovi dokumentu, tedy tomu, kdo jej podepsal. Pro všechny ostatní zaměstnance

bude tato část DMS neviditelná. Správce biometrické části a vlastník budou mít odlišné oprávnění. Správce bude moci vyhledávat, zatímco vlastníkovi bude umožněno si jím podepsané doklady stáhnout na vybrané úložiště. Žádný uživatel nebude mít oprávnění doklady mazat, změnit jeho atributy či obsah.

Zálohování dat

Zálohování dat bude probíhat na dvě záložní paměťová média pravidelně dle zálohovacího kalendáře. K zálohám bude využíván specializovaný software Acronis True Image[19], který umožňuje zálohování do několika umístění najednou pro silnější ochranu. Úplné, tzv. full-image zálohy budou probíhat na týdenní bázi, vždy v sobotu v 11 hodin. Replika celého disku umožňuje rychlou obnovu. Složky DMS obsahující biometricky podepsané dokumenty budou zálohovány 2 krát denně v 11 a v 20 hodin pomocí rozdílové metody. Administrátoři budou emailem informováni o aktuální statusu zálohování včetně informace o úspěšnosti či neúspěšnosti záloh. Taktéž bude zpracovaný tzv. disaster recovery, tedy plán obnovy po havárii, který bude poskytovat odpovědi na otázky, jak obnovit data a systémy v případě incidentu, kdo jej provede, jak dlouho trvat apod.

5.6.2 Aplikační zabezpečení

Import organizační struktury

Import uživatelů bude probíhat denně automaticky z ERP systému firmy pomocí LDAP. Při tomto importu budou uživatelé přiděleni do tzv. skupiny, kdy v LDAP budou tyto skupiny vytvořeny, pro případ, kdy by nebylo schvalování směřované pouze na konkrétního uživatele ale na více uživatelů na stejné pozici. Příklady těchto skupiny jsou – asistenti, manažeři, účetní, podrobněji níže. U uživatelů bude uvedena úroveň oprávnění k aplikaci. Oprávnění k aplikaci bude rozděleno do tří skupiny. Tato oprávnění jsou definována níže.

Skupiny uživatelů a jejich oprávnění

Uživatelé jsou dle jejich pracovní činnost rozděleni do skupin. Tyto skupiny budou jak globální – GL (tedy pro celý podnik, například skupina Asistenti GL zahrnuje všechny asistenty v podniku), tak i lokální (například skupina Asistenti VRZ zahrnuje všechny

[19] https://www.acronis.cz/produkt/true-image-2017/

asistenty z oddělení výroby a realizace zakázek). Toto rozdělení zachycuje následující tabulka.

Tab. č. 7: Rozdělení uživatelů do skupin

Typ	Popis
Ředitel	Ředitel společnosti, který má na starost chod celého podniku.
Manažer - **Globální** - **Lokální**	Manažeři jednotlivých oddělení – personální, finanční, CIO, obchodní, výroby a realizace
Asistent - **Globální** - **Lokální**	Asistenti jednotlivých oddělení
Vedoucí týmu - **Globální** - **Lokální**	Vedoucí, kteří jsou součástí týmu IT, obchodních či výrobních realizačních.
Provozní účetní	Tzv. vedoucí účetních, která má na starost například vracení daňových dokladů dodavateli, distribuuje doklady na správné schvalovatele či řeší situace s neproplatitelnými doklady.
Účetní referenti	Účetní odpovědné veškeré zaúčtování, vedení účetních knih či odpisových plánů.

Všichni uživatelé, kteří jsou členy výše uvedených skupin, mají oprávnění přístupu do podpisové aplikace a vlastní podpisový pad.

Rozsah oprávnění pro uživatele do podepisovací aplikace je rozdělen na několik úrovní – běžný, vedoucí či úplný. Dostupné oprávnění zachycuje následující tabulka. Přičemž vyšší úroveň oprávnění zahrnuje oprávnění z nižší úrovně a je doplněné o další oprávnění navíc.

Tab. č. 8: Typy oprávnění

Oprávnění	Popis oprávnění
Běžný (výkonný zaměstnanec)	- přístup do podpisové aplikace - dostupný seznam dokladů ke schválení včetně detailu ke zpracování - proces schvalování (workflow)

	- dostupný přehled svých dokončených workflow - notifikace distribuovaného schvalování, blíží se konce lhůty pro schválení
Vedoucí	- stejná práva jako Běžný - právo na založení nového schvalovacího workflow - možnost předčasně ukončit workflow, která založil - dostupný seznam workflow, která založil - notifikace týkající se ním založených workflow – informace o schválení, neschválení - možnost distribuování workflow, které založil, na jiné schvalovatele
Úplný (finanční manažer, příp. ředitel podniku)	- stejná práva jako Vedoucí - přehled všech workflow - možnost předčasně ukončit všechna workflow - možnost distribuování všech workflow na jiné schvalovatele

Administrace systému

Administrace systému je rozložena mezi dva uživatele – správce biometrické části a správce systému.

Tab. č. 9: Administrace

Typ	**Popis oprávnění**
Správce biometrické části	Uživatel s oprávněním přístupu k dokladům s biometrickými informacemi.
Správce systému	Správce celého DMS a biometrického systému. Na rozdíl do správce biometrické části nemá přístup do zabezpečené části DMS k dokladům s biometricky podepsaným dokladům.

Notifikace

Během procesu schvalovacího workflow jsou odesílány patřičným uživatelům notifikace. Tyto notifikace jsou automaticky odesílány na pracovní email v případě:

- vzniku nového úkolu a jeho distribuování ke schválení
- jeho vyřízení včetně výsledku schválení či neschválení
- vrácení při nesprávném přidělení

- ukončení celého schvalovacího procesu
- blížícího se konce lhůty pro schválení.

5.7 Porovnání papírového a elektronického řešení z finančního hlediska

Rozdíl v nákladech mezi zpracováním dokladů v papírové a elektronické verzi zachycuje následující tabulka. V nákladech na jeden doklad jsou zahrnuty veškeré související náklady s jeho zpracováním od vzniku po archivování.

Tab. č. 10: Porovnání papírového a elektronického řešení vč. DPH

	Papírové řešení	**Elektronické řešení**
Počet zpracovaných dokladů za 1 rok	5 240 ks	5 240 ks
Náklad na 1 doklad	69 Kč	8,28 Kč
Celkové náklady za 1 rok	361 560 Kč	43 387 Kč

Celkové náklady jsou určeny jako součin počtu zpracovaných dokladů za jeden rok a nákladu na jeden doklad. Z tabulky vyplývá, že elektronické řešení přináší pokles celkových nákladů spojených se zpracováním dokladů na přibližně 12 % původních ročních nákladů. Konkrétně úspora v tomto počtu zpracovaných dokladů za období jednoho roku je 318 173 Kč vč. DPH. Úspora na jeden doklad je 60,72 Kč vč. DPH.

Přibližné náklady na řešení jsou obsahem následující tabulky.

Tab. č. 11: Náklady řešení vč. DPH

Položka	**Celková cena za položku**
Podpisové pady	147 500 Kč
Licence Inovio	147 400 Kč
Licence SignoSoft	91 560 Kč
Inovio – konfigurace, integrace, implementace	281 000 Kč
SignoSoft – konfigurace, integrace, implementace	173 000 Kč
Školení uživatelů	30 000 Kč
Servisní program, Acronis True Image	183 600 Kč
Celkové náklady	1 054 060 Kč

Návratnost investice v čase při plánovaném objemu zpracovaných dokladů zahrnuje následující tabulka v Kč. Roční úspora je vyjádřena jako součin úspory na jeden zpracovaný doklad a počtu dokladů. Denní úspora představuje roční dělenou 365. Návratnost vyjadřuje, za jakou dobu by mělo dojít ke splacení počáteční investice při daném počtu zpracovaných dokladů. Je vypočítána jako podíl roční počáteční investice a ročního výnosu.

Tab. č. 12: Návratnost investice řešení v Kč

			Úspora		**Návratnost**	
Odhad zvýšení počtu zpracovaných dokladů	**Úspora na 1 doklad**	**Počet dokladů**	**Roční**	**Denní**	**Rok**	**Den**
Současný stav	60,72	5 240	318 172,8	871,7	3,31	1 209
Δ o 3 %	60,72	5 397	327 718,0	897,9	3,22	1 174
Δ o 6 %	60,72	5 554	337 263,2	924,0	3,13	1 141
Δ o 9 %	60,72	5 712	346 808,4	950,2	3,04	1 109
Δ o 12 %	60,72	5 869	356 353,5	976,3	2,96	1 080

Z tabulky vyplývá, že pokud podnik zpracuje podobný počet dokumentů, jako je stanovený průměr, bude návratnost investice cca 3,31 let. Pokud bude podnik ročně zpracovávat více dokladů, doba návratnosti investice se bude zkracovat.

5.8 Porovnání DBP a vlastnoručního podpisu z hlediska bezpečnostních aspektů

Jak již bylo uvedeno, při podepisování elektronického dokumentu dynamickým biometrických podpisem se podepisující osoba se podepíše na podpisový pad, který snímá nejen tvar podpisu, ale i dynamické parametry, jako je tlak, sklon, zrychlení apod. Nasnímaný podpis je v podpisovém padu zašifrován a veškerá komunikace mezi pracovní stanicí a serverem probíhá pomocí zabezpečených komunikačních protokolů. Tyto dynamické parametry jsou zašifrovány a přidány k digitálnímu dokumentu (podrobněji kapitola Popis podepsání dokumentu a označení časovým razítkem). Rozšifrování těchto dat je možné pouze za použití privátního klíče, který je uložen u důvěryhodné třetí strany, typicky u certifikační autority (podle Nařízení poskytovatele služeb vytvářejících

důvěru). Certifikační autorita má přísné kontrolní předpisy a procesy pro úschovu či případné vydání tohoto klíče. K rozšifrování biometrických dat může dojít na základě rozhodnutí soudu nebo správního orgánu a za přítomnosti písmoznalce a kryptografa, kteří na proces dešifrování dohlíží.

Klasický vlastnoruční podpis je v porovnání s dynamickým biometrických podpisem méně bezpečný. V případě klasického podpisu je možné porovnávat s podpisovým vzorem pouze jeho grafickou podobu. Obrázek podpisu může být, jak se v mnoha případech také stalo, zručným padělatelem napodoben nebo připojen z jiného dokumentu. V případě dynamického biometrického podpisu je možné porovnávat i biometrické charakteristiky, přičemž napodobení těchto charakteristik podpisu je prakticky nemožné. Biometricky podepsaný dokument je uložen v zabezpečené části DMS, do kterého není umožněn přístup osobám bez potřebného důvodu a povolení. Podpis je tedy v tomto případě významně bezpečnější než jeho běžná podoba na papíře, neboť v dnešní době se mnoho podepsaných listinných dokumentů skenuje a objevuje na internetových stránkách.

Vzhledem k výše uvedeným skutečnostem lze konstatovat, že dynamický biometrický podpis je výrazně bezpečnější než vlastnoruční podpis na papíru. Dalo by se diskutovat i o tom, že je bezpečnější nežli podpis kryptografický, a to proto, že údaje pro vytvoření podpisu nemůže u DBP podepisující osoba nikomu předat, zatímco u kryptografického ano (token či přístup k úložišti lze zpřístupnit jiné osobě nebo se jej osoba může protiprávně zmocnit).

6 ZÁVĚR

Tato práce byla věnována problematice biometrického podepisování elektronických daňových dokladů. Toto řešení přinese podniku nejen zrychlení procesu schvalování a větší kontrolu nad ním, ale taktéž i úsporu nákladů na zpracování a archivaci.

Cílem této diplomové práce bylo vytvoření metodiky pro implementaci dynamického biometrického podpisu v podniku po nabytí účinnosti nařízení eIDAS, s přihlédnutím k dalším právním předpisům a technickým normám. Dílčími cíli bylo shrnout platnou legislativu týkající se elektronického podpisování v České republice a taktéž porovnat kryptografický elektronický podpis s dynamickým biometrickým podpisem z hlediska technologického a bezpečnostního. Tyto stanovené cíle se podařilo splnit. Konkrétní řešení bylo navrženo pro zpracování daňových dokladů v podniku, ale pokud vstupní analýza ukáže, že po stránce obsahové a organizační lze i další druhy dokladů zpracovat elektronicky, je toto řešení aplikovatelné obecně.

Teoretická část diplomové práce přibližuje současnou legislativu této problematiky, především nařízení eIDAS, jím definované cíle a pojmy, a tzv. adaptační zákony č. 297/2017 Sb. a č. 298/2017 Sb. Nechybí rozbor vybraných pojmů z nařízení eIDAS, jako například kvalifikované služby vytvářející důvěry, elektronický podpis či elektronická časová razítka. Poslední část teorie je věnována porovnání kryptografického elektronického podpisu s dynamickým biometrickým podpisem.

V části analýza současného stavu podniku je ve zkratce charakterizován model podniku, ve kterém byl v návrhové části implementován dynamický biometrický podpis. Je zde popsán původní papírový proces zpracování a schvalování daňových dokladů. Z analýzy vyplývá, že papírové řešení přináší vyšší náklady na tisk i na čas potřebný pro vyřízení spojený s fyzickou distribucí dokumentů.

Část návrh řešení se zabývá již konkrétním návrhem daného problému. Funkční návrh je rozdělen na několik části, ve kterých je navrhované řešení popsáno z několika hledisek, a to jak funkčního, procesního, hardwarového a softwarového, či hlediska bezpečnostního. Závěr kapitoly obsahuje finanční porovnání původního papírového

řešení s novým elektronickým řešením. Je zjištěno, že díky novému řešení dojde v modelovém podniku ročně k úsporám cca 318 000 Kč, přičemž předpokládaná návratnost investice se pohybuje kolem 3,3 let. Také bezpečnost tohoto řešení je na vyšší úrovni, nežli u klasického zpracování na papíru.

Tak, jak bylo řešení navrženo, splňuje následující požadavky:

1. vyhovuje požadavkům podnikové praxe,
2. je v souladu se zákony upravujícími nakládání s daňovými doklady,
3. je bezpečné, protože DBP není možné padělat, ani oddělit od podepsaného dokumentu,
4. odpovídá požadavkům podle Nařízení eIDAS a adaptačních zákonů č. 297/2016 Sb. a č. 298/2016 Sb.,
5. je ekonomicky přínosné a racionální.

Pokud bylo cílem této diplomové práce vytvoření obecně použitelné metodiky pro implementaci dynamického biometrického podpisu v podniku po nabytí účinnosti nařízení eIDAS, pak s využitím příkladu nasazení DBP pro agendu vyřizování přijatých daňových dokladů – faktur toto bylo splněno. Obdobným způsobem lze jakoukoliv další agendu spočívající ve zpracování dokumentů v podniku převést na zpracování digitálních dokumentů podepsaných dynamickým biometrickým podpisem.

SEZNAM POUŽITÉ LITERATURY

[1] DAWSON, M., D. R. KISKU, P. GUPTA, J. K. SING a W. LI. *Developing next-generation countermeasures for homeland security threat prevention*. Hershey PA: IGI Global, 2017. 428 s. ISBN 978-1522-50-7031.

[2] MATES, P. a V. SMEJKAL. *E-government v České republice: Právní a technologické aspekty*. 2. vyd. Praha: Leges, 2012. 464 s. ISBN 978-80-87576-36-6.

[3] SMEJKAL, V., KODL, J. a M. UŘIČAŘ. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie,* VI., 2015. č. 11, s. 189-235. ISSN 1805-2797.

[4] SMEJKAL V. a K. RAIS. *Řízení rizik ve firmách a jiných organizacích.* 4. vyd. Praha: Grada, 2013. 488 s. ISBN 978-80-247-4644-9.

[5] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

[6] MAISNER, M. a J. BÁTRLA. EIDAS a praktické důsledky v praxi. *Data security management*, XX., 2016. č. 3, s. 8-11. ISSN 1211-8737.

[7] Zákon č. 298/2016 Sb., zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

[8] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

[9] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *eIDAS, elektronický podpis*. Mvcr.cz [online]. © 2017 [cit. 2017-03-02]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx.

[10] Prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru.

[11] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

[12] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Prohlášení NBÚ k využívání hashovacích funkcí*. Nbu.cz [online]. [cit. 2017-04-25]. Dostupné z: https://www.nbu.cz/cs/aktualne/prohlaseni-a-tiskove-zpravy/776-4150-prohlaseni-nbu-k-vyuzivani-hashovacich-funkci/.

[13] WACOM. STU-430. Wacom.cz [online]. © 2016-2017. Dostupné z: http://www.wacom.com/en-us/enterprise/business-solutions/hardware/signature-pads/stu-430

[14] Smejkal, V., Kodl J. and J. Kodl Jr. Implementing Trustworthy Dynamic Biometric Signature according to the Electronic Signature Regulations. Proceedings of 47th Annual 2010 IEEE International Carnahan Conference on Security Technology (ICCST), 9-11 October 2013, Medellín, Colombia, pp. 165–170. ISBN: 978-958-8790-65-7.

[15] ZIMMER JAN. *Zkoumání pravosti vlastnoručních biometrických podpisů se zaměřením na řešení SignoSoft*. Stará Boleslav: 2013. 3 s.

[16] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.

[17] Standard ITU-T X.509. Information technology – Open Systems Interconnection - The Directory: Publickey and attribute certificate frameworks.

[18] Standard ITU-T X.500. Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.

[19] RAK, R. a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada Publishing, a.s., 2008, s. 415 a násl. ISBN 978-80-247-2365-5.

[20] Důvodová zpráva k návrhu zákona č. 297/2016 Sb. Sněmovní tisk č. 763/0, volební období 2013-2017.

SEZNAM TABULEK

SEZNAM OBRÁZKŮ