Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Možnosti implementace elektronického podpisu při víceúrovňové komunikaci v informačním systému

Bakalářská práce

Jakub Řeřicha

Školitel: RNDr. Libor Dostálek

České Budějovice 2017

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Jakub Řeřicha

Obor – zaměření studia: Aplikovaná informatika – specializace Elektronické bankovnictví

Katedra/ústav, kde bude práce vypracovávána: Ústav aplikované informatiky

Školitel/ Garant z PřF: RNDr. Libor Dostálek

Vedoucí práce: Miroslav Plecer, GLOBIS s.r.o.,
Husova 5 České Budějovice 370 01
e-mail: miroslav.plecer@globis.cz

Téma bakalářské práce: Možnosti implementace elektronického podpisu při víceúrovňové komunikaci v informačním systému

Cíle práce:

1. Zmapovat existující prostředky firmy pro prokázání původu dokumentů (jako např. čtečky čipových karet, čtečky otisků prstů, tablet s dotykovým perem či biometrickými senzory).
2. Zmapovat potřeby (ekonomické, právní, organizační) elektronického podpisu při komunikaci:
    a. Mezi zaměstnanci
    b. Mezi firmou a externisty
    c. Mezi firmami (např. při podpisu smlouvy)
    d. Mezi firmou a státní správou
3. Zmapovat způsoby elektronického podpisu:
    a. vlastnoruční podpis, biometrický podpis,
    b. otisk prstů,
    c. elektronický podpis, zaručený elektronický podpis,
    d. podpis pomocí tlačítka
4. Navrhnout nejvhodnější řešení implementace elektronického podpisu pro potřeby informačního systému.
5. Řešení musí být v souladu s Obecným nařízením o ochraně osobních údajů (GDPR).
6. Proof-of-concept navrhovaného řešení.

Základní doporučená literatura:

DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

VONDRUŠKA, Pavel, et al. Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů. Olomouc: ANAG, 2002. ISBN 80-7263-125-X

PETERKA, Jiří. *Báječný svět elektronického podpisu.* vyd. 1. Praha : CZ.NIC. 430 s. ISBN 978-80-904248-3-8.

Financování práce: .....

Vedoucí práce: .....podpis: .....

U externích vedoucích fakultní garant práce: .....podpis: .....

Garant oboru bak. studia, pokud je obor zajišťován jinou katedrou/ústavem, než ze které je školitel (nepožaduje se u oboru biologie): .....podpis: .....

Vedoucí katedry/ústavu, kde bude práce vypracovávána: .....podpis:.....

Případný souhlas vedoucího ústavu AV: .....podpis:.....

V Českých Budějovicích dne 25.11.2016 .....Podpis studenta: Říčka

Bibliografické údaje

Řeřicha, J., 2017: Možnosti implementace elektronického podpisu při víceúrovňové komunikaci v informačním systému. [Possibilities of Implementation of Electronic Signature in Multi-level Communication in an Information System. Bc. Thesis, in Czech.] – 73 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se zabývá využitím elektronického podpisu při podepisování elektronických dokumentů ve firemní praxi. V teoretické části je představena problematika elektronického podpisu ve světle nově vydané legislativy EU a ČR, přiblíženy současné technické možnosti a popsány jednotlivé druhy elektronického podpisu.

V analytické části práce byl zpracován přehled všech posuzovaných variant elektronického podpisu s výčtem hlavních výhod a nevýhod a byla posouzena jejich vhodnost pro úrovně komunikace dané informačním systémem firmy. Dále se práce věnuje mapování aktuálních prostředků a potřeb elektronického podpisu při zpracování dokumentů v elektronické podobě v prostředí informačního systému firmy. V práci je dále navrženo řešení pro aktuální potřeby firmy a toto řešení je předvedeno v podobě proof-of-concept.

Klíčová slova: Elektronický podpis, certifikát pro elektronický podpis, eIDAS, poskytovatel služeb vytvářejících důvěru, proof-of-concept, USB token, digitální podpis, grafický tablet.

Annotation

This bachelor thesis deals with the use of the electronic signature for signing electronic documents in corporate practice. The theoretical part of the bachelor thesis introduces the problematics of electronic signature from the point of view of the new legislation of the European Union and the Czech Republic, outlines current technical possibilities and describes individual types of electronic signature.

In the analytical part of the thesis, an overview of all evaluated means of the electronic signature was prepared, listing main advantages and disadvantages and their suitability for the communication levels given by the company information system. In addition, the thesis is focused on the mapping of current means and needs of electronic signature in the processing of documents in electronic form in the company information system environment. Further in the thesis a solution for identified needs of the company is also designed and this solution is demonstrated in the form of proof-of-concept.

Key words: Electronic signature, certificate for electronic signature, eIDAS, trust service provider, proof-of-concept, USB token, digital signature, graphic tablet.

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, 5. prosince 2017

Podpis studenta: ……

Jakub Řeřicha

Elektronický podpis: Jakub Řeřicha Digitálně podepsal Jakub Řeřicha
Datum: 2017.12.05 08:24:08 +01'00'

Poděkování

Děkuji RNDr. Liboru Dostálkovi za odborné vedení a cenné rady při zpracování této práce, velice si cením jeho vstřícného přístupu a času, který věnoval zodpovězení mých otázek. Velký dík patří také panu Miroslavu Plecerovi ze společnosti GLOBIS s.r.o., Ing. Emilu Zelendovi za podnětné připomínky a důvěru při zpracování praktické části práce v Chemické obchodní společnosti s.r.o. Dále děkuji svým blízkým za podporu během studia a při zpracování bakalářské práce.

OBSAH

1 ÚVOD

V oblasti informačních systémů přirozeným vývojem vzniká potřeba používat elektronickou dokumentaci místo papírové dokumentace. Jedná se např. o elektronické faktury, úřední oznámení a výzvy přes datové schránky, elektronické servisní reporty v běžném obchodním styku apod. Tato potřeba často vzniká v rámci optimalizace vnitropodnikových procesů. Aby mohla být digitální dokumentace v podnikovém informačním systému použita, musí mít lidé k elektronickým dokumentům alespoň takovou důvěru jako k papírovým.

Je třeba mít na paměti, že podpis dokumentů je právní akt, který je úzce spjatý s legislativou. V oblasti rychle se rozvíjející elektronické komunikace jsou i legislativní procesy neustále přizpůsobovány potřebám praxe, s ohledem na pokrok v používaných technologiích. Konkrétní nedávnou změnou je nabytí účinnosti Nařízení Evropské unie č. 910/2014, tzv. Nařízení eIDAS (1), které upravuje pravidla pro uznávání elektronických podpisů v rámci Evropské unie. V návaznosti na účinnost Nařízení eIDAS (1) ukončila České republika, ke dni 19. 9. 2016, platnost zákona č. 227/2000 Sb., o elektronickém podpisu (2), a nahradila ho zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (3), přičemž nový zákon ustanovuje pravidla pro přechodné období 2 let, tj. do 19. 9. 2018.

V souladu s novým Nařízením eIDAS (1) se tato bakalářská práce mimo jiné věnuje:

- Zmapování dostupných způsobů elektronického podpisu.
- Zmapování prostředků pro vytváření elektronického podpisu.
- Posouzení variant elektronického podpisu pro různé druhy komunikace v informačním systému (dále také jen IS).
- Zmapování potřeb použití elektronického podpisu při komunikaci na různých úrovních v rámci vnitřního informačního systému firmy Chemická obchodní společnost s.r.o. (dále také jen CHOS).

Cílem práce je zmapování současného stavu a návrh nejvhodnějšího řešení implementace elektronického podpisu pro potřeby CHOS ve vnitřním informačním systému, jehož autorem a poskytovatelem je firma GLOBIS s.r.o. (dále také jen Globis). V závěru práce je proveden proof-of-concept vybraného návrhu řešení.

1.1 Cíle práce

1. V teoretické části představit způsoby elektronického podpisu:
    1.1 prostý elektronický podpis;
    1.2 elektronický podpis, zaručený elektronický podpis;
    1.3 biometrický podpis;
    1.4 podpis pomocí tlačítka;
    1.5 otisk prstů.
2. Posoudit varianty elektronického podpisu pro různé druhy komunikace v IS.
3. Zmapovat existující prostředky firmy pro prokázání původu dokumentů (jako např. čtečky čipových karet, čtečky otisků prstů, tablet s dotykovým perem či biometrickými senzory).
4. Zmapovat potřeby (ekonomické, právní, organizační) elektronického podpisu při komunikaci:
    4.1 mezi zaměstnanci;
    4.2 mezi firmami při servisní činnosti;
    4.3 mezi firmami při podpisu smlouvy;
    4.4 mezi firmou a státní správou.
5. Navrhnout nejvhodnější řešení implementace elektronického podpisu pro potřeby informačního systému.
6. Řešení musí být v souladu s Obecným nařízením o ochraně osobních údajů (GDPR).
7. Proof-of-concept navrhovaného řešení.
8. Závěr.

1.2 Metodika práce

Bakalářská práce je obsahově rozdělena do dvou hlavních částí, teoretické a analytické. Asi nejvýstižnějším termínem, který jsem zvolil pro zpracování teoretické části, je rešerše. S využitím znalostí získaných během studia na JU, z dostupné literatury a legislativy jsou zde popsány základní principy elektronického podpisu, vysvětleny důležité pojmy problematiky a sestaven přehled jednotlivých druhů elektronického podpisu, jak jsou definovány současnými platnými zákony Evropské unie a České republiky a technickými prostředky k jejich vytvoření.

Analytická část práce začíná výčtem jednotlivých posuzovaných způsobů elektronického podepisování a porovnáním jejich hlavních výhod a nevýhod. Dále je zhodnocena vhodnost jednotlivých druhů elektronického podpisu ve vztahu k různým úrovním komunikace v rámci informačního systému.

Obecné závěry jsou ověřeny na konkrétním případu z praxe, v informačním systému CHOS, poskytovaném firmou Globis. Jsou zmapovány potřeby využití elektronického podpisu v běžném obchodním styku a ve firemní komunikaci CHOS. Během osobních návštěv a rozhovorů se členy vedení společnosti je rozkryta aktuální situace a zmapovány existující prostředky firmy pro prokázání původu zpracovávaných dokumentů. S využitím informací z teoretické části jsou způsoby elektronického podpisu následně porovnány a konzultovány se zástupci CHOS a Globis.

Na základě všech takto získaných poznatků je navrženo nejvhodnější řešení implementace elektronického podpisu. K ověření funkčnosti navrhovaného řešení je v závěru analytické části sestaven proof-of-concept.

2 STAV POZNATKŮ O ŘEŠENÉ PROBLEMATICE (TEORETICKÁ VÝCHODISKA)

2.1 Podpis dokumentu

2.1.1 Vlastnoruční podpis

Písemný dokument v listinné podobě je možné – obvykle i nutné – vybavit podpisem. Zpravidla k tomu stačí vlastnoruční podpis, popř. ověřený vlastnoruční podpis (např. notářsky). Vlastnoruční podpis lze podrobit zkoumání grafologa, který by se zajímal o jednotlivé charakteristiky podpisu, např. styl tahu perem, sklon a tvar jednotlivých znaků a také jaký papír či inkoust byl použit. Srovnáním těchto vlastností podpisu s jeho známým podpisovým vzorem je možné zjistit pravost podpisu. (4, s. 27-29)

2.1.2 Elektronický dokument

Pro práci s písemnými dokumenty v elektronické podobě je nutné zajistit vhodný nástroj s funkcí obdobnou vlastnoručnímu podpisu. Obecně lze takto chápat elektronický podpis. Ale v elektronické podobě se nemusíme omezovat pouze na textové dokumenty, může se jednat o zvukové nahrávky, grafiku, video a jiné formáty. Dříve platný zákon, č. 227/2000 Sb., o elektronickém podpisu (2), definuje termín *„datová zpráva“* a dále zákon říká toto: *„Datovou zprávou jsou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou.“*. Avšak nově přímo uplatnitelné Nařízení Evropské unie eIDAS (1) používá termín *„elektronický dokument“*, který je nařízením chápán velmi obecně, jako: *„jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka“*.

2.1.3 Elektronický podpis

Elektronický podpis chápeme jako data v elektronické podobě, které jsou připojena k jiným datům v elektronické podobě (resp. k elektronickému dokumentu) nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání (1).

Tato specifikovaná data nahrazují klasický vlastnoruční podpis a identifikují toho, kdo podpis vytvořil. Potom hovoříme o tzv. podepsané či podepisující osobě (4, s. 31). Elektronický podpis nemusí přitom mít formu připomínající rukou psaný podpis (např. jako data získaná z dotykové podložky při podpisu elektronickým perem). Dnes je elektronický podpis realizován především metodou asymetrické kryptografie (5, s. 85), která využívá k šifrování tajný (soukromý) a veřejný klíč, a jejíž principy budou vysvětleny v kapitole 2.2. Prostředky pro vytváření elektronických podpisů jsou nejčastěji uchovávány na čipové kartě, USB tokenu atp. Variantně jsou vytvořeny pomocí snímače otisků prstů nebo dalšími způsoby.

Elektronický podpis, oproti tomu vlastnoručnímu, také svým mechanizmem zajišťuje pravost dokumentů, je schopen zaručit důkaz, že se podepsaný dokument od okamžiku podepsání nezměnil. Nebo nám naopak při vyhodnocování platnosti podpisu pomůže prokazatelně zjistit, že dokument po podepsání změněn byl. Nedozvíme se sice, jak moc a v jakém místě byl upraven, ale spolehlivě poznáme, že nejde o stejný dokument, jaký byl původně podepsán. Naproti tomu elektronický podpis nemůže zabránit tomu, že podepsaný dokument bude následně nějak pozměněn. (4, s. 29-33; 7, s. 27)

2.1.4 Digitální podpis

V praxi i literatuře se můžeme setkat také s pojmem digitální podpis, který možná více odráží povahu elektronického podpisu. V digitálním světě je podpis zpracován číselně, respektive číslicově (digitálně) pomocí matematických výpočtů. Někdy se digitálním podpisem rozumí konkrétnější forma elektronického podpisu založeného na certifikátu a infrastruktuře veřejného klíče. Pojem elektronický podpis chápeme jako něco obecnějšího a nadřazeného různým prostředkům pro vytvoření digitálních údajů k podpisu. To dokládá i způsob jakým je elektronický podpis definován v zákoně a vyhláškách, které pracují pouze s pojmem elektronický podpis. Předmětem této práce však budou převážně technologie digitálního podpisu, pro který se využívá metody asymetrického šifrování neboli asymetrické kryptografie. (4, s. 30; 7, s. 30-31)

2.2 Asymetrická kryptografie

Problematika vytváření elektronického podepisování a vyhodnocování platnosti podpisu je postavena na principech asymetrické kryptografie. Metody asymetrických

šifer používají pro šifrování a dešifrování dvou odlišných klíčů, jeden klíč pro šifrování a druhý klíč pro dešifrování. Pro tento pár klíčů platí to, že data šifrovaná klíčem pro šifrování nelze již dešifrovat týmž klíčem, ale pouze druhým klíčem z uvedeného páru klíčů. U digitálního podpisu se využívá skutečnosti, že operace šifrování a dešifrování jsou u některých šifer zaměnitelné, a proto se zde nepoužívá označení šifrovací a dešifrovací klíč, ale klíč soukromý a klíč veřejný. Příkladem algoritmu, který záměnu operací šifrování a dešifrování umožňuje, je šifrovací algoritmus RSA. K využití elektronického podpisu je proto nutné vygenerovat dvojici klíčů tvořenou soukromým a veřejným klíčem. (7, s. 25-28; 8)

Rozdíl mezi soukromým a veřejným klíčem vystihují právě jejich přívlastky:

- soukromý (též zvaný privátní) klíč je nutné pečlivě chránit a je žádoucí ho uložit do důvěryhodného úložiště (např. na disk nebo na čipovou kartu) a neposkytovat jej nikomu jinému;
- veřejný klíč naproti tomu smí být distribuován zcela volně a měl by být poskytnut tomu, kdo si chce ověřit platnost našeho elektronického podpisu. (4, s. 36; 8)

Soukromý klíč je důležité aktivum potřebné pro vytvoření vlastního elektronického podpisu, a proto vlastnictví soukromého klíče jednoznačně identifikuje podepisující osobu, nikdo jiný bez znalosti daného soukromého klíče nemůže stejný podpis vytvořit. Je tedy nutné soukromé klíče dobře střežit. Poskytnout někomu jinému svůj soukromý klíč znamená umožnit dotyčnému podepisovat se za naši osobu. (4, s. 36)

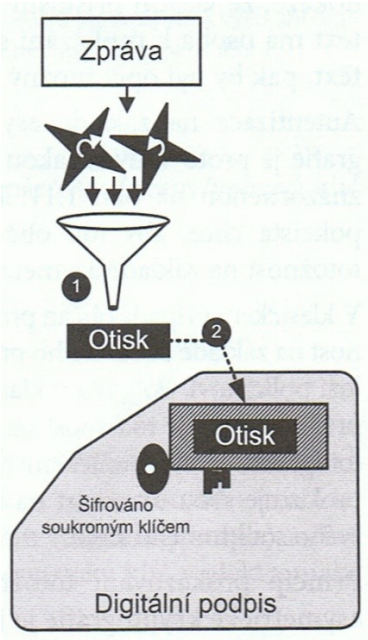
Veřejný klíč se využije až k ověření již existujícího elektronického podpisu. Elektronický podpis vytvořený pomocí soukromého klíče se povede úspěšně ověřit pouze pomocí jemu příslušného veřejného klíče. Chceme-li příjemce námi podepsaného dokumentu ujistit o tom, že je podpis platný a patří skutečně nám, musíme mu dát svůj veřejný klíč. (4, s. 36)

2.3 Mechanizmus elektronického podpisu

2.3.1 Vytvoření elektronického podpisu

Nepopiratelnost podepsaných dat zajišťuje následující mechanizmus. Vytvoření elektronického podpisu se provádí ve dvou hlavních krocích:

1. Je spočítán takzvaný otisk z podepisovaných dat (např. z elektronického dokumentu, který chceme podepsat). (7, s. 27)
2. Výsledný otisk se zašifruje soukromým klíčem osoby, která podpis vytváří. Soukromým klíčem šifrovaný otisk dat je elektronickým podpisem daných dat. (7, s. 27)



Obrázek 1: Vytvoření elektronického podpisu (43)

2.3.2 Otisk dokumentu

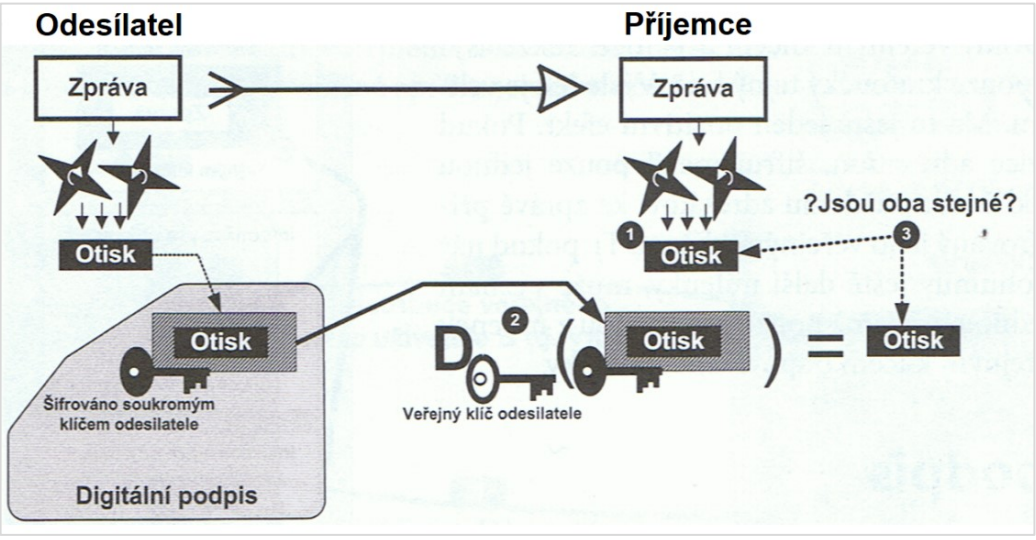
Otisk (anglicky hash) je řetězec znaků, který lze vypočítat z každého elektronického dokumentu. Jedná se o výsledek jednocestné funkce, která z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky. Hlavním předpokladem otisku je, že by měl maximálně identifikovat původní text – sebemenší změna v dokumentu musí mít za následek vznik otisku odlišného od otisku původního dokumentu. Algoritmy k provedení oné jednocestné funkce nejsou výpočetně náročné, ale je výpočetně velmi náročné (ideálně v rozumné časové míře nemožné) z otisku vytvořit původní

dokument. Pro vytvoření otisku dokumentu je, od roku 2010, v oblasti elektronického podpisu doporučeno používat algoritmy z rodiny SHA-2, které produkují řetězce o délce 224, 256, 384 nebo 512 bitů. K vytváření otisku z podepisovaných dat vedou následující důvody. Metody a algoritmy používané k podepisování dokumentů vyžadují práci s bloky dat o pevné velikosti a zároveň je třeba udržet tyto bloky o pevné velikosti dostatečně malé na to, aby mohlo šifrování a podepisování probíhat dostatečně rychle. (7, s. 21-22; 4, s. 70-71; 9)

2.3.3 Ověřování elektronického podpisu

Při ověřování elektronického podpisu je nutné na straně příjemce podepsaného dokumentu (popř. datové zprávy) realizovat tři hlavní kroky:

1. Příjemce dokumentu samostatně spočítá otisk dokumentu stejným algoritmem, který byl použit při podepisování. (7, s. 27)
2. Příjemce použije veřejný klíč odesílatele k dešifrování přijatého elektronického podpisu. Tím získá další otisk dokumentu, tj. ten, který spočítal odesílatel v okamžiku podepisování dokumentu. (7, s. 27)
3. Příjemce následně porovná výsledný otisk z bodu 1. s otiskem získaným v bodě 2. Když se oba otisky shodují, znamená to, že podpis mohl vytvořit pouze vlastník soukromého klíče – tedy odesílatel. A současně tím byla prokázána integrita dokumentu, to znamená, že dokument nebyl po podepsání odesílatelem změněn. (7, s. 27)



Obrázek 2: Ověření elektronického podpisu (44)

V případě, že se oba otisky neshodují nebo pokud příjemce nemůže pomocí veřejného klíče úspěšně dešifrovat podpis, není potvrzeno, že dokument nebyl po podepsání změněn a zda byl skutečně podepsán odesílatelem a jestli příjemce obdržel správný veřejný klíč. Takový podpis není možné ověřit a je pak považován za neplatný. Praktickou obranu proti podvržení veřejného klíče nabízí certifikace veřejného klíče nezávislou třetí stranou, dříve označovanou jako certifikační autorita, nyní novým nařízením chápanou jako poskytovatel služeb vytvářejících důvěru. (10; 11; 7, s. 27, 56; 1)

2.4 Certifikát pro elektronický podpis

„Certifikátem pro elektronický podpis se rozumí elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby.“ (1)

Certifikát je tedy datovou strukturou obsahující veřejný klíč a identifikační údaje osoby, které daný veřejný klíč patří. Úkolem certifikátu je stvrzení toho, že konkrétní veřejný klíč patří osobě popsané v certifikátu a současně stvrzuje i to, že tato osoba opravdu příslušný soukromý klíč vlastní a má jej výlučně ve své moci. V legislativě je specifikováno, že certifikát je na základě podané žádosti vydáván poskytovatelem služeb vytvářejících důvěru. Aby tento subjekt plnil správně svou funkci, musí jím být nezávislá, dostatečně důvěryhodná organizace. (7, s. 56-58; 4, s. 37-39; 12)

2.4.1 Struktura certifikátu

Struktura certifikátu vychází z několika norem (X.509, EDI, WAP apod.) (7, s. 59). Nejčastěji se používá struktura certifikátu verze 3, podle mezinárodního standardu ITU-T X.509 (7, s. 59; 38). Pro potřeby internetu byl také vytvořen internetový profil standardu X.509, kterým je dnes standard RFC-5280 (7, s. 59; 37).

Každý certifikát musí obsahovat následující údaje:

- verze certifikátu, uvádí, je-li certifikát odvozen od normy X.509, verze může být 1, 2 nebo 3;
- pořadové (resp. sériové) číslo certifikátu, které musí být vždy jedinečné, v rámci konkrétního poskytovatele služeb vytvářejících důvěru;

- platnost, tj. datum počátku a konce platnosti certifikátu;
- algoritmus podpisu, specifikuje algoritmy použité poskytovatelem služeb vytvářejících důvěru pro vytvoření elektronického podpisu certifikátu (výpočet otisku a algoritmus šifrování);
- identifikační údaje subjektu, kterému je certifikát vydán;
- veřejný klíč subjektu, kterému je certifikát vydán, je sekvencí dvou informací: identifikací algoritmu, pro nějž je veřejný klíč určen, a samotným veřejným klíčem;
- identifikační údaje subjektu, který certifikát vydal;
- podpis certifikátu soukromým klíčem poskytovatele služeb vytvářejících důvěru. (7, s. 58-64; 12)

Podpis certifikátu soukromým klíčem poskytovatele služeb vytvářejících důvěru zajišťuje zmíněné spojení veřejného klíče a identifikačních údajů subjektu, jemuž je certifikát vydán, a zároveň je tak certifikát chráněn před neoprávněnou změnou a zfalšováním. Při ověřování platnosti certifikátu proto musíme mít k dispozici také certifikát poskytovatele služeb vytvářejících důvěru pro potvrzení platnosti jeho podpisu na ověřovaném certifikátu. Tyto certifikáty je obvykle možné získat na internetových stránkách daného poskytovatele služeb vytvářejících důvěru. (7, s. 56-57; 12)

2.4.2 Rozšíření certifikátu

Kromě výše uvedených údajů může certifikát obsahovat ještě další informace a tzv. rozšíření certifikátu. Může se jednat například o omezení účelu, pro který smí být certifikát používán (podpis elektronické pošty, podpis kódu softwarové aplikace, potvrzení totožnosti klienta či serveru atd.), o cestu k certifikátům poskytovatele služeb vytvářejících důvěru nebo cestu k seznamu zneplatněných certifikátů a podobně. (12; 7, s. 64-65)

2.4.3 Druhy certifikátů

Certifikáty lze rozdělit na dva specifické druhy, tzv. komerční certifikáty a kvalifikované certifikáty. Základní rozdíl mezi nimi je ten, že požadavky na kvalifikované certifikáty a jejich obsah vymezuje legislativa Evropské unie a České

republiky, kdežto u komerčních certifikátů zákon jejich obsah nevymezuje. Dále však ještě u těchto druhů certifikátů rozlišujeme možnosti jejich užití v praxi. (4, s. 40; 13)

Komerční certifikát

Komerční certifikáty nejsou spjaty se zákonem ČR a nařízením Evropské unie, nemusí tedy striktně splňovat všechny náležitosti zákona a je pouze na daném poskytovateli služeb vytvářejících důvěru, jaké podmínky si stanoví. Komerční certifikáty vydává certifikační autorita (dále také CA), která ověří žadatele dle svých vlastních směrnic (tzv. certifikační politiky). (14)

Slovní spojení *„certifikační autorita“* je možné chápat dvojím způsobem: buď jako aplikaci, která vydává certifikáty, nebo jako instituci, která zajišťuje proces vydávání certifikátů. Jako instituce může CA existovat jako samostatná firma či jako samostatný útvar v rámci firmy (7, s. 76-77). Certifikačních autorit existuje celá řada, vydavatelem certifikátů může být v podstatě ten, kdo disponuje potřebnou technologií pro poskytování certifikačních služeb, certifikační autoritu může provozovat například banka, zaměstnavatel, internetový poskytovatel nebo stejně tak my sami na svém vlastním počítači, zpravidla se však jedná o specializovanou organizaci (4, s. 42). Důležité je, aby CA fungovala v rámci komunikace jako ona důvěryhodná třetí strana, která prostřednictvím vydaného certifikátu stvrzuje spojení identity subjektu (podepisující osoby) s jeho elektronickou totožností (dvojicí klíčů), čímž je umožněna zabezpečená komunikace i osobám, které se fyzicky nikdy nesetkaly (15, s. 40; 4, s. 37). Nové Nařízení eIDAS (1) navíc, v článku 19, požaduje jak po kvalifikovaných, tak i po nekvalifikovaných poskytovatelích služeb vytvářejících důvěru (dále také jako PSVD) přijmout technická a organizační opatření k zajištění úrovně bezpečnosti, která je přiměřená míře rizik.

Díky tomu, že na komerční certifikát není kladen žádný požadavek ze strany zákona, jejich využití je volnější a mají široké uplatnění. Na rozdíl od kvalifikovaných certifikátů, komerční certifikáty nejsou automaticky uznávány. Avšak (1) v článku 25, odstavec 1, uvádí: *„Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“*.

Komunikující strany se tudíž, např. v obchodních vztazích, mohou na důvěře v daný certifikát zvoleného PSVD nějak dohodnout (např. smluvně). (14; 16)

Komerční certifikáty je možné využít například pro:

- ověřování elektronických podpisů;
- šifrování komunikace;
- autentizaci uživatele. (14; 17; 4, s. 40)

Komerční certifikáty jsou vydávány nejen konkrétním osobám (tzv. osobní komerční certifikát), ale i pro využití nějakými technickými zařízeními či automatizovanými systémy, např. servery a aplikacemi pro identifikaci a šifrování, vytváření elektronických pečetí a elektronických časových razítek apod. Potom jde o tzv. systémové komerční certifikáty neboli, s přihlédnutím k terminologii Nařízení eIDAS, o komerční certifikáty pro elektronickou pečeť, elektronické časové razítko nebo pro autentizaci internetových stránek. (16; 4, s. 40; 1)

Kvalifikovaný certifikát

Kvalifikovaný certifikát vydává pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru (4, s. 119) a splňuje náležitosti dané Nařízením Evropské unie č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) (1) a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru (3).

Kvalifikované certifikáty jsou určeny výhradně k:

- ověřování podpisů;
- ověřování elektronických pečetí;
- autentizaci webových stránek (1).

Pro komunikaci se subjekty státní správy je vyžadován právě certifikát vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Kvalifikovaný elektronický podpis zajišťuje integritu a autenticitu elektronického dokumentu a důvěřuje mu nejen celá veřejná správa České republiky, ale také orgány veřejné správy v dalších členských státech Evropské unie. Důvěryhodnost kvalifikovaných

poskytovatelů služeb vytvářejících důvěru je kontrolována příslušnými orgány dohledu. (14; 16; 17; 4, s. 119; 13; 18)

Kvalifikovaný certifikát pro elektronický podpis musí podle přílohy I, Nařízení eIDAS (1), obsahovat:

- označení, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis;
- soubor dat jednoznačně identifikujících kvalifikovaného PSVD, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a
    - v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,
    - v případě fyzické osoby: jméno osoby;
- alespoň jméno podepisující osoby nebo pseudonym a je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;
- data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů;
- označení začátku a konce doby platnosti certifikátu;
- identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného PSVD;
- zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného PSVD, který certifikát vydává;
- údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle předchozího odstavce;
- údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;
- pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

Kvalifikovaný certifikát pro elektronický podpis je vydán výhradně fyzické osobě a slouží k vytváření elektronických podpisů. Vychází se z logiky, že rukou psaný

podpis rovněž nemůže vytvořit nikdo jiný než konkrétní fyzická osoba (i v případě, že zastupuje např. právnickou osobu). Avšak pro potřeby automatizovaných systémů a podpisů vytvářených servery fyzická osoba podpis vytvořit nemůže, v okamžiku automatizovaného vytváření podpisu totiž nemá příslušný soukromý klíč pod svou kontrolou. Z tohoto důvodu je definován tzv. kvalifikovaný certifikát pro elektronickou pečeť, který může být vydán jak fyzické, tak právnické osobě, a pomocí kterého je umožněno elektronické dokumenty opatřit automatizovaně tzv. elektronickou pečetí. (7, s. 73; 13; 4, s. 123-125)

2.4.4 Poskytovatel služeb vytvářejících důvěru

Dle terminologie zákona a Nařízení eIDAS (1) certifikáty vydává poskytovatel služeb vytvářejících důvěru (PSVD). V Nařízení eIDAS (1) je rovněž přesně určeno, že onou poskytovanou službou vytvářející důvěru se rozumí elektronická služba, která je zpravidla poskytována za úplatu, a že spočívá:

- *„ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo*
- *ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo*
- *v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami“*.

Jak již bylo výše v textu uvedeno, kvalifikované certifikáty mohou vydávat pouze kvalifikovaní PSVD, kteří splňují všechny zákonné požadavky. PSVD, kteří mají v plánu začít poskytovat kvalifikované služby, musí nechat provést audit subjektem posuzování shody, který je k tomu akreditovaný určeným orgánem dohledu, v České republice je orgánem dohledu Ministerstvo vnitra. Účelem auditu je potvrzení toho, že kvalifikovaní PSVD i jimi poskytované kvalifikované služby splňují požadavky dané Nařízením eIDAS (1). Poté PSVD předloží oznámení o svém úmyslu společně se zprávou o posouzení shody orgánu dohledu, který vyhodnotí, zdali PSVD splňuje požadavky nařízení – a pokud tomu tak skutečně je, udělí tomuto PSVD status kvalifikovaného poskytovatele služeb vytvářejících důvěru a rovněž jeho

poskytovaným službám. Orgán dohledu následně zveřejní tuto skutečnost aktualizací důvěryhodných seznamů obsahující informace o kvalifikovaných PSVD a jimi poskytovaných kvalifikovaných službách vytvářejících důvěru, až poté mohou kvalifikovaní poskytovatelé své služby vytvářející důvěru poskytovat. Důvěryhodný seznam kvalifikovaných PSVD je všem dostupný například na internetových stránkách Ministerstva vnitra. V současné době působí v České republice čtyři kvalifikovaní poskytovatelé služeb vytvářejících důvěru: První certifikační autorita, a. s., Česká pošta, s. p. (resp. její služba PostSignum), společnost eIdentity a. s. a Software602 a. s. (1; 3; 4, s. 42-43; 19)

2.4.5 Životní cyklus certifikátu

Certifikát za dobu své existence prochází několika fázemi, které všeobecně tvoří jeho životní cyklus. Životní cyklus certifikátu se skládá z těchto fází:

1. *Vytvoření žádosti o certifikát.* Zpravidla lze vyplnit formulář získaný na internetových stránkách příslušného PSVD. Vytvoření žádosti může, ale také nemusí, předcházet generování soukromého a veřejného klíče (v méně častém případě může generovat párová data PSVD po obdržení žádosti). (7, s. 74)
2. *Zpracování žádosti o certifikát.* PSVD ověří údaje uvedené v žádosti, případně některé informace přidá nebo odebere. (20, s. 26-27)
3. *Vydání certifikátu.* PSVD vydá certifikát a buďto on, nebo žadatel může následně certifikát publikovat. (7, s. 74)
4. *Platnost certifikátu.* Je chybné se domnívat, že certifikát je automaticky platný od doby jeho vydání. Začátek a konec platnosti certifikátu je uveden v certifikátu a může začínat až v době po jeho vydání. Platnost certifikátu může být též ukončena odvoláním certifikátu. (7, s. 74)
5. *Vypršení platnosti certifikátu.* Po uplynutí doby uvedené v certifikátu (platnost *„do“*) je certifikát neplatný. (7, s. 74)
6. *Odvolání certifikátu.* Ještě před uplynutím původně deklarované platnosti certifikátu může PSVD certifikát zneplatnit jeho odvoláním (resp. revokací), které je zpravidla provedeno tak, že zveřejní identifikaci certifikátu v seznamu odvolaných certifikátů. PSVD odvolá certifikát například když zjistí, že údaje v certifikátu už nejsou pravdivé či na samotnou žádost držitele certifikátu, který

si již nepřeje, aby certifikát dále platil, anebo byl kompromitován či zničen jeho soukromý klíč. (7, s. 74; 4, s. 96-97)

2.5 Druhy elektronického podpisu

Podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (3), v návaznosti na přímo použitelné Nařízení Evropské unie č. 910/2014, ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (1), rozlišujeme několik druhů elektronického podpisu, u kterých zákon upravuje zejména požadavky na jednotlivé druhy podpisu v závislosti na podepisující osobě a osobě, vůči níž je právně jednáno. (21; 1)

2.5.1 Prostý elektronický podpis

Zákon definuje elektronický podpis, který je často pro svou obecnou definici označován jako prostý elektronický podpis, takto: Elektronickým podpisem se rozumí *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“* (1). Takto definovaný elektronický podpis je dále v textu nazýván prostým elektronickým podpisem.

Definici prostého elektronického podpisu vyhovuje například naskenovaný vlastnoruční podpis, podpis nasnímaný na dotykovém zařízení, dokonce i podpis e-mailové zprávy ve formě textového označení odesílatele a rovněž podepsání elektronického dokumentu napsáním jména uvnitř dokumentu. (21; 6)

Jak již bylo uvedeno, Nařízení eIDAS (1) stanoví, že: *„Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“* Z toho lze odvodit, že prostý elektronický podpis lze např. použít k podepisování elektronického dokumentu, kterým se právně jedná mezi osobami soukromého práva, a že při jednání v soukromoprávních vztazích zrovnoprávňuje všechny formy elektronického podpisu s vlastnoručním podpisem jednající osoby, pokud se na tom strany dohodnou. (21; 22; 23)

Avšak z technického hlediska může v případě prostého elektronického podpisu panovat nejistota ohledně identifikační a autentizační funkce takového podpisu a také je postrádáno zaručení integrity dokumentu. Záležet proto bude na dohodě smluvních stran, jaká pravidla si nastaví. Zatím ale není jasné, jaké obrysy získá široce formulovaná definice elektronického podpisu v rozhodovací praxi Soudního dvora Evropské unie a tuzemských soudů, zda definici výkladově zúží a dovolí dodatečné podmínky. Účinek prostého elektronického podpisu je tak zatížen důkazním břemenem o tom, že jednání bylo učiněno osobou, identifikovanou v daném elektronickém právním jednání. V případě, že by jednající soukromoprávní osoba chtěla zajistit uznatelnou správnost obsahu dokumentu nebo splnění funkce ověření totožnosti podepisující osoby, může využít některou z vyšších forem elektronického podpisu. (21; 22; 23)

2.5.2 Zaručený elektronický podpis

Zaručený elektronický podpis podle svého názvu dává, oproti prostému elektronickému podpisu, a dokonce i vlastnoručnímu podpisu, jisté záruky. Zaručený elektronický podpis zajišťuje integritu dokumentu, je tedy možné zjistit jakoukoliv následnou změnu dat. Zaručený elektronický podpis zároveň umožňuje identifikovat podepisující osobu tím, že poskytne určité údaje o identitě této osoby. Zaručený elektronický podpis je založen na certifikátu, na který však nejsou kladeny žádné požadavky. Může se jednat o jakýkoli certifikát, například komerční certifikát, testovací certifikát či jiný certifikát, jenž není kvalifikovaný. Nelze proto dostatečně ověřit poskytnutou identitu podepisující osoby natolik, aby bylo možné uznat tento druh elektronického podpisu např. pro komunikaci s orgány veřejné správy. (4, s. 31-33; 23; 6; 21; 1; 7, s. 30-31, 129)

Nicméně v Nařízení Evropské unie eIDAS je definováno, že zaručený elektronický podpis musí splňovat následující požadavky:

- *„a) je jednoznačně spojen s podepisující osobou;*
- *b) umožňuje identifikaci podepisující osoby;*
- *c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a*

- *d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.“* (1).

2.5.3 Kvalifikovaný elektronický podpis

Nejvyšší formou elektronického podpisu, dle Nařízení eIDAS (1), je kvalifikovaný elektronický podpis, pro který platí, že musí jít o zaručený elektronický podpis vytvořený kvalifikovaným prostředkem pro vytváření elektronických podpisů a založeném na kvalifikovaném certifikátu pro elektronické podpisy. (21; 6)

Kvalifikovaným prostředkem pro vytváření elektronických podpisů se rozumí konfigurované programové vybavení nebo technické zařízení pro vytváření elektronických podpisů, které splňuje požadavky stanovené v příloze II, Nařízení eIDAS (1). Jde především o čipové karty a USB tokeny, jež prošly potřebnou certifikací a představují tak bezpečné úložiště pro soukromý klíč a kvalifikovaný certifikát používaný k podepisování, jelikož tato zařízení fungují na principu, že soukromý klíč, ke kterému je kvalifikovaný certifikát vystavován, musí být generován uvnitř tohoto zařízení a nesmí jej opustit, není tedy možný jeho export. (6; 21)

Díky kvalifikovaným prostředkům nutným k jeho použití naplňuje kvalifikovaný elektronický podpis, vedle zajištění integrity dokumentu a identifikace jednající osoby, funkci ověření totožnosti jednající osoby, poskytuje proto vysokou míru důvěryhodnosti. (21; 6; 24)

Tuto formu elektronického podpisu proto podle Nařízení eIDAS (1) a § 5 zákona č. 297/2016 Sb., o službách vytvářejících důvěru (3), musí používat vyjmenované orgány veřejné moci a jiné fyzické či právnické osoby při výkonu působnosti v oblasti veřejné správy. Zároveň je kvalifikovaný elektronický podpis podle § 6 zákona o službách vytvářejících důvěru uznáván i při opačné situaci, tedy podání občana či firmy vůči úřadu, a to nejen v České republice, ale ve všech zemích Evropské unie. A podle odst. 2, článku 25, Nařízení eIDAS (1), má kvalifikovaný elektronický podpis *„právní účinek rovnocenný vlastnoručnímu podpisu“*. Z toho vyplývá že, záměrem nového Nařízení eIDAS (1) je poskytnout kvalifikovaným elektronickým podpisům ve všech členských státech Evropské unie stejné právní účinky jako vlastnoručnímu podpisu a zajistit uznávání kvalifikovaného elektronického podpisu vydaného

v jednom členském státě za kvalifikovaný elektronický podpis ve všech ostatních státech (25). Výhodu uznávání a vysoké úrovně důvěry tento druh podpisu přináší zároveň také při jednání v soukromoprávních vztazích, např. obchodních. (21; 6; 24)

2.5.4 Zaručený el. podpis založený na kvalifikovaném certifikátu

Tento druh elektronického podpisu se v mnohém podobá kvalifikovanému elektronickému podpisu, stále se musí jednat o zaručený elektronický podpis a také musí být založený na kvalifikovaném certifikátu, avšak liší se tím, že nepožaduje použití kvalifikovaného prostředku pro vytváření elektronických podpisů. Tímto se ocitá o stupeň níže na pomyslné stupnici důvěryhodnosti než kvalifikovaný elektronický podpis, a tudíž ani Nařízení eIDAS (1) zaručený elektronický podpis založený na kvalifikovaném certifikátu neuznává pro komunikaci s orgány Evropské unie a jiných členských zemí. Jak je tomu v případě České republiky, bude vysvětleno v následující kapitole 2.5.5. (6; 23; 21; 26; 1)

2.5.5 Uznávaný elektronický podpis

Je důležité uvést, že adaptační zákon č. 297/2016 Sb., o službách vytvářejících důvěru (3), zachovává dosud používaný pojem uznávaný elektronický podpis, ale upravuje jeho obsah a význam, než jaký měl doposud. Nový výklad termín užívá jako tzv. legislativní zkratku za dva různé druhy elektronických podpisů, a to podle § 6, odst. 2, za:

- zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo
- kvalifikovaný elektronický podpis. (6; 3)

Dále zákon o službách vytvářejících důvěru (3) v § 6 stanoví, že pouze uznávaný elektronický podpis lze použít, např. soukromoprávní osobou, k podepsání elektronického dokumentu, kterým se jedná vůči veřejnoprávnímu podepisujícímu nebo osobě vykonávající jeho působnost. Jelikož zaručený elektronický podpis založený na kvalifikovaném certifikátu není rovnocenný kvalifikovanému elektronickému podpisu, je potřeba rozlišit například to, že pro komunikaci s orgány veřejné správy České republiky lze použít jak zaručený elektronický podpis založený

na kvalifikovaném certifikátu, tak i kvalifikovaný elektronický podpis (tedy uznávaný elektronický podpis), ale při komunikaci s orgány veřejné správy jiných členských zemí je požadován pouze kvalifikovaný elektronický podpis. (6; 21; 1)

2.6 Jiné druhy elektronického podpisu

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, paragrafem 7, říká: *„K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1“* (3). Zjednodušeně řečeno, § 7 se netýká komunikace s úřady v úředních věcech, ale právě všech ostatních případů ano, obecně tedy veškerého soukromoprávního jednání, např. jednání občanů s bankami, operátory, firmami či jednání mezi firmami navzájem. A zákon v těchto případech připouští použití všech vyjmenovaných variant elektronických podpisů tak, jak je zná Nařízení eIDAS (1), a staví je na roveň vlastnoručnímu podpisu, tudíž i včetně elektronického podpisu bez přívlastku, resp. prostého elektronického podpisu. Z tohoto důvodu bych dále v této kapitole rád uvedl některé další druhy elektronického podpisu, které vyhovují definici elektronického podpisu bez přívlastku, avšak nejsou tak úplně *„prosté“*, a proto mohou být ve výše uvedených případech použitelné a efektivní. (23; 27, s. 10, 33-36; 22; 3)

2.6.1 Dynamický biometrický podpis

Stále častěji používaným řešením při uzavírání zákaznických smluv s nejrůznějšími poskytovateli služeb, např. s bankami, pojišťovnami, různými přepravci atd., je využití tzv. dynamického biometrického podpisu (DBP) (23). Jak název napovídá, DBP jistým způsobem využívá biometrické charakteristiky podepisující osoby, v užším slova smyslu se tyto biometrické charakteristiky týkají toho, jak konkrétní osoba vytváří svůj klasický vlastnoruční podpis (4, s. 56-57).

Výhodou je, že celý proces se velmi podobá klasickému vlastnoručnímu podepisování dokumentu v listinné podobě, avšak při podepisování elektronického dokumentu pomocí DBP je podepisující osoba, většinou se jedná o zákazníka, vyzvána k vytvoření svého vlastnoručního podpisu speciálním perem na dotykové ploše či tabletu, přičemž

se nesnímá pouze obrazová podoba podpisu, tedy záznam křivky podpisu, nýbrž také rychlost tahu perem a přítlak. Tím vznikne jakýsi unikátní vzorek dat podepisující osoby, který by neměl být schopen vytvořit nikdo jiný. Z důvodu ochrany osobních údajů je vzorek dat podepisující osoby obvykle ještě šifrován a následně je připojen v roli prostého elektronického podpisu k elektronickému dokumentu, nad kterým se právě jedná. Připojení je realizováno tak, že podepisovaný dokument i s vloženým zašifrovaným vzorkem DBP osoby podepíše ještě samo technické zařízení, na kterém se DBP vytváří, a aby mohla být zaručena integrita podepsaného dokumentu, použije k tomu některou vyšší formu elektronického podpisu, obvykle například zaručenou elektronickou pečeť. (23; 4 s. 57)

Po zákazníkovi, který postupem popsaným výše potvrdil svůj projev vůle vůči smluvnímu dokumentu, pomocí DBP v roli prostého elektronického podpisu, zbývá ještě vložit projev vůle vůči smluvnímu dokumentu vyjádřený protistranou, která ho učiní rovněž podepsáním dokumentu vyšší formou elektronického podpisu (23). Zde se hodí druh elektronického podpisu, jenž vyhovuje definici uznávaného elektronického podpisu již podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru (3).

Vzhledem k uvedenému postupu je odbornou veřejností akceptováno, že vzorek dat DBP může plnit roli prostého elektronického podpisu a současně přitom poskytnout vyšší kvalitu a důvěru než jiné prosté elektronické podpisy. A to také díky unikátním datům, která dostatečně specifikují podepisující osobu a která je možné, v případě potřeby, podrobit zkoumání znalcem z oboru kybernetiky a písmoznalectví, jenž je poté schopen posoudit, jestli podpis skutečně patří dané osobě či nikoli a zda do dat, jež charakterizují biometrický podpis, mohlo být nějakým způsobem zasaženo. (28)

Je nutné dodat, že ono technické zařízení musí zajistit bezpečný proces získávání vzorku podpisových dat podepisující osoby a jak je s ním dál nakládáno. To platí především pro skutečnost, že vzorek bude připojen ke konkrétnímu smluvnímu dokumentu, a ne k nějakému jinému, a že vzorek dat je kvůli ochraně osobních dat před připojením k dokumentu zašifrován bezpečným klíčem zpřístupněným výhradně pro potřebu případného znaleckého zkoumání. Z těchto důvodů se výrobci podpisových zařízení snaží, aby jejich produkty plnily nejrůznější bezpečnostní normy

a certifikace, a poskytují informace o používaných algoritmech přenosu dat a šifrování. (28; 23; 29)

DBP mohou být pro společnosti v běžném obchodním styku přínosem umožňujícím manipulaci s dokumenty v elektronické podobě, namísto v listinné, což může přinést úsporu času a nákladů zrychlením oběhu dokumentů uvnitř i vně společnosti. DBP dokáží usnadnit práci například dopravcům, obchodním zástupcům, servisním technikům, manažerům apod. (29; 28)

2.6.2 Podpis pomocí tlačítka – „click-wrap“

K podepisování elektronických dokumentů prostým elektronickým podpisem může posloužit i podpis pomocí tlačítka – *„click-wrap“* (30), který může najít uplatnění přímo v informačním systému, nebo může být poskytován třetí stranou jako služba, pomocí které se pracuje s elektronickými dokumenty. Podstatou tohoto podepisování je vytvořit v informačním systému či v aplikaci služby kontrolované prostředí, v rámci kterého se zaznamenávají všechny relevantní skutečnosti, jako například:

- kdy se do systému přihlásil jaký uživatel;
- jakými způsoby autentizace ověřil svoji identitu;
- z jaké IP adresy se uživatel přihlásil;
- jaké konkrétní úkony každý uživatel provedl atd. (23)

Příslušné záznamy systém vede pro každý jednotlivý dokument a ukládá je jako auditní záznam, tzv. log dokumentu. Pokud se právě přihlášený uživatel rozhodne podepsat konkrétní dokument, který má v rámci systému k dispozici, stačí pak kliknout na tlačítko *„Podepsat dokument“* či *„Souhlasím a podepisuji“* a systém následně provede všechny potřebné úkony. Do logu příslušného dokumentu je zapsáno, že daný uživatel vyjádřil svou vůli podepsat stanovený dokument, a na určené místo v dokumentu je vloženo něco, co takovýto podpis symbolizuje, může se jednat o obrázek vlastnoručního podpisu nebo speciálním písmem napsané jméno uživatele. Systém či služba dále sama podepíše žurnál se záznamy všech relevantních úkonů některou vyšší formou elektronického podpisu a přikládá jej k samotnému elektronickému dokumentu. Podle logu mohou další strany posuzovat, zda a kým je dokument podepsán. Míra důvěryhodnosti elektronického podpisu vytvořeného

pomocí tlačítka závisí především na způsobu identifikace a autentizace uživatele v systému či službě, a dále také na kvalitě vytváření logů dokumentů. (23; 31)

2.6.3 Podpis pomocí otisku prstů

V současnosti existují dvě možné varianty využití otisku prstu při elektronickém podepisování dokumentů. V prvním případě je podpis pomocí otisku prstu obdobou dynamického biometrického podpisu, avšak jako unikátní vzorek dat podepisující osoby zde slouží biometrická charakteristika otisku prstu nasnímaná na speciálním zařízení ke čtení otisků prstů. Ostatní principy se již shodují s dynamickým elektronickým podpisem, vzorek dat podepisující osoby je také z důvodu ochrany osobních dat nejprve šifrován a posléze je připojen k dokumentu pomocí elektronického podpisu provedeného samotným technickým zařízením. Přestože tento druh elektronického podepisování nabízí rychlý a jednoduchý postup vytvoření elektronického podpisu při zaručení jistých bezpečnostních opatření, v praxi se netěší přílišné oblibě a není zatím nijak významně využíván. Odborná veřejnost se domnívá, že za to může psychologický efekt této metody, jelikož pro mnoho lidí není poskytnutí biometrických údajů otisku prstů ke zpracování, ač jen za účelem vytvoření elektronického podpisu, komfortní. I když je podpis vytvářen pomocí certifikovaného zařízení protistrany, z pohledu podepisující osoby se jedná víceméně o cizí zařízení. (4, s. 56-57; 23; 32)

Paradoxně je to přesně naopak v dalším případě, kdy je otisků prstů v praxi stále více využíváno na mobilních zařízeních, noteboocích, tabletech a zejména v chytrých mobilních telefonech, vybavených čtečkou otisků prstů. Tato zařízení má vlastník neustále pod osobní kontrolou, nabízí se tudíž možnost využít je také pro připojování elektronických podpisů k dokumentům, což opět vede ke zrychlení procesů. V případě ztráty či krádeže zařízení může vlastník podpisový certifikát nechat okamžitě zneplatnit. (33)

Na mobilních zařízeních přináší čtení otisku prstů přirozenější a snadnější způsob autentizace uživatele či autorizace některých jeho činností. Při podepisování dokumentů na mobilních zařízeních tak otisk prstu podepisující osobě umožňuje přístup do kontrolovaného prostředí, poskytujícího funkce potřebné pro práci

s důvěryhodnými elektronickými dokumenty, a rovněž umožňuje rychlejší potvrzení připojení elektronického podpisu k dokumentu. (33; 34)

Například společnost Software602 a. s., vedená na seznamu kvalifikovaných služeb vytvářejících důvěru, nabízí aplikaci Signer pro osobní počítače, tablety a chytré mobilní telefony poskytující služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí a služby uchování kvalifikovaných elektronických podpisů a pečetí. Verze aplikace Signer pro platformu iOS na zařízeních Apple iPhone a Apple iPad vybavených funkcí Touch ID umožňuje autorizovat připojení zaručeného či uznávaného elektronického podpisu k elektronickému dokumentu právě pomocí otisku prstu, namísto doposud používaného hesla či kódu PIN. Touch ID je funkce pro rozpoznávání otisků prstů, kterou navrhla a vyvíjí společnost Apple Inc. od roku 2013 a představuje způsob používání unikátního otisku prstu místo hesla či kódu na zařízeních vybavených snímačem otisků prstů, označovaným též jako snímač Touch ID. Pro podepisující osobu je tak podepsání deseti dokumentů na mobilním zařízení s autorizací pomocí otisku prstu snazší a rychlejší než s autorizací pomocí kódu PIN nebo hesla, s využitím malých a velkých písmen, číslic a zvláštních znaků. (33; 35; 34; 36)

3 ANALYTICKÁ ČÁST

3.1 Zhodnocení jednotlivých řešení elektronického podpisu

Na základě informací zjištěných v průběhu práce, s využitím studiem nabytých vědomostí, uvádím v následující tabulce č. 1 stručný přehled všech posuzovaných variant s výčtem hlavních výhod a nevýhod, s cílem usnadnit výběr a doporučit optimální způsob elektronického podpisu.

Způsob el. podepisování	**druh el. podpisu**	**výhody**	**nevýhody**
napsání jména v el. dokumentu	prostý el. podpis	-velmi jednoduché vytvoření podpisu -srozumitelná podoba -nulové náklady	-zatížen důkazním břemenem -velmi nízká důvěryhodnost -nezajistí integritu dokumentu -problém ověření podpisu
sejmutí rukou psaného podpisu bez biometriky	prostý el. podpis	-akt podobný klasickému podepisování -relativně dobře dostupná technologie (dotyk, graf. tablet) -lehká charakteristika podepisující os.	-nezajistí integritu dokumentu -méně srozumitelná podoba -problém ověření podpisu
kliknutím – *„click-wrap“*	prostý el. podpis, zaručená el. pečeť	-jednoduchost vytvoření podpisu -možnost integrace do IS -vyšší forma el. podpisu -zajistí integritu dokumentu	-režie podpisových žurnálů (velký počet dokumentů) -velký zásah do IS
DBP pomocí specializovaného zařízení	prostý el. podpis, zaručená el. pečeť	-akt podobný klasickému podepisování -velké možnosti písmoznalecké analýzy -biom. charakteristika os.	-nutný souhlas se zpracováním biom. informací -potřeba spec. zařízení -pořizovací náklady
pomocí otisku prstu	prostý el. podpis, zaručená el. pečeť	-rychlé a jednoduché vytvoření podpisu -zajistí integritu dokumentu	-potřeba spec. zařízení -nejednotné technologie -psychologický efekt
pomocí čipové karty či USB tokenu	zaručený el. podpis	-zajistí integritu dokumentu -identifikuje podepisující os.	-potřeba spec. zařízení (karta a čtečka nebo USB token) - nižší důvěryhodnost
pomocí čipové karty či USB tokenu	uznávaný el. podpis	-vysoká důvěryhodnost -uznáván úřady -zajistí integritu dokumentu -jednoznačně identifikuje podepisující osobu	-potřeba spec. zařízení -pořizovací náklady
pomocí úložiště certifikátů Windows	uznávaný el. podpis	-nevyžaduje spec. zařízení -vysoká důvěryhodnost -uznáván úřady -zajistí integritu dokumentu -jednoznačně identifikuje podepisující os. -jednoduché vytvoření podpisu -možnost autorizace	-úložiště certifikátů Windows není kvalifikovaným prostředkem pro vytvoření el. podpisu -bez použití časového razítka je čas vytvoření podpisu neprůkazný.

Tabulka 1: Zhodnocení jednotlivých řešení elektronického podpisu

3.2 Posouzení variant el. podpisu pro různé druhy komunikace v IS

V následující tabulce č. 2 jsou shrnuty závěry o vhodnosti použití jednotlivých posuzovaných způsobů elektronického podepisování pro úrovně komunikace dané informačním systémem firmy. Pro každou variantu vytvoření elektronického podpisu je výslovně uvedeno, zda ji lze či nelze v daném případě použít, příp. jsou doplněny další informace. V určitých případech sice zákon použití některých způsobů podpisu dovoluje, ale nelze je však z uvedených důvodů pro danou komunikaci doporučit.

Způsob el. podepisování			napsání jména v el. dokumentu	sejmutí rukou psaného podpisu bez biometriky	kliknutím – click-wrap	DBP pomocí specializovaného zařízení	pomocí otisku prstu	pomocí čipové karty, USB tokenu nebo úložiště certifikátů Windows	pomocí čipové karty, USB tokenu nebo úložiště certifikátů Windows
druh el. podpisu			prostý el. podpis	prostý el. podpis	prostý el. podpis + zaručená el. pečeť	prostý el. podpis + zaručená el. pečeť	prostý el. podpis + zaručená el. pečeť	zaručený el. podpis	uznávaný el. podpis
komunikace	mezi zaměstnanci		nelze doporučit - důkazní břemeno - problém ověření podpisu - nezajistí integritu - nutná dohoda o uznávání	nelze doporučit - důkazní břemeno - problém ověření podpisu - nezajistí integritu	lze použít - rozsáhlá integrace do IS - zátěž při velkém objemu dokumentů	lze použít, nelze doporučit - existují lepší varianty - nutný souhlas o zpracování osobních informací - potřeba vytvořit podpisový vzor - další povinnosti (GDPR)	nelze doporučit - nutný souhlas o zpracování osobních informací	lze použít	lze použít
	mezi firmami	při servisní činnosti	nelze doporučit - důkazní břemeno - problém ověření podpisu - nezajistí integritu - nutná dohoda o uznávání	lze použít pro podpis zákazníka - nutná dohoda o uznávání - nezajistí integritu - nutné podpořit důkazy	lze použít - rozsáhlá integrace do IS - zátěž při velkém objemu dokumentů - nutná dohoda o uznávání	lze použít - vhodné pro podpis zákazníka - nutný souhlas o zpracování osobních informací - nutná dohoda o uznávání	nelze doporučit - nutný souhlas o zpracování osobních informací - nutná dohoda o uznávání	lze použít - nutná dohoda o uznávání - nelze vyžadovat po zákazníkovi	lze použít - nelze vyžadovat po zákazníkovi
		při podpisu smlouvy	nelze doporučit - důkazní břemeno - problém ověření podpisu - nezajistí integritu - nutná dohoda o uznávání	nelze doporučit - nutná dohoda o uznávání - problém ověření podpisu - nezajistí integritu	lze použít - rozsáhlá integrace do IS - zátěž při velkém objemu dokumentů - nutná dohoda o uznávání	lze použít - nutný souhlas o zpracování osobních informací - nutná dohoda o uznávání	nelze doporučit - nutný souhlas o zpracování osobních informací - nutná dohoda o uznávání	lze použít - nutná dohoda o uznávání - nelze vyžadovat po zákazníkovi	lze použít - avšak není rovnocenný úředně ověřenému podpisu
	mezi firmou a státní správou		nelze použít - není uznávaný el. podpis	nelze použít - není uznávaný el. podpis	nelze použít - není uznávaný el. podpis	nelze použít - není uznávaný el. podpis	nelze použít - není uznávaný el. podpis	nelze použít - není uznávaný el. podpis	lze použít.

Tabulka 2:Vhodnost variant el. podpisu pro případy komunikace

3.3 Představení společnosti CHOS

Chemická obchodní společnost s r.o. (dále také CHOS) byla založena v roce 1995 s cílem prodávat desinfekční a čisticí prostředky pro zemědělské podniky. Od konce roku 1996 až do současnosti se aktivně věnuje aplikaci nových technologií pro úpravu vody. Hlavním oborem je úprava vody ve všech průmyslových odvětvích, kde je voda nepostradatelnou součástí technologií, např. chemická úprava vody pro výrobu páry v energetice, potravinářství, dále stabilizace parametrů vody a ochrana proti růstu biologie v chladicích okruzích průmyslových výrob, např. chemického, farmaceutického, automobilového průmyslu, ale i ochrana proti korozi v topných okruzích nebo rozvodech dálkového vytápění, klimatizačních systémech budov apod. Zárukou spolehlivosti je zejména pravidelný servis navrženého způsobu ochrany vodních a parních systémů, vyhodnocení kvality ošetření a dosažených úspor na základě pravidelných provozních analýz, nastavení měřidel, regulačních a dávkovacích zařízení. (40)

Tým pracovníků je rozdělen na:

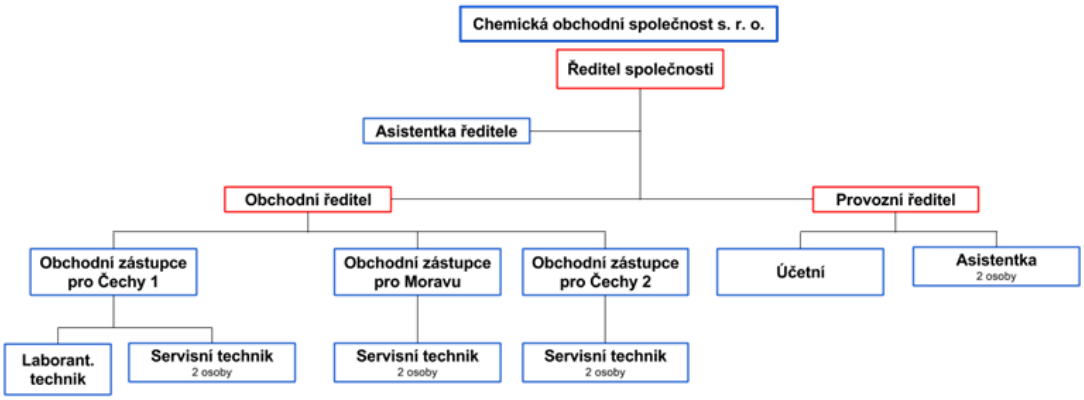
- obchodní a servisní oddělení;
- provozně ekonomické oddělení. (40)

Servisní technici pravidelně navštěvují své zákazníky s četností minimálně 1x za měsíc. Celý systém prodeje a servisu chemie pro úpravu průmyslových vod je podřízen potřebám zákazníků, kteří oceňují vysokou úroveň poskytovaných služeb a v neposlední řadě minimalizaci úkonů, které zákazník musí vykonávat. V současnosti má firma více než 250 zákazníků. (40)

Při servisní návštěvě provede technik CHOS všechny potřebné analýzy a stanovení koncentrace účinné látky v okruhu. Na základě naměřených hodnot doporučí další postup. O každé návštěvě je vypracována zpráva, tzv. Záznam o servisní návštěvě (dále také ZoSN), který je předán provozovateli. Tak je zaručen neustálý přehled o stavu ošetřovaného okruhu. (40)

3.3.1 Organizační struktura společnosti CHOS

Organizační strukturu společnosti CHOS tvoří obchodní a provozní oddělení.



Obrázek 3: Organizační struktura CHOS

Základní struktura obchodního oddělení má 4 úrovně, shora: ředitel, obchodní ředitel, obchodní zástupce (3 osoby), servisní technik (6 osob). Obchodní ředitel odpovídá za chod celého oddělení a jsou mu přímo podřízeni obchodní zástupci. Každému obchodnímu zástupci podléhají 2 servisní technici, kteří jsou orientováni na jim přidělený okruh zákazníků v určeném regionu České republiky.

Základní struktura provozního oddělení má 3 úrovně, shora: ředitel, provozní ředitel, účetní a asistentka (2 osoby). Provozní ředitel odpovídá za vnitřní chod firmy a jsou mu přímo podřízeni účetní a asistentky.

3.4 Představení společnosti GLOBIS

Společnost GLOBIS s.r.o. byla založena v roce 1996 a od roku 2005 se specializuje na systémové vzdělávání především v korporátní sféře. Dlouholeté zkušenosti z výuky promítají do tvorby vlastních e-learningových modulů. Pro podporu manažerské a personální práce vyvíjí praktické a užitečné aplikace a informační systémy. (41)

Hlavními obory, na které se společnost zaměřuje jsou:

- systémové školení, vzdělávání, koučink a poradenství;
- GEDU – software pro manažery a personalisty;
- optimalizace firemních procesů. (41)

Společnost Globis ve společnosti CHOS úspěšně zavedla systém GEDU, v tomto konkrétním případě pro interní komunikaci firmy, sledování postupů jednotlivých obchodních případů při získávání nových zakázek, evidenci a vyhodnocení servisních prací u stávajících zákazníků apod. V souvislosti s naposledy uvedenou funkcí

je potřeba pracovat s elektronickou verzí dokumentů, reportů ze servisních návštěv. Systém GEDU umožňuje přizpůsobit nastavení přesně potřebám firmy CHOS a obě firmy velice úzce spolupracují na jeho dalším vývoji. Vzájemná důvěra umožňuje poskytovat detailní zpětnou vazbu z praktických aplikací jednotlivých programových modulů GEDU. V kombinaci s vývojem informačních technologií společnost Globis udává směr při uplatňování efektivnějších postupů v každodenním chodu firmy.

3.5 Existující prostředky firmy CHOS pro prokázání původu dokumentů

V případech vysoké důležitosti dokumentů, jakými jsou pro firmu například zakladatelské listiny, společenská smlouva apod., se stále používá notářsky ověřený vlastnoruční podpis. Pro dokumenty v listinné podobě mezi firmou a státní správou je obvyklý úředně ověřený vlastnoruční podpis. S nástupem datových schránek se komunikace se státními orgány zjednodušuje. Důvěryhodnost komunikace zaručuje již samotné přihlášení firmy uživatelským jménem a heslem do systému datových schránek.

Písemná forma běžného obchodního styku CHOS s ostatními firmami probíhá dnes již převážně elektronickou cestou, tj. e-mailovou komunikací. Pro svou jednoduchost je prostý elektronický podpis používaný v e-mailové komunikaci tou nejvíce užívanou formou elektronického podpisu. V případě potřeby je přílohou e-mailu naskenovaná kopie dokumentu v listinné podobě s vlastnoručním podpisem autora a často i s otiskem firemního razítka. To považují obě strany v průběhu obchodní transakce za dostačující s tím, že originály smluv jsou následně zasílány v listinné podobě poštou.

Se čtečkou čipových karet žádný ze zaměstnanců firmy CHOS nepracuje, čtečky otisků prstů někteří z nich používají na svých počítačích pro přihlášení do uživatelského účtu operačního systému, o tabletu s dotykovým perem či biometrickými senzory se teprve uvažuje pro potřeby podepisování elektronických dokumentů v terénu.

3.6 Potřeby elektronického podpisu při komunikaci

3.6.1 Mezi zaměstnanci

Písemná komunikace zaměstnanců CHOS probíhá e-mailem či SMS zprávami. Za dostatečně průkaznou formu podpisu se bez zvláštních nároků považuje prostý elektronický podpis. Důvěryhodnost daného dokumentu je podpořena tím, že e-mail byl odeslán z e-mailové adresy zaměstnance.

Ve vnitřním informačním systému firmy je přístup jednotlivým osobám povolen na základě autentizace jejich uživatelským jménem a heslem. Dokumenty vytvořené zaměstnancem v tomto systému nemůže bez jeho souhlasu nikdo jiný změnit.

Dle mého zjištění tento případ komunikace změnu formy elektronického podpisu nevyžaduje.

3.6.2 Mezi firmami při servisní činnosti

Podstatou této písemné komunikace je nyní listinná podoba Záznamu o servisní návštěvě (Příloha 2), s vlastnoručními podpisy zástupců obou stran, tj. servisního technika CHOS a pověřeného zástupce zákazníka. Nevýhodou stávajícího zpracování ZoSN je listinná podoba tohoto dokumentu. Při další práci s informacemi v ZoSN je potřeba mnoho údajů znovu ručně přepisovat. Společnost CHOS nyní intenzivně spolupracuje s firmou Globis na vývoji systému elektronického zpracování ZoSN. Je zcela zřejmé, že elektronická podoba ZoSN vyžaduje i elektronický podpis zástupců obou stran, CHOS a zákazníka.

3.6.3 Mezi firmami při podpisu smlouvy

Statutární zástupce firem v současné době žádná legislativní úprava nenutí na stávajících zvyklostech něco měnit. To znamená, že navzdory současným technickým možnostem je pro podpis smluv stále využíván tradiční vlastnoruční podpis, razítko a zasílání smluv poštou. Uzavírání smluv není každodenní rutinou, smlouva se uzavírá cca 1x měsíčně. I to může být důvodem, proč elektronický podpis v této situaci prozatím uplatnění nenachází.

3.6.4 Mezi firmou a státní správou

Pro potřeby státní správy je dostatečnou zárukou samotná datová schránka. Už přihlášení firmy do systému datové schránky je pro státní správu dostatečně průkazné a žádný další druh ověření identity či původu dokumentů, např. prostřednictvím elektronického podpisu, již nevyžaduje.

Podle sdělení ekonoma společnosti, ve firmě CHOS byli nuceni používat elektronický podpis pouze v jednom případě, a to ve formě zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Jednalo se o komunikaci s finančním úřadem Slovenské republiky při vyúčtování daně z přidané hodnoty. Pro další období již nebylo potřeba si certifikát pro elektronický podpis obnovovat, české úřady elektronický podpis nepožadují.

3.6.5 Shrnutí v tabulce

Komunikace		**potřeby elektronického podpisu**
mezi zaměstnanci		ne
mezi firmami	při servisní činnosti	ano – elektronický podpis dokumentu ZoSN
	při podpisu smlouvy	ne
mezi firmou a státní správou		ne.

Tabulka 3: Shrnutí zjištěných potřeb el. podpisu

3.7 Záznam o servisní návštěvě – ZoSN

Aby bylo možné určit a doporučit optimální formu elektronického podpisu pro potřeby ZoSN, bylo nezbytné podrobně zmapovat proces zpracování tohoto dokumentu ve firmě CHOS. Mám tím na mysli informace o tom, kdo všechno s dokumentem pracuje a kdo dokument podepisuje.

Jedná se o arch předtištěného průpisového papíru formátu A4, který je schopen tvořit 2 kopie (3 stránky A4 – originál, kopie 1 a kopie 2). Dokument slouží jako:

- doklad o servisní návštěvě technika společnosti, o výsledcích analýzy odebraných vzorků vod a o další servisní práci pro zákazníka s doporučením pro další provoz úpravny vody;
- výkaz o pracovní činnosti servisního technika pro vnitřní potřebu společnosti CHOS.

3.7.1 Proces zpracování dokumentu – ZoSN

Do procesu záznamu o servisní návštěvě jsou zapojeni pracovníci obchodního oddělení a také asistentka z provozního oddělení společnosti CHOS. Detailní postup je zdokumentován v procesním diagramu v Příloze č. 1. Diagram jsem zpracoval především proto, abych se ujistil, že jsem správně porozuměl výkladu vedení společnosti CHOS.

Sestava plánu servisních návštěv

Servisní technik si pomocí informačního systému sestaví na každý týden plán servisních návštěv. V informačním systému GEDU pak u zákazníků, které hodlá daný týden navštívit, vytvoří činnost *„Servisní návštěva u zákazníka“*.

Dále si servisní technik na každou servisní návštěvu k zákazníkovi ze své vlastní evidence připraví několik ZoSN z minulých návštěv u zákazníka, aby měl informace o stavu po poslední návštěvě u zákazníka. Tyto připravené záznamy vozí s sebou k zákazníkovi.

Vyplnění dokumentu ZoSN

Během každé servisní návštěvy servisní technik vyplňuje ZoSN. Jedná se především o položky jako obchodní jméno zákazníka, aktuální stav zařízení, výsledky chemické analýzy vod, nastavení dávkovacích čerpadel a následně hodnocení stavu, případně návrh opatření.

Důležitá je vzájemná zastupitelnost servisních techniků. Může se stát, že je potřeba poslat k zákazníkovi na servis technika z jiného regionu, např. o dovolených. A také se může stát, že žádný servisní technik nebude volný a pojede za něho udělat servis kdokoli z nadřízených, tj. některý z obchodních zástupců.

Podpis dokumentu ZoSN

Vyplněný ZoSN podepisuje za stranu společnosti CHOS ten, kdo ho vypracoval. To může být servisní technik či zastupující servisní technik nebo některý z obchodních zástupců.

Dále servisní technik předkládá ZoSN k podpisu zástupci zákazníka. U podpisu je vždy čitelně uvedeno jméno a příjmení podepsané osoby. Tou bývá většinou vedoucí provozu (jinak také vedoucí údržby, chlazení nebo kotelny). Vedoucí provozu je většinou stěžejní a kontaktní osobou ve smluvním vztahu mezi společností CHOS a zákazníkem. Svým podpisem vyplněného ZoSN potvrzuje převzetí servisních prací, dodaného materiálu a časový průběh servisní návštěvy. V době nepřítomnosti vedoucího daného provozu podepisuje ZoSN pracovník z obsluhy zařízení daného provozu. Kdo to je, závisí většinou na dané směně v tomto provozu a není to ani nijak smluvně definované, jde spíše o individuální domluvu se zákazníkem a dále už to závisí na vnitřní organizaci společnosti zákazníka, kdy obsluha zařízení předá kopii ZoSN vedoucímu provozu.

Distribuce dokumentu ZoSN

Po vyplnění a podepsání ZoSN oběma stranami předá servisní technik jednu kopii ZoSN zástupci zákazníka. Druhou kopii ZoSN si servisní technik zařadí do své vlastní evidence. Originál ZoSN servisní technik naskenuje do elektronické formy, většinou formátu PDF, tento soubor nahraje do informačního systému GEDU a přiřadí ho k příslušné činnosti *„Servisní návštěva u zákazníka“*. Originály ZoSN v papírové formě je servisní technik povinen odeslat jednou týdně poštou na adresu sídla společnosti CHOS.

Archivace a přepis do databáze

Nyní do procesu dokumentu vstupuje asistentka z provozního oddělení společnosti. Ta pracuje s naskenovaným originálem ZoSN, protože ten bývá v rámci informačního systému k dispozici dříve. Asistentka přepisuje údaje ze ZoSN do databáze a jakmile jsou poštou doručeny originály dokumentů, zakládá je do příslušných šanonů k archivaci.

Další využití ZoSN

Servisními techniky vyplněné ZoSN kontrolují jejich nadřízení – obchodní zástupci, aby měli přehled o situaci v ošetřovaných provozech. Tato činnost však obchodní zástupce velmi zatěžuje, protože musí jednotlivě procházet mnoho servisních záznamů. Každý servisní technik uskuteční cca 30 až 35 servisních návštěv za měsíc, na jednoho obchodního zástupce tedy vychází kontrola cca 70 servisních záznamů měsíčně.

V případě řešení nějakého problému, reklamace či prosté konzultace stavu servisovaného systému se zákazníkem je obvykle potřeba dohledat a připravit ZoSN za posledních 6 až 12 měsíců. Z těchto ZoSN připravuje pověřený obchodní zástupce report pro zákazníka. Při současném stavu to znamená obvykle půldenní přípravu před jednáním se zákazníkem.

3.7.2 Elektronická podoba dokumentu ZoSN

Výsledkem diskuze s vedením CHOS a Globis jsou parametry procesu zpracování ZoSN v elektronické podobě.

Vnitřní informační systém CHOS bude rozšířen o databázové rozhraní, do kterého budou zadávány výsledky analýz prostřednictvím formulářové aplikace. Servisní technik bude vybaven odpovídajícím hardwarem pro online přístup k formulářové aplikaci. V průběhu servisní návštěvy tak bude moci zapisovat výsledky provozních analýz vzorků odebraných vod, provedené práce a doporučení pro další provoz. Na závěr servisní návštěvy technik CHOS vytvoří stiskem tlačítka ve formulářové aplikaci elektronickou podobu ZoSN ve formátu PDF. Tento dokument předloží k podpisu zástupci zákazníka a následně ho sám elektronicky podepíše. Podepsaný dokument servisní technik nahraje zpět do informačního systému, který ho obratem automaticky odešle e-mailem k zákazníkovi.

3.8 Návrh řešení elektronického podpisu ZoSN

Z analýzy procesu elektronického dokumentu vyplývá, že za stranu zákazníka se v celkovém odhadu jedná o poměrně velkou skupinu lidí, kteří potenciálně budou ZoSN podepisovat. Jejich počet jsem stanovil podle následujícího výpočtu:

35 ZoSN za měsíc x 6 servisních techniků x 5 osob na zákazníka = 1050 osob

Lze předpokládat, že s dalším rozvojem firmy bude zákazníků přibývat. V následujících třech kapitolách postupně shrnuji klady a zápory porovnávaných způsobů elektronického podpisu, z mého pohledu, z pohledu dodavatelské firmy CHOS a z pohledu poskytovatele informačního systému. Konečné řešení bylo vybráno po zhodnocení všech dostupných řešení při společné diskuzi všech zúčastněných stran.

3.8.1 Zhodnocení jednotlivých řešení el. podpisu ZoSN zástupci CHOS a Globis

Následující tabulka č. 4 shrnuje subjektivní pohled firmy na praktické využití jednotlivých druhů elektronického podpisu, jak jsem je zaznamenal v průběhu osobních rozhovorů se zástupci CHOS a Globis. Základními kritérii CHOS jsou pořizovací náklady technologie a průkaznost podpisů v případě sporu se zákazníkem. Poradním hlasem CHOS byl zástupce firmy Globis, zejména z důvodu navazující implementace elektronického dokumentu a podpisu do informačního systému.

Č.	Způsob elektronického podepisování	pro	proti	posouzení vhodnosti
1	napsání jména v el. dokumentu	-nejjednodušší způsob -nulové náklady	-nízká důvěryhodnost -těžká průkaznost v případě sporu -chybí obrázek podpisu	pro předání ZoSN nedostatečné
2	sejmutí rukou psaného podpisu bez biometriky	-jednoduché vytvoření podpisu -příznivá pořizovací cena zařízení	-vybavit technika grafickým tabletem či notebookem s dotykovým displejem -nedostatečná průkaznost dokumentu a podpisu v případě sporu	-sám o sobě je nedostatečný -je potřeba ho podpořit dalšími důkazy -nutno doplnit o čitelnou podobu jména a příjmení
3	kliknutím *„click-wrap“*	-rychlé -uživatelsky přívětivé -zaznamená systémový čas vytvoření podpisu	-zatížení IS (velký počet ZoSN) -nepoužitelné pro podpis zákazníka (nemá identitu v IS)	nepoužitelné
4	DBP pomocí specializovaného zařízení	-vyšší průkaznost podpisu -uživatelsky nejblíže vlastnoručnímu podpisu -zaznamená systémový čas vytvoření podpisu	-vyšší pořizovací cena -zpracování citlivých dat, zejména zákazníků	-první samostatně dostatečně průkazná varianta podpisu -použitelný s písemným souhlasem podepisujícího zástupce zákazníka
5	pomocí otisku prstu	-rychlé -dobrá průkaznost porovnáním biometrických dat -zaznamená systémový čas vytvoření podpisu	-zpracování citlivých dat -nepříjemné pro zákazníka -vyžaduje čtečku otisků prstů	-v praxi nepoužitelné -nutno doplnit o čitelnou podobu jména a příjmení
6	pomocí čipové karty či USB tokenu + uznávaný el. podpis	-výborná průkaznost podpisu a celého dokumentu -zaznamená systémový čas vytvoření podpisu	pořizovací náklady -čipová karta + čtečka, tj. cca 800 Kč -USB token cca 700 Kč -možnost ztráty nosného média -certifikát cca 400 Kč/rok	-dobré řešení pro techniky CHOS -pro zákazníky příliš komplikované řešení
7	pomocí úložiště certifikátů Windows + uznávaný el. podpis	-není potřeba žádné další zařízení -zaznamená systémový čas vytvoření podpisu	pořizovací náklady certifikát cca 400 Kč/rok	-dobré řešení pro techniky CHOS -pro zákazníky příliš komplikované řešení.

Tabulka 4: Zhodnocení jednotlivých řešení el. podpisu ZoSN zástupci CHOS a Globis

3.8.2 Řešení elektronického podpisu ZoSN

Díky všem získaným podnětům mohu nyní z variant, které se jeví jako přípustné, vybrat nejvhodnější řešení. Po analýze procesu zpracování ZoSN mohu nyní posoudit klady a zápory jednotlivých variant jak pro podpis zaměstnance CHOS, tak i pro podpis zástupce zákazníka.

Ukázalo se, že je velmi obtížné použít stejnou variantu podpisu pro technika CHOS i pro zákazníka. Při konzultacích se zástupci firmy CHOS se nám nepodařilo vybrat takový průnik variant, resp. jeden druh podpisu, který by byl pro obě smluvní strany použitelný v praxi. Pro potřeby firmy CHOS jsou dle daných kritérií, co do zajištění průkaznosti podpisu a dokumentu, nejvhodnější varianty 6 a 7. V současné době však stále není běžné od zaměstnanců v provozech zákazníků takovou formu elektronického podpisu vyžadovat. Pro potřeby ZoSN jsou pro zákazníka přijatelné varianty podpisu č. 2, v kombinaci s variantou č. 1, tj. grafická + tištěná podoba podpisu, nebo varianta č. 4.

Jako řešení, které je schopné nejlépe zajistit integritu daného dokumentu a obhájit v případě sporu průkaznost podpisů osob vstupujících do procesu daného dokumentu, se jeví kombinace dvou druhů elektronického podpisu. Pro podpis zaměstnance CHOS použít uznávaný elektronický podpis (vytvořený pomocí USB tokenu či úložiště certifikátů Windows) a pro podpis zástupce zákazníka použít dynamický biometrický podpis získaný pomocí speciálního podpisového padu.

Avšak nasazení této kombinace podpisů pro účely ZoSN brání skutečnost, že pro potřeby firmy CHOS není zcela optimálním řešením. Dynamický biometrický podpis (č. 4) má své nesporné přednosti, ale při jeho vytváření se automaticky zpracovávají citlivé osobní údaje, vyžaduje výslovný písemný souhlas se zpracováním osobních údajů od všech zaměstnanců každého zákazníka, kteří budou ZoSN takto podepisovat. Získávání souhlasu zaměstnanců zákazníka, spolu s plněním dalších povinností obecného nařízení o ochraně osobních údajů, Nařízení GDPR (39), a s vynaložením prostředků na technické vybavení pro snímání DBP, představuje pro firmu nemalou zátěž, které by se pochopitelně nejraději vyhnula.

Jinak je tomu například v případě bank nebo pojišťoven, které DBP využívají pro podpis zákazníka, který je přímou osobou, se kterou mají uzavřenou smlouvu

a není proto tak složité tuto smlouvu rozšířit o výslovný souhlas a další právní náležitosti, např. zákazník jako subjekt údajů musí být informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období, také o právu na přístup k informacím o zpracování, přičemž správce tento souhlas musí být schopen prokázat po celou dobu zpracování. (42)

Jako výsledné řešení byla proto zvolena kombinace uznávaného podpisu pro zaměstnance CHOS a sejmutí vlastnoručního podpisu bez biometriky pro podpis zástupce zákazníka. Absence zpracování osobních údajů a také dostupnější technologie je nyní naopak výhodou. Grafická podoba vlastnoručního podpisu může být nasnímána pomocí dotykového displeje, grafického tabletu či podpisového padu bez biometrie. Integrita takto podepsaného dokumentu bude ošetřena uznávaným podpisem zaměstnance. Autenticita druhého podpisu bude podpořena doplněním čitelné podoby jména autora podpisu a také skutečností, že dokument ZoSN bude ihned po podepsání oběma stranami automaticky odeslán na kontaktní e-mail zákazníka a bude vyžadováno potvrzení o přečtení. Datum odeslání e-mailu se bude shodovat s datem vyplněným v záhlaví ZoSN a s datem obsaženým v uznávaném elektronickém podpisu zaměstnance CHOS.

Dohoda mezi stranami o uznávání takové formy podpisu ve svém obchodním vztahu bude zakotvena v rámcové servisní smlouvě, kterou firma CHOS se svými zákazníky uzavírá na začátku každé dlouhodobější spolupráce. Taková dohoda je mnohem jednodušší, než získávání výslovného souhlasu i samotné zpracování osobních informací od zaměstnanců zákazníka (viz Příloha 3 – Doplnění servisní smlouvy).

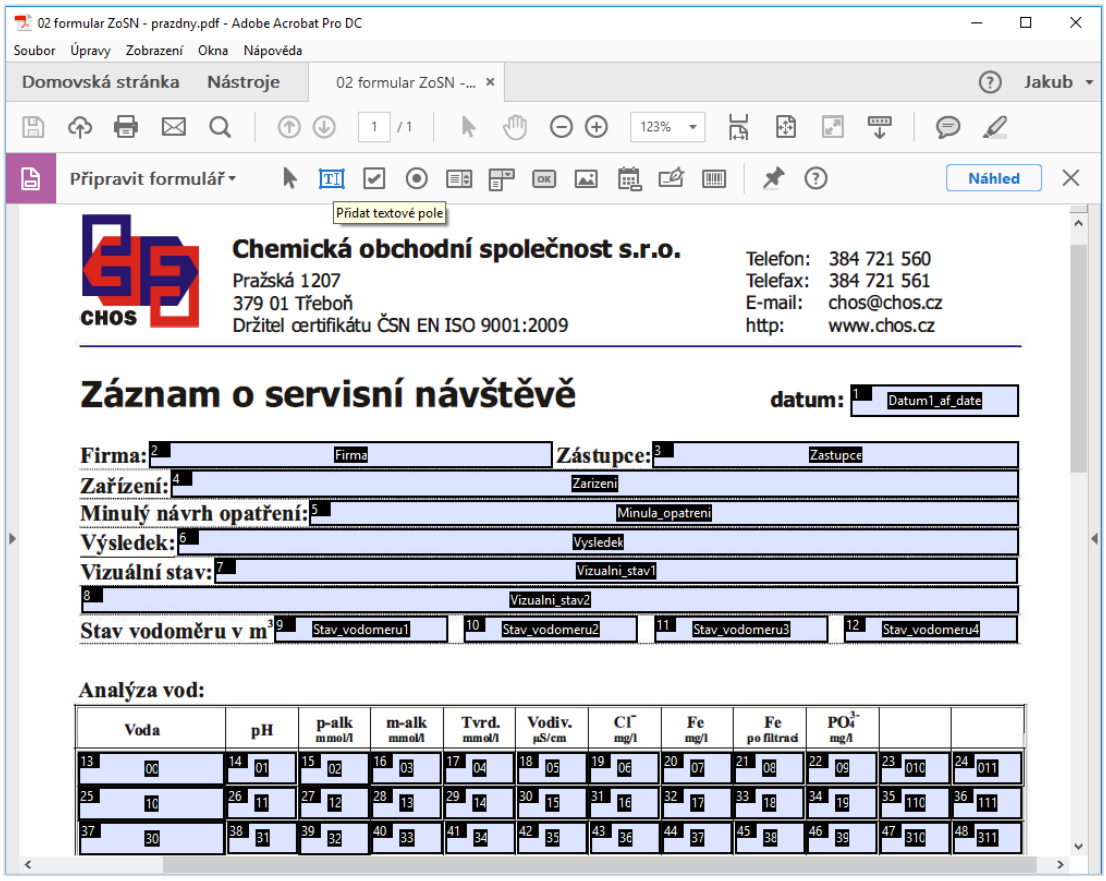
3.9 Proof-of-concept

V této kapitole je popsáno ověření funkčnosti navrhovaného řešení elektronického podepisování v praxi, které jsem provedl vytvořením funkčního modelu, tzv. proof-of-concept. Záměrem je prokázat využitelnost návrhu a prozkoumat jeho případné další praktické aspekty. Proveden je podpis elektronické verze dokumentu ZoSN sejmutím vlastnoručního podpisu pomocí grafického tabletu připojeného k notebooku, jenž simuluje použití podpisového padu nebo malého notebooku s dotykovým displejem. Následně je přidán uznávaný elektronický podpis vytvořený jak pomocí USB tokenu, tak i pomocí certifikátu a soukromého klíče v úložišti certifikátů

Windows. Kromě toho jsou v této kapitole popsány postupy získání a instalace navrhovaných forem elektronického podpisu.

3.9.1 Vytvoření formulářové verze dokumentu ZoSN

Za účelem realizace funkčního modelu řešení jsem z původní písemné verze ZoSN, úpravou struktury a vytvořením formulářových polí v programu Adobe Acrobat Pro, zhotovil elektronickou verzi ZoSN v podobě formulářového dokumentu formátu PDF (dále jako elektronický formulář ZoSN). S tímto elektronickým formulářem ZoSN je možné pracovat podobně jako s plánovanou formulářovou aplikací informačního systému firmy a jelikož odpovídá potřebám původní verze ZoSN, lze si práci s ním vyzkoušet, včetně navrhovaného řešení podepisování i přímo v terénu. Na obr. 4 je ukázka vytváření elektronického formuláře ZoSN v editoru formulářových polí programu Adobe Acrobat Pro (celý formulář ZoSN s vytvořenými vyplňovacími poli je k nahlédnutí v Příloze 4).



Obrázek 4: Vytvoření formulářové verze dokumentu ZoSN

Ve spodní části elektronického formuláře ZoSN se nachází místo pro podpisy (viz obr. 5). Podpisu zástupce zákazníka je vyhrazeno místo u kolonky *„Převzal:“* a pod ním je pole pro čitelnou podobu jména zástupce zákazníka, které před podpisem dokumentu vyplní servisní technik CHOS. Místo u kolonky *„Vypracoval:“* je určené pro podpis zaměstnance CHOS a zde jsem umístil speciální pole pro elektronický podpis, takže po kliknutí na toto pole se v prohlížeči PDF automaticky zahájí proces elektronického podepisování a spustí se průvodce vytvořením elektronického podpisu.

Obrázek 5: Detail řešení podpisů el. formuláře ZoSN

3.9.2 USB token – získání kvalifikovaného certifikátu pro elektronický podpis

Jelikož mě zaujala nabídka poskytovatele služeb vytvářejících důvěru PostSignum, rozhodl jsem se pořídit si kvalifikovaný certifikát pro elektronický podpis spolu s kvalifikovaným prostředkem pro vytváření elektronického podpisu pro testování elektronického podepisování v praxi. Kvalifikovaný prostředek aktuálně dodávaný službou PostSingum je USB token TokenME, což je PKI token postavený na kryptografickém mikroprocesoru s certifikací Common Criteria EAL4+ a FIPS 140-2 level 3.

Pro získání osobního kvalifikovaného certifikátu pro elektronický podpis je zapotřebí uskutečnění následujících kroků:

1. Vyplnit smlouvu s Českou poštou, s. p., o poskytování certifikačních služeb. Dále ještě vyplnit formulář s údaji pro vydání certifikátů. Oba dokumenty lze získat na internetových stránkách služby PostSignum.
2. Vygenerování elektronické žádosti o certifikát pomocí programu iSignum, který je dostupný ke stažení rovněž na stránkách PostSignum.
3. Dostavit se osobně na pobočku České pošty, s. p., se službou Czech POINT, spolu s vyplněnými dokumenty, dvěma osobními doklady totožnosti a s vygenerovanou elektronickou žádostí o certifikát na USB flash paměti,

nebo s identifikačním číslem této žádosti, kterou pak pracovnice pobočky vyhledá v interním systému.

4. Po ověření a vyřízení všech potřebných náležitostí na pobočce je následně, téměř obratem, certifikát žadateli vydán a je zaslán na žadatelovu uvedenou e-mailovou adresu.
5. Posledním krokem je instalace vydaného certifikátu do systému nebo programu, kde se chceme elektronicky podepisovat.

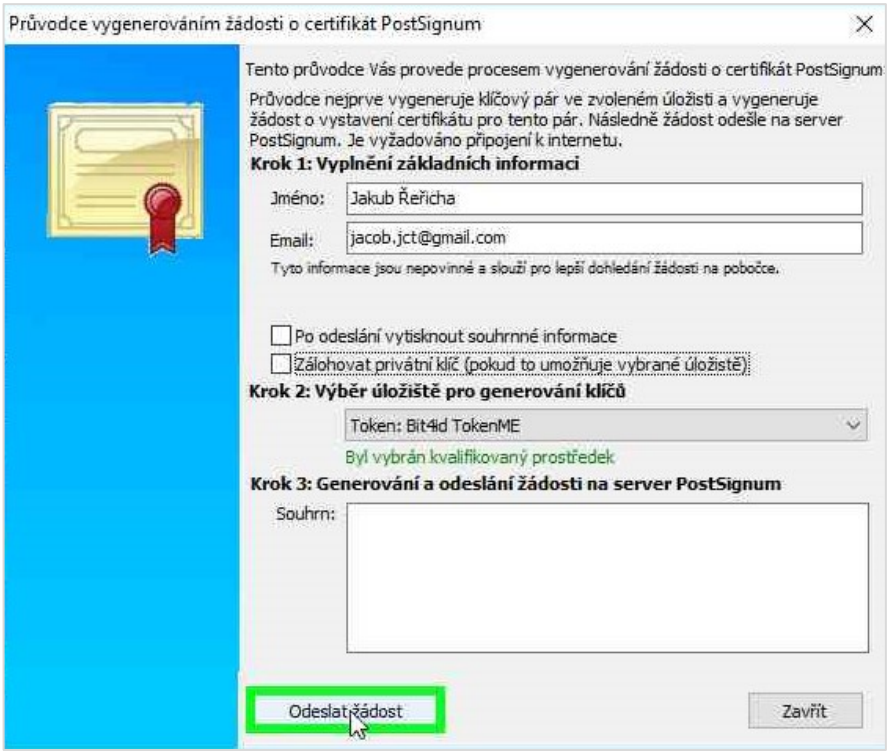
Generování elektronické žádosti o certifikát

Před vlastním generováním žádosti je nutné nainstalovat ovladače dodávané k USB tokenu a podle příslušné uživatelské příručky provést přípravu tokenu pro generování klíčů. Ta zpravidla spočívá ve změně implicitních kódů PIN a PUK za vlastní.

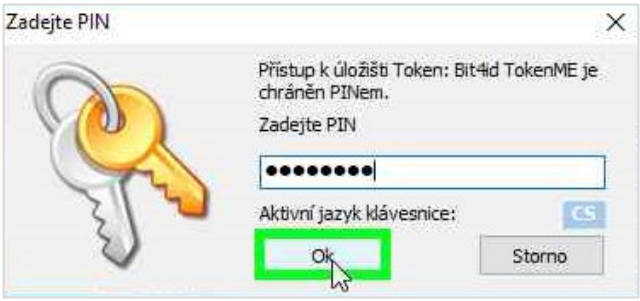
Když je USB token připraven, ujistíme se, že je vložen do USB portu počítače. Spustíme program iSignum. Průvodce vygenerováním žádosti otevřeme kliknutím na tlačítko *„Nový“* (obr. 6).

Obrázek 6: Spuštění průvodce vygenerováním žádosti

V průvodci vyplníme jméno a e-mailovou adresu, zkontrolujeme také, že jako úložiště pro generování klíčů je nastaven námi požadovaný USB token. Dále je nutné stisknout tlačítko *„Odeslat žádost“* (obr. 7, str. 44). Generování klíčů a žádosti je třeba potvrdit zadáním kódu PIN (obr. 8, str. 44).

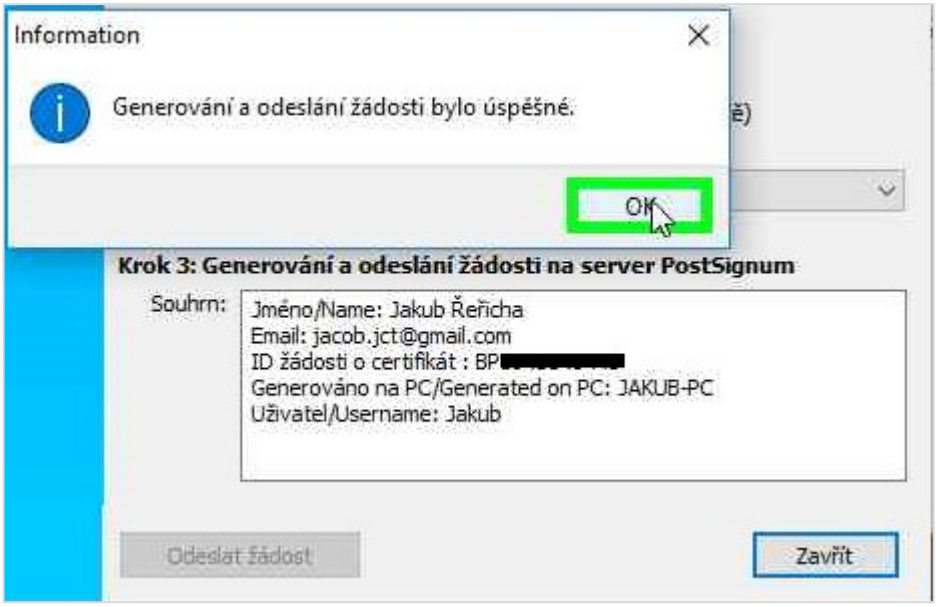


Obrázek 7: Odeslání vyplněné žádosti



Obrázek 8: Autorizace generování klíčů a žádosti kódem PIN

Po vygenerování klíčů a žádosti o certifikát je navázána komunikace se systémem certifikační autority PostSignum, kam je žádost o certifikát bezpečně předána. Za předpokladu, že vše proběhne v pořádku, program vrátí identifikační číslo žádosti, které je posléze možné použít na pobočce České pošty, s. p., při procesu vydání certifikátu (obr. 9, str. 45).



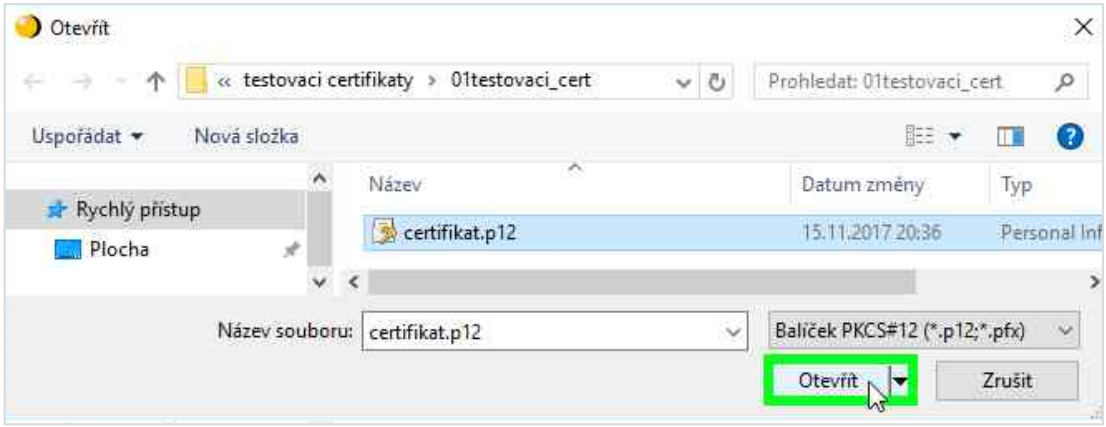
Obrázek 9: Úspěšné generování žádosti

Instalace certifikátu

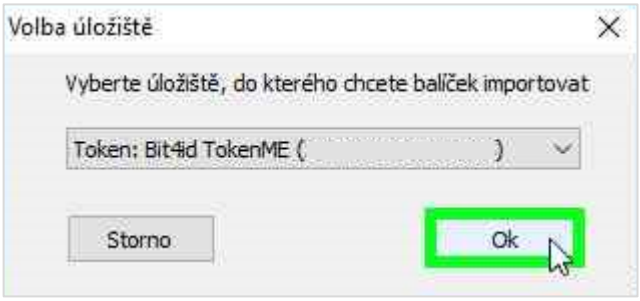
Instalaci vydaného certifikátu provedeme rovněž prostřednictvím aplikace iSignum. USB token musí být opět vložen do USB portu počítače, poté v programu iSignum klikneme na tlačítko *„Importovat“* (obr. 10).

Obrázek 10: Zahájení instalace certifikátu

V otevřeném dialogovém okně vybereme certifikát, který chceme nainstalovat (obr. 11, str. 46), a v dalším kroku zvolíme cílové úložiště, do kterého se certifikát nainstaluje, v tomto případě je to USB token (obr. 12, str. 46).

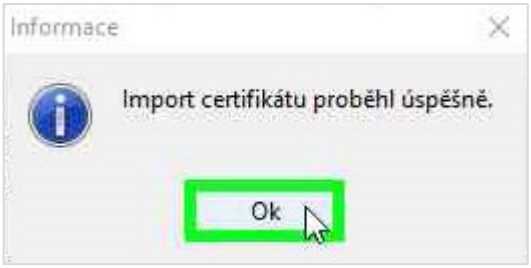


Obrázek 11: Výběr instalovaného certifikátu



Obrázek 12: Volba cílového úložiště certifikátu

Nakonec je nutné instalaci certifikátu autorizovat kódem PIN a pokud operace proběhne úspěšně, zobrazí se příslušné oznámení (obr. 13). Nyní už se můžeme elektronicky podepisovat.



Obrázek 13: Úspěšný import certifikátu

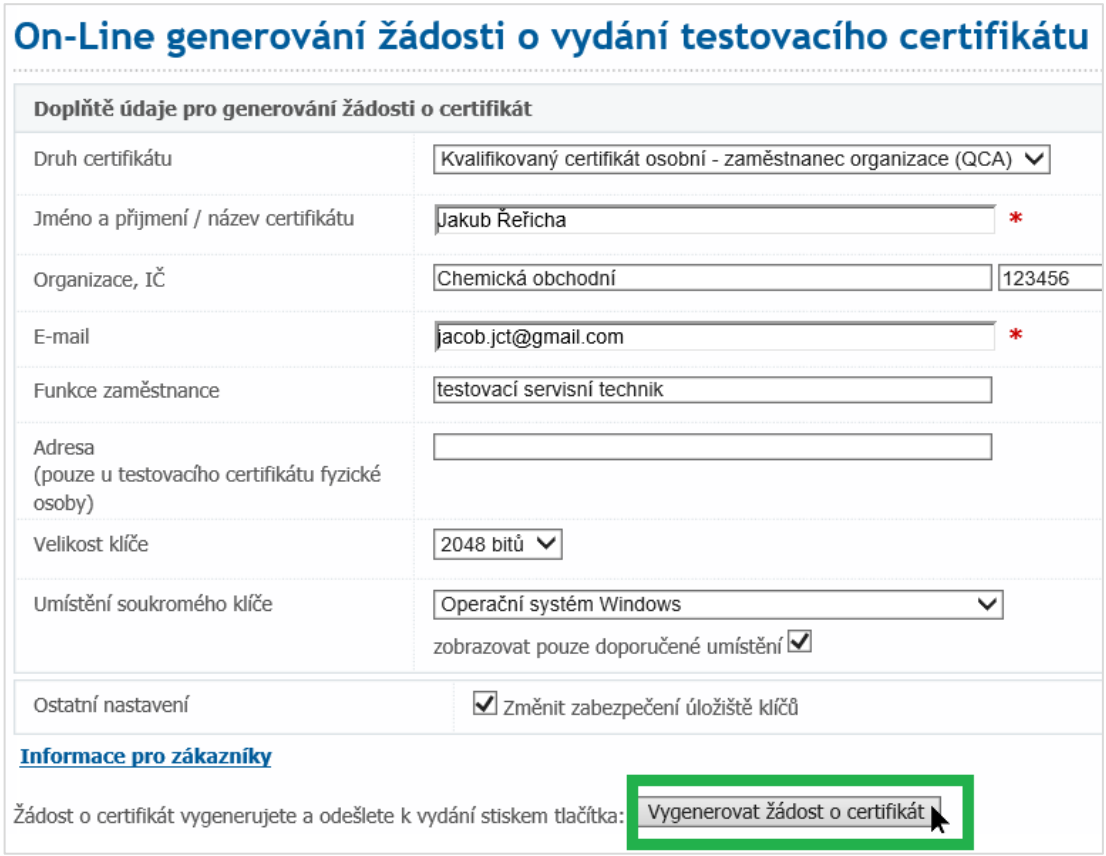
3.9.3 Úložiště certifikátů Windows – testovací kvalifikovaný certifikát

Pro ověření funkčnosti elektronického podpisu pomocí úložiště certifikátů Windows se nabízí využít testovacího certifikátu vydávaného službou PostSignum s platností 30 dní. Žádost o vydání certifikátu je možné provést nejsnáze v internetovém

prohlížeči on-line nástrojem generování žádosti o vydání testovacího certifikátu na webu služby PostSignum.

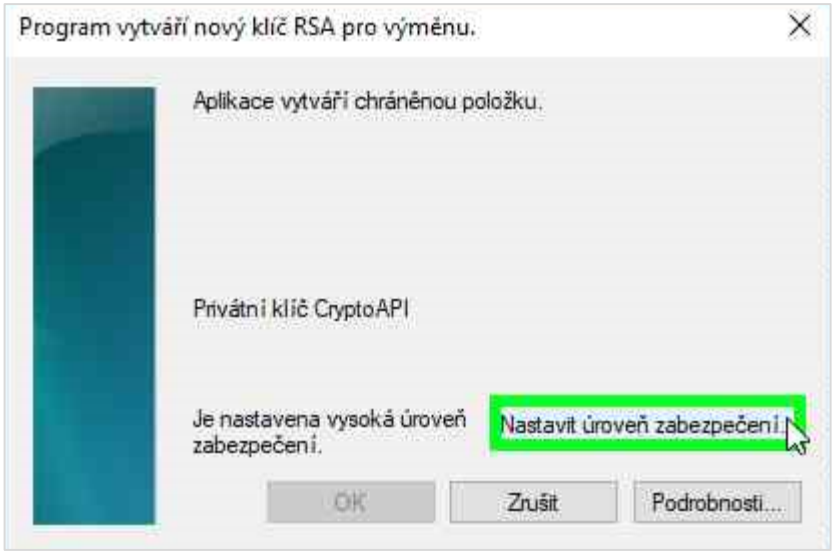
On-line generování žádosti o testovací certifikát

Nejprve nutné vyplnit údaje pro generování žádosti, povinné je vyplnit pouze jméno, příjmení a e-mail. Také je potřeba vybrat druh certifikátu a umístění soukromého klíče, v tomto případě jde o kvalifikovaný certifikát zaměstnance organizace a operační systém Windows (obr. 14). Zaškrtnutím položky *„Změnit zabezpečení úložiště klíčů“* nastavíme vysokou úroveň zabezpečení uložení klíčů, při této volbě nás systém vybídne k nastavení hesla, které bude vyžadovat při každém využití daných klíčů, tj. při každém vytváření podpisu. Po vyplnění žádosti pokračujeme kliknutím na tlačítko *„Vygenerovat žádost o certifikát“*.



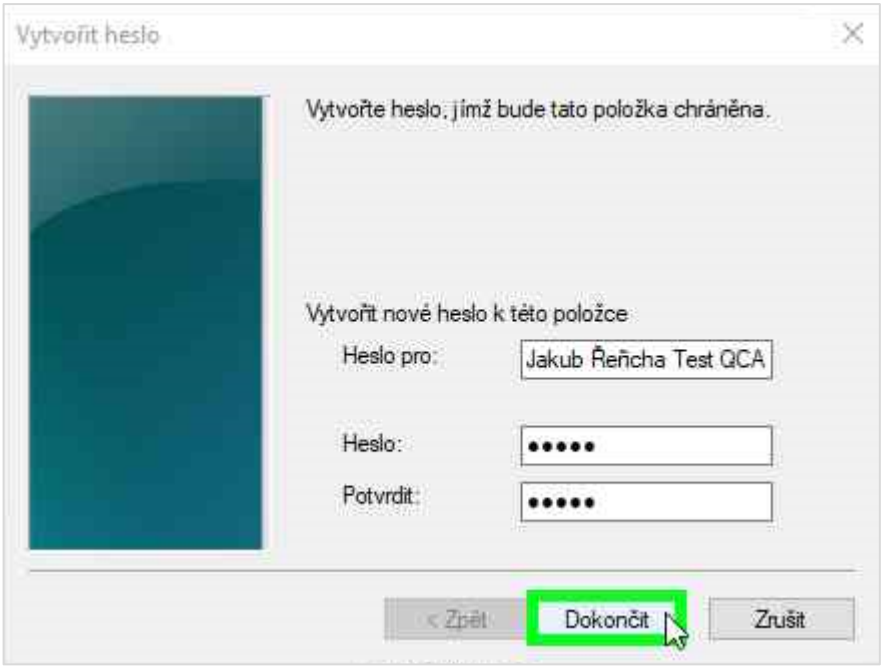
Obrázek 14: On-line generování žádosti o certifikát

Nástroj generování žádosti vyvolá systémový program pro vytvoření nového klíče RSA. Předtím je ale nutné nastavit heslo, kliknutím na tlačítko *„Nastavit úroveň zabezpečení“* (obr. 15, str. 48).



Obrázek 15: Vytvoření nového klíče RSA

V následujícím okně (obr. 16) vyplníme námi požadovaný název vytvářeného prostředku pro vytvoření elektronického podpisu a požadované heslo a vše potvrdíme tlačítkem *„Dokončit“*, čímž se vrátíme na předešlou obrazovku (obr. 15), kde klikneme na již aktivní tlačítko *„Ok“*.



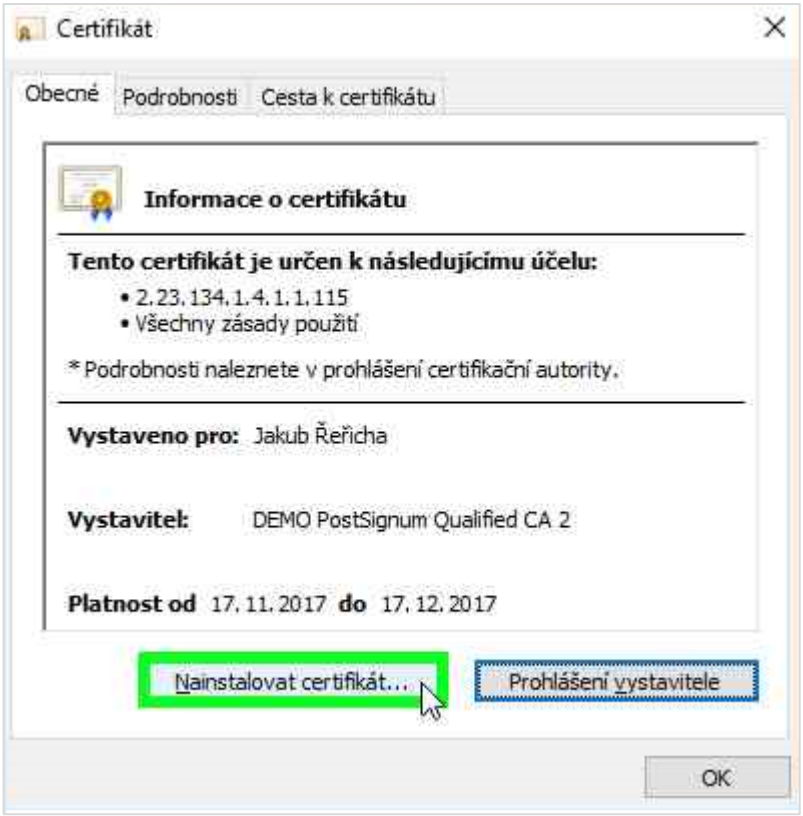
Obrázek 16:Nastavení hesla pro zabezpečení

Program posléze vytvoří klíč RSA, vygeneruje a odešle žádost o certifikát. Vydaný testovací certifikát zašle služba PostSignum na zadanou e-mailovou adresu během následujících 30 minut.

Instalace certifikátu do úložiště Windows

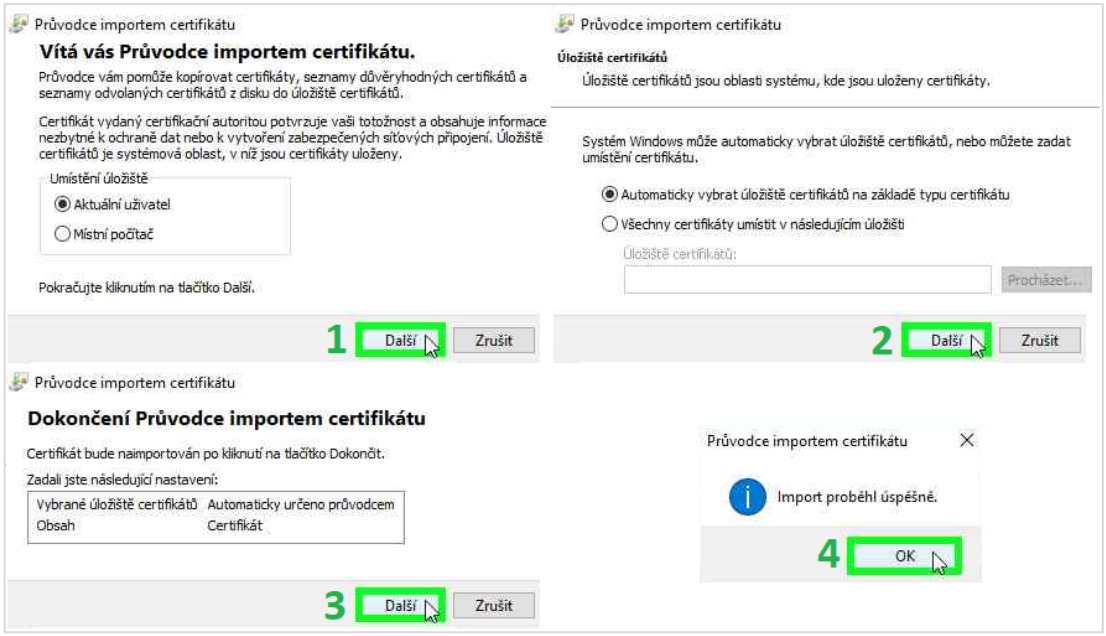
Po obdržení e-mailu s vydaným testovacím certifikátem je možné ho nainstalovat. Pro správné fungování testovacího certifikátu je nutné nainstalovat také certifikáty certifikační autority *„DEMO PostSignum“*, které jsou rovněž součástí přílohy e-mailu. Instalace certifikátů certifikační autority se provádí stejným způsobem jako instalace vydaného testovacího certifikátu, která je popsána v této kapitole.

Soubor s vydaným certifikátem má příponu `.crt`. Abychom mohli certifikát nainstalovat, nejprve tento soubor uložíme z e-mailu do počítače. Soubor spustíme dvojitým poklepáním, otevře se okno s certifikátem, kde můžeme zkontrolovat obsah certifikátu a následně spustit instalaci certifikátu kliknutím na tlačítko *„Nainstalovat certifikát“* (obr. 17).



Obrázek 17: Zahájení instalace certifikátu

Dále můžeme pokračovat podle pokynů průvodce importem certifikátu (obr. 18, str. 50). Nejdříve provedeme výběr uživatele, jehož úložiště má být použito, následuje výběr úložiště certifikátů, v dalším kroku zkontrolujeme předchozí dvě volby a stisknutím tlačítka *„Další“* potvrdíme operaci instalace certifikátu. Pokud operace proběhne úspěšně, zobrazí se příslušné oznámení a stiskneme tlačítko *„Ok“*.



Obrázek 18: Postup průvodcem importu certifikátu

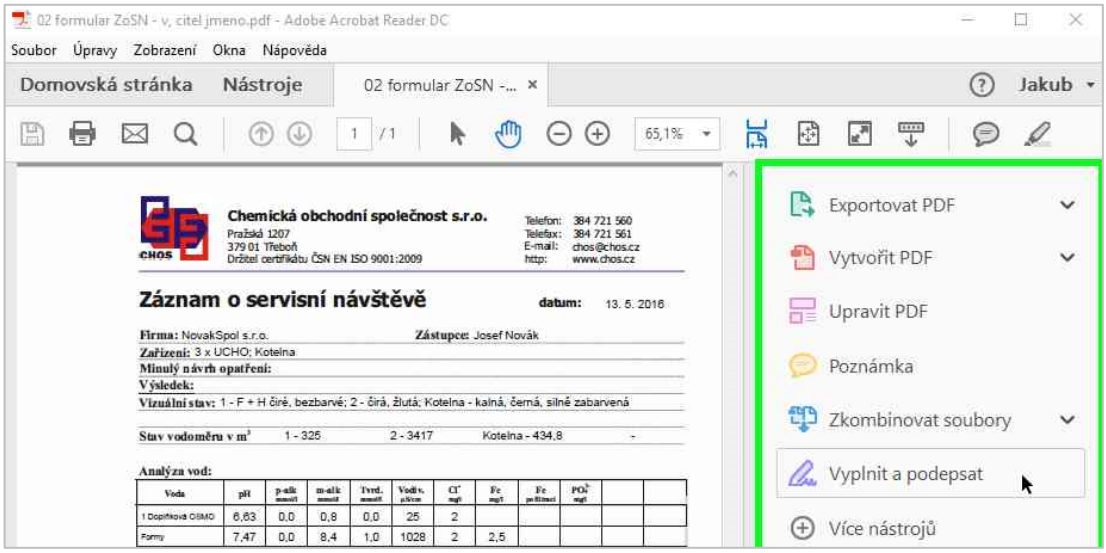
3.9.4 Vyplnění a podepsání elektronického formuláře ZoSN

V průběhu servisní návštěvy servisní technik CHOS zaznamenává zjištěné poznatky a výsledky chemických analýz do elektronického formuláře ZoSN pomocí malého notebooku s operačním systémem Windows. Zpracování formuláře ZoSN probíhá v běžném prohlížeči dokumentů PDF Adobe Acrobat Reader DC (dále také jako Acrobat Reader). Tato kapitola popisuje sled kroků vedoucích k podepsání vyplněného elektronického formuláře ZoSN.

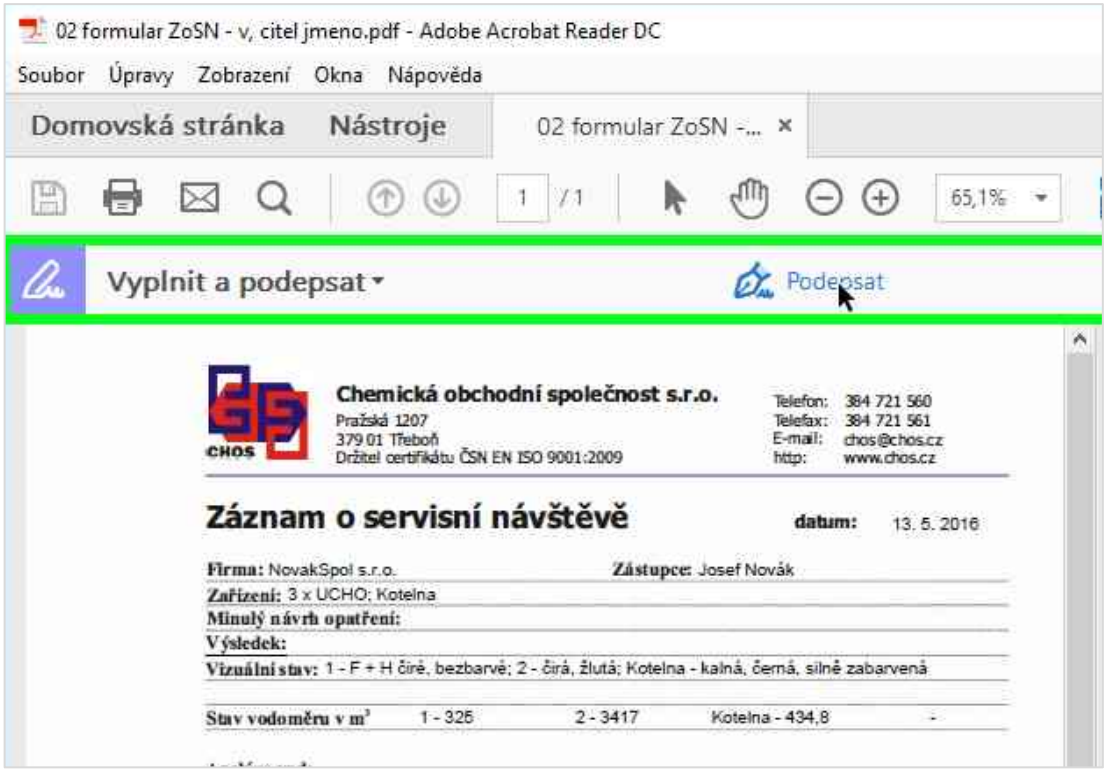
Servisní technik poskytne vyplněný formulář k nahlédnutí zástupci za stranu zákazníka a seznámí ho s obsahem dokumentu. Servisní technik zapíše do formuláře celé jméno podepisujícího zástupce za stranu zákazníka. Příslušné pole pro čitelnou podobu jména zástupce zákazníka je umístěno pod místem pro grafickou podobu vlastnoručního podpisu, ve spodní části dokumentu (obr. 19, str. 51).

Obrázek 19: Čitelné jméno zástupce zákazníka

Následně servisní technik zahájí proces vytvoření podpisu zástupce zákazníka výběrem nástroje programu Acrobat Reader *„Vyplnit a podepsat“* (obr. 20) a pokračuje kliknutím na tlačítko *„Podepsat“* (obr. 21, str. 52).



Obrázek 20: Vyplnit a podepsat



Obrázek 21: Podepsat

Kliknutím na tlačítko *„Podepsat“* je vyvoláno dialogové okno pro vytvoření podpisu (obr. 22), zde je již vybrána volba vytvořit podpis *„kreslením“*. Servisní technik nyní vyzve zástupce zákazníka k podpisu na grafickém tabletu. Grafická podoba snímaného podpisu se v reálném čase vykresluje na obrazovce počítače (viz obr. 22).

Obrázek 22: Vytvoření podpisu

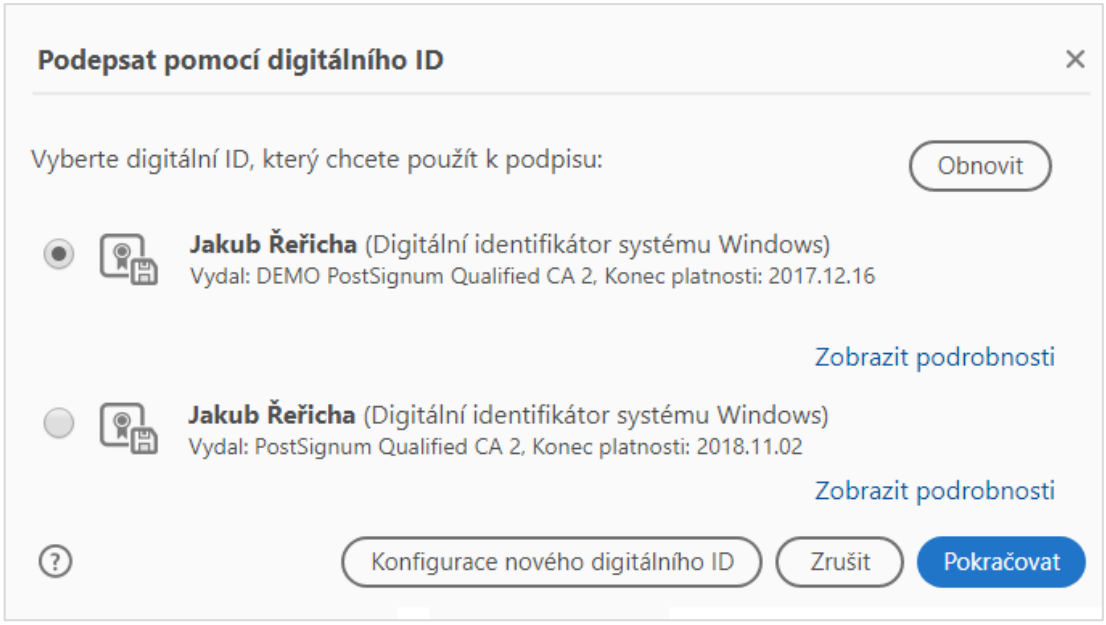
Vytvořený grafický záznam vlastnoručního podpisu zástupce zákazníka potvrdí servisní technik tlačítkem *„Použít“* a dalším kliknutím ho umístí na požadované místo na stránce formuláře ZoSN (obr. 23). Tímto je proces vytvoření podpisu zástupce zákazníka hotový.

Obrázek 23: Vytvořený podpis zástupce za zákazníka

Zbývá ještě podepsat dokument uznávaným elektronickým podpisem servisního technika. Jak bylo uvedeno v kapitole 3.9.1, pro podpis servisního technika je v elektronickém formuláři ZoSN připraveno speciální podpisové pole a kliknutím do něj zahájí servisní technik proces vytvoření svého elektronického podpisu (viz obr. 5 na straně 42).

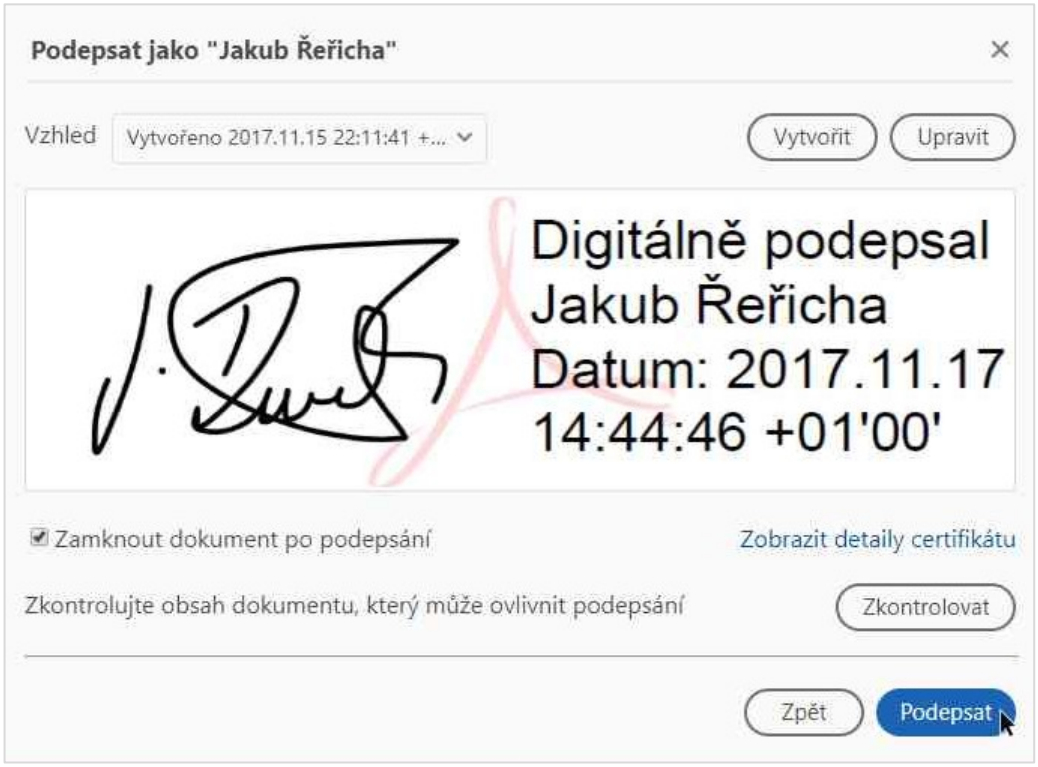
Kliknutím do podpisového pole se spustí dialogové okno pro výběr dostupných prostředků pro vytvoření elektronického podpisu (obr. 24, str. 54). V našem případě je zde na výběr podpis pomocí:

- testovacího kvalifikovaného certifikátu z úložiště certifikátů Windows (horní položka na obr. 24, str. 54) nebo
- získaného kvalifikovaného certifikátu uloženého na kvalifikovaném USB tokenu (spodní položka na obr. 24, str. 54).



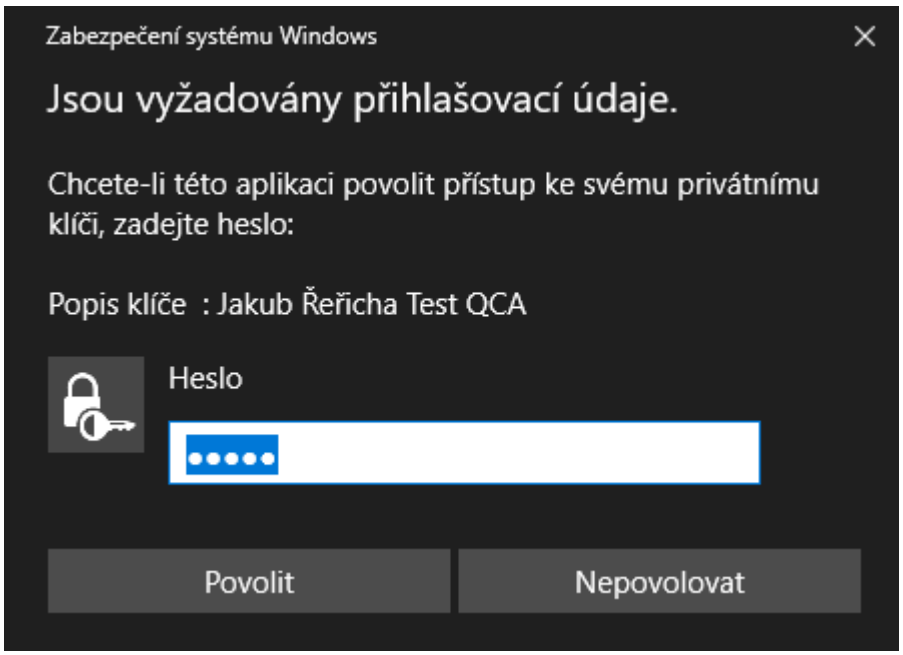
Obrázek 24: Výběr prostředku pro vytvoření el. podpisu

Servisní technik zkontroluje výběr prostředku pro vytvoření elektronického podpisu a potvrdí ho tlačítkem *„Pokračovat“*. V následujícím okně (obr. 25) má servisní technik možnost zobrazit podrobnosti certifikátu a zvolit viditelnou podobu elektronického podpisu. Důležité je, že zde také zaškrtne volbu pro zamknutí souboru po podepsání. Dále servisní technik pokračuje kliknutím na tlačítko *„Podepsat“*.



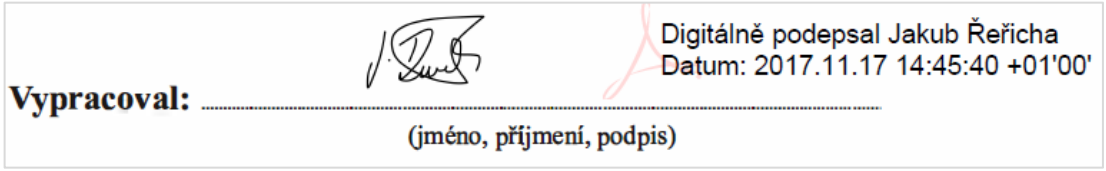
Obrázek 25: Volba vlastností el. podpisu

Následně se zobrazí dialogové okno pro uložení podepsané verze vyplněného formuláře ZoSN, kde servisní technik vybere požadované umístění a název souboru, a to potvrdí tlačítkem *„Uložit“*. V tuto chvíli začne samotné vytváření elektronického podpisu, na jehož začátku musí servisní technik zadat heslo pro potvrzení operace (obr. 26). Jedná se o stejné heslo, které bylo nastaveno při on-line generování žádosti o certifikát (v případě testovacího certifikátu) nebo PIN kód (v případě použití USB tokenu).



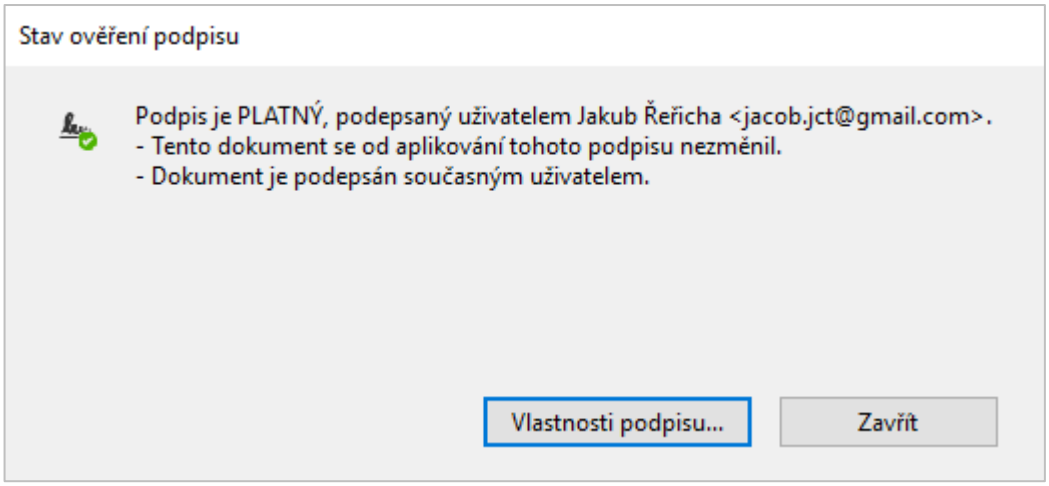
Obrázek 26: Potvrzení operace

Po tom, co servisní technik vytvoření elektronického podpisu potvrdí, program jeho elektronický podpis vytvoří (obr. 27). Elektronický formulář ZoSN je tak prokazatelně podepsán oběma zúčastněnými stranami. Ukázka celého vyplněného a podepsaného formuláře ZoSN je v Příloze 5.

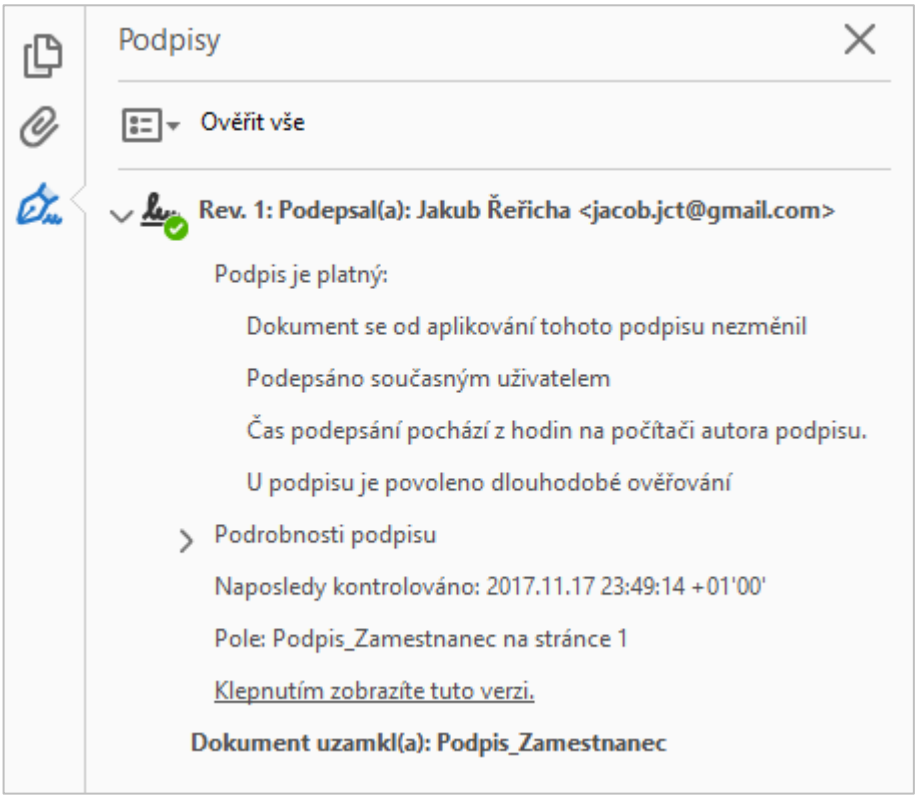


Obrázek 27: Elektronický podpis servisního technika

Na obr. 28 je ukázka výsledku ověření vytvořeného elektronického podpisu za servisního technika, které provádí samotný prohlížeč Acrobat Reader při každém otevření dokumentu nebo na vyžádání uživatele. Program také poskytuje podrobný přehled vlastností a podrobností o podpisu daného dokumentu (obr. 29).



Obrázek 28: Stav ověření podpisu



Obrázek 29: Podrobnosti el. podpisu

4 ZÁVĚR

Tato bakalářská práce se zabývala využitím elektronického podpisu při podepisování elektronických dokumentů ve firemní praxi. Vzhledem k tomu, že legislativa se v této problematice změnila poměrně nedávno, přijetím Nařízení eIDAS a navazujícím zákonem č. 297/2016 Sb., považoval jsem za důležité novou situaci co nejvíce zpřehlednit a na změny upozornit. Bylo mi umožněno využít pro svou práci reálné prostředí fungující firmy, kde jsem měl možnost podílet se na procesu zavádění moderních technologií do praxe.

V teoretické části byla představena problematika elektronického podpisu ve světle nově vydané legislativy EU a ČR, byly přiblíženy současné technické možnosti a popsány jednotlivé druhy elektronického podpisu. Pro vymezení tematického okruhu a pochopení zpracovávané problematiky bylo nejprve potřeba vysvětlit pojmy, které s problematikou elektronického podpisu bezprostředně souvisejí, jako například: co je to digitální podpis, asymetrická kryptografie, otisk dokumentu, certifikát pro elektronický podpis apod. Informace sestavené v teoretické části, které jsem získal v průběhu studia a ze všech dostupných pramenů, umožnily nastínit další postup a pomohly mi zvolit metodiku pro analytickou část práce.

V analytické části práce byly různé způsoby elektronického podepisování nejprve v širší obecné rovině porovnány a vhodnost jejich použití byla posouzena pro jednotlivé druhy komunikace v IS firmy.

Dále se práce věnovala mapování aktuálních prostředků a potřeb elektronického podpisu při zpracování dokumentů v elektronické podobě v prostředí informačního systému konkrétní firmy. V práci bylo navrženo řešení pro aktuální potřeby firmy CHOS a toto řešení bylo předvedeno v podobě proof-of-concept.

V analytické části práce se podařilo:

- zhodnotit jednotlivá řešení elektronického podpisu;
- posoudit varianty el. podpisu pro různé druhy komunikace v IS;
- zjistit potřeby implementace elektronického podpisu ve firmě CHOS;
- zmapovat existující prostředky firmy pro prokázání původu dokumentů;
- pro zjištěné potřeby firmy navrhnout nejvhodnější způsoby elektronického podpisu;
- zpracováním proof-of-concept ověřit návrh řešení.

Řešení, které bylo nakonec vybráno jako nejvhodnější, je i v souladu s obecným nařízením o ochraně osobních údajů (GDPR). Lze tedy říci, že cílů bakalářské práce bylo dosaženo.

Implementace elektronického podpisu zde byla nejprve řešena obecně a následně prakticky na příkladu jedné firmy, pro kterou bylo nalezeno konkrétní řešení. Informační systém ale nabízí mnohem širší možnosti využití el. podpisu, například při potvrzování absolvovaných školení formou e-learningu apod. Poznatky zpracované v této bakalářské práci výběr vhodného typu elektronického podpisu usnadní a při jeho širší implementaci do IS lze s nimi dále pracovat.

5 SEZNAM POUŽITÝCH INFORMAČNÍCH ZDROJŮ

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. In: *EUR-Lex* [online právní informační systém]. Brusel: Evropská unie, 2014, ročník 2014, číslo 910. Dostupné také z: http://data.europa.eu/eli/reg/2014/910/oj

2. Zákon č. 227/2000 Sb.: Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). *Zákony pro lidi.cz* [online]. Zlín: AION CS, c2010-2017 [cit. 2017-11-21]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-227

3. Zákon ze dne 24. srpna 2016, o službách vytvářejících důvěru pro elektronické transakce. *Epravo.cz* [online]. Praha: Epravo.cz, c1999-2017 [cit. 2017-11-21]. Dostupné z: https://www.epravo.cz/top/zakony/sbirka-zakonu/zakon-ze-dne-24-srpna-2016-o-sluzbach-vytvarejicich-duveru-pro-elektronicke-transakce-21255.html

4. PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-3-8. Dostupné také z: https://knihy.nic.cz/files/edice/bajecny_svet_elektronickeho_podpisu_cznic.pdf

5. SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2., aktualiz. a rozš. vyd. Praha: C.H. Beck, 2004. Právo a hospodářství (C.H. Beck). ISBN 80-717-9765-0.

6. PETERKA, Jiří. EIDAS a elektronické podpisy: jak poznáme, o jaký podpis jde? In: *Lupa.cz* [online]. Praha: Internet Info, 2016 [cit. 2017-11-21]. Dostupné z: https://www.lupa.cz/clanky/eidas-a-elektronicke-podpisy-jak-pozname-o-jaky-podpis-jde/

7. DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

8. Asymetrická kryptografie. *Univerzitní informační systém MENDELU* [online]. Brno: Mendelova univerzita v Brně, c2017 [cit. 2017-11-22]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7027

9. Otisk – Hash. *Bonanza* [online]. Praha: BONOsoft, c2009-2017 [cit. 2017-11-22]. Dostupné z: http://www.datove-schranky-software.cz/otisk-hash.html

10. What are digital signatures?: How do digital signatures work? *DocuSign* [online]. San Francisco: DocuSign [cit. 2017-11-22]. Dostupné z: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

11. Algoritmus RSA: Princip asymetrické kryptografie. *Algoritmy.net* [online]. Neckář, c2016 [cit. 2017-11-22]. Dostupné z: https://www.algoritmy.net/article/4033/RSA

12. Co to je digitální certifikát. *Interval.cz* [online]. Brno: Zoner software, 2003 [cit. 2017-11-22]. Dostupné z: https://www.interval.cz/clanky/co-to-je-digitalni-certifikat/

13. LECHNER, Tomáš. Různé druhy certifikátů a jejich použití. *Národní pojištění: odborný měsíčník* [online]. Praha: Česká správa sociálního zabezpečení, 2014, **45**(6) [cit. 2017-11-22]. ISSN 0323-2395. Dostupné z: http://www.cssz.cz/cz/casopis-narodni-pojisteni/archiv-vydanych-cisel/clanky/NP-06-2014-ruzne-druhy-certifikatu-a-jejich-pouziti.htm

14. Jaký je rozdíl mezi komerčním a kvalifikovaným certifikátem. *Digitalni-podpis.cz* [online]. [Havířov]: [Kontár] [cit. 2017-11-22]. Dostupné z: https://www.digitalni-podpis.cz/rozdil-mezi-komercnim-a-kvalifikovanym-certifikatem

15. BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. Olomouc: ANAG, 2008. Právo (ANAG). ISBN 978-80-7263-465-1.

16. Komerční certifikáty. *Certifikační autorita PostSignum* [online]. Praha: Česká pošta, c2010 [cit. 2017-11-22]. Dostupné z: http://www.postsignum.cz/komercni_certifikaty.html

17. Využití certifikátů. *Certifikační autorita PostSignum* [online]. Praha: Česká pošta, c2010 [cit. 2017-11-22]. Dostupné z: http://www.postsignum.cz/vyuziti_certifikatu.html

18. Komerční a kvalifikované certifikáty. *První certifikační autorita* [online]. [Praha]: První certifikační autorita [cit. 2017-11-22]. Dostupné z: http://www.ica.cz/Certifikaty

19. Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2017 [cit. 2017-11-22]. Dostupné z: http://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx

20. *Certifikační politika: Vydávání kvalifikovaných certifikátů*. Verze 3.1. [Praha]: První certifikační autorita, 2011, 65 s. Dostupné také z: http://www.ica.cz/Userfiles/files/politika/CP_QCv31.pdf

21. RADA, Ivan a František TIKAL. K nové právní úpravě elektronického podpisu. In: *Epravo.cz* [online]. Praha: Epravo.cz, 2017 [cit. 2017-11-27]. Dostupné z: https://www.epravo.cz/top/clanky/k-nove-pravni-uprave-elektronickeho-podpisu-106077.html

22. ZELENKOVÁ, Nela. Kdy je nově prostý elektronický podpis rovnocenný s podpisem vlastnoručním? In: *Epravo.cz* [online]. Praha: Epravo.cz, 2017 [cit. 2017-11-27]. Dostupné z: https://www.epravo.cz/top/clanky/kdy-je-nove-prosty-elektronicky-podpis-rovnocenny-s-podpisem-vlastnorucnim-104697.html

23. PETERKA, Jiří. EIDAS a elektronické podpisy: Nepřehnali jsme to s našimi výjimkami? In: *Lupa.cz* [online]. Praha: Internet Info, 2016 [cit. 2017-11-27]. Dostupné z: https://www.lupa.cz/clanky/eidas-a-elektronicke-podpisy-neprehnali-jsme-to-s-nasimi-vyjimkami/

24. PETERKA, Jiří. Unijní eIDAS přichází. O co přijdeme u elektronických podpisů? In: *Lupa.cz* [online]. Praha: Internet Info, 2016 [cit. 2017-11-27]. Dostupné z: https://www.lupa.cz/clanky/unijni-eidas-prichazi-o-co-prijdeme-u-elektronickych-podpisu/

25. KORBEL, František a Dalibor KOVÁŘ. Změny v regulaci elektronických podpisů (eIDAS). In: *Právní prostor* [online]. [Ostrava]: [ATLAS consulting], 2016 [cit. 2017-11-27]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/zmeny-v-regulaci-elektronickych-podpisu-eidas

26. Kvalifikované certifikáty. *Certifikační autorita PostSignum* [online]. Praha: Česká pošta, c2010 [cit. 2017-11-27]. Dostupné z: http://www.postsignum.cz/kvalifikovane_certifikaty.html

27. Vládní návrh zákona o službách vytvářejících důvěru pro elektronické transakce: Návrh zákona včetně důvodové zprávy. In: Poslanecká sněmovna Parlamentu České republiky [online]. Praha: Poslanecká sněmovna Parlamentu České republiky, 2016, ročník 0, číslo 763. Dostupné také z: http://www.psp.cz/doc/00/12/57/00125785.pdf

28. BÝČKOVÁ, Michaela. Závaznost dynamického elektronického podpisu. In: *Právní prostor* [online]. [Ostrava]: [ATLAS consulting], 2016 [cit. 2017-11-27]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/zavaznost-dynamickeho-elektronickeho-podpisu

29. Podpisové pady: Sigma pad. *Contrisys* [online]. Praha: Contrisys, c2012 [cit. 2017-11-29]. Dostupné z: http://www.contrisys.com/podpisove-pady-4-sigma-pad

30. Click wrap. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2017 [cit. 2017-11-29]. Dostupné z: https://en.wikipedia.org/wiki/Click_wrap

31. KMENT, Vojtěch. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? In: *Bulletin-advokacie.cz* [online]. Praha: Česká advokátní komora, 2016 [cit. 2017-11-29]. Dostupné z: http://www.bulletin-advokacie.cz/nahradi-elektronicky-podpis-prosty-ten-tradicni-vlastnorucni?

32. DOSKOČILOVÁ, Veronika. Napodobením biometrických údajů můžete přijít o identitu (Rozhovor). In: *Měšec.cz* [online]. Praha: Internet Info, c1998-2017 [cit. 2017-11-29]. Dostupné z: https://www.mesec.cz/clanky/napodobenim-biometrickych-udaju-muzete-prijit-o-identitu-rozhovor/

33. Podpis otiskem palce se vrací. In: *Software602* [online]. Praha: Software602, 2015 [cit. 2017-11-29]. Dostupné z: https://www.602.cz/o-nas/novinky/tiskove-zpravy/podpis-otiskem-palce-se-vraci/

34. Jak funguje vyspělá zabezpečovací technologie Touch ID. In: *Podpora Apple* [online]. [Cupertino]: Apple, 2017 [cit. 2017-11-29]. Dostupné z: https://support.apple.com/cs-cz/HT204587

35. Elektronický podpis pomocí otisku prstu. In: *Software602* [online]. Praha: Software602, 2015 [cit. 2017-11-29]. Dostupné z: https://www.602.cz/o-nas/novinky/elektronicky-podpis-pomoci-otisku-prstu/

36. Touch ID. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2017-11-29]. Dostupné z: https://en.wikipedia.org/wiki/Touch_ID

37. COOPER, D., S. SANTESSON, S. FARRELL, S. BOEYEN, R. HOUSLEY a W. POLK. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: RFC 5280. In: *RFC Editor* [online]. [Fremont]: [Association Management Solutions], 2008 [cit. 2017-11-29]. Dostupné z: https://www.rfc-editor.org/rfc/rfc5280.txt

38. ITU-T X.509 (10/2016): Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. In: *ITU-T Recommendations* [online]. [Geneva]: International Telecommunication Union, 2016 [cit. 2017-11-29]. Dostupné z: http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509

39. Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *EUR-Lex [online právní informační systém]*. Brusel: Evropská unie, 2016, ročník 2016, číslo 679. Dostupné také z: http://data.europa.eu/eli/reg/2016/679/oj

40. *Chos.cz* [online]. Třeboň: Chemická obchodní společnost [cit. 2017-11-29]. Dostupné z: http://www.chos.cz/

41. *Globis.cz: Vzdělávání z praxe* [online]. České Budějovice: GLOBIS, c2017 [cit. 2017-11-29]. Dostupné z: http://www.globis.cz/

42. Stanovisko č. 2/2014 - Dynamický biometrický podpis z pohledu zákona o ochraně osobních údajů. In: *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2014 [cit. 2017-11-29]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id=11298&n=stanovisko-c-2-2014-dynamicky-biometricky-podpis-z-pohledu-zakona-o-ochrane-osobnich-udaju

43. Obrázek 1.9: Digitální podpis. DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, s. 27. ISBN 978-80-251-2619-6.

44. Obrázek 1.10: Verifikace digitálního podpisu. DOSTÁLEK, Libor a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, s. 28. ISBN 978-80-251-2619-6.

6 SEZNAM POUŽITÝCH ZKRATEK

biom.	biometrický
CA	certifikační autorita
DBP	dynamický biometrický podpis
EAL4+	Evaluation Assurance Level 4+ – mezinárodní standard ohodnocení úrovně jistoty
el.	elektronický
EU	Evropská unie
FIPS 140-2	Federal Information Processing Standard Publication 140-2
GDRP	General Data Protection Regulation – Obecné nařízení o ochraně osobních údajů
CHOS	Chemická obchodní společnost s.r.o.
IS	informační systém
ITU	International Telecommunication Union
mj.	mimo jiné
obr.	obrázek
os.	osoba
PIN	Personal Identification Number – osobní identifikační číslo
PKI	Public Key Infrastructure – označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie
PSVD	poskytovatel služeb vytvářejících důvěru
PUK	Personal Unlocking Key – osobní odblokovací kód
RFC	Request For Comments
RSA	Rivest, Shamir, Adleman – šifra s veřejným klíčem (algoritmus)
SHA	Secure Hash Algorithm – rozšířená hašovací funkce
spec.	speciální
USB	Universal Serial Bus – moderní způsob připojení periferií k počítači
ZoSN	Záznam o servisní návštěvě

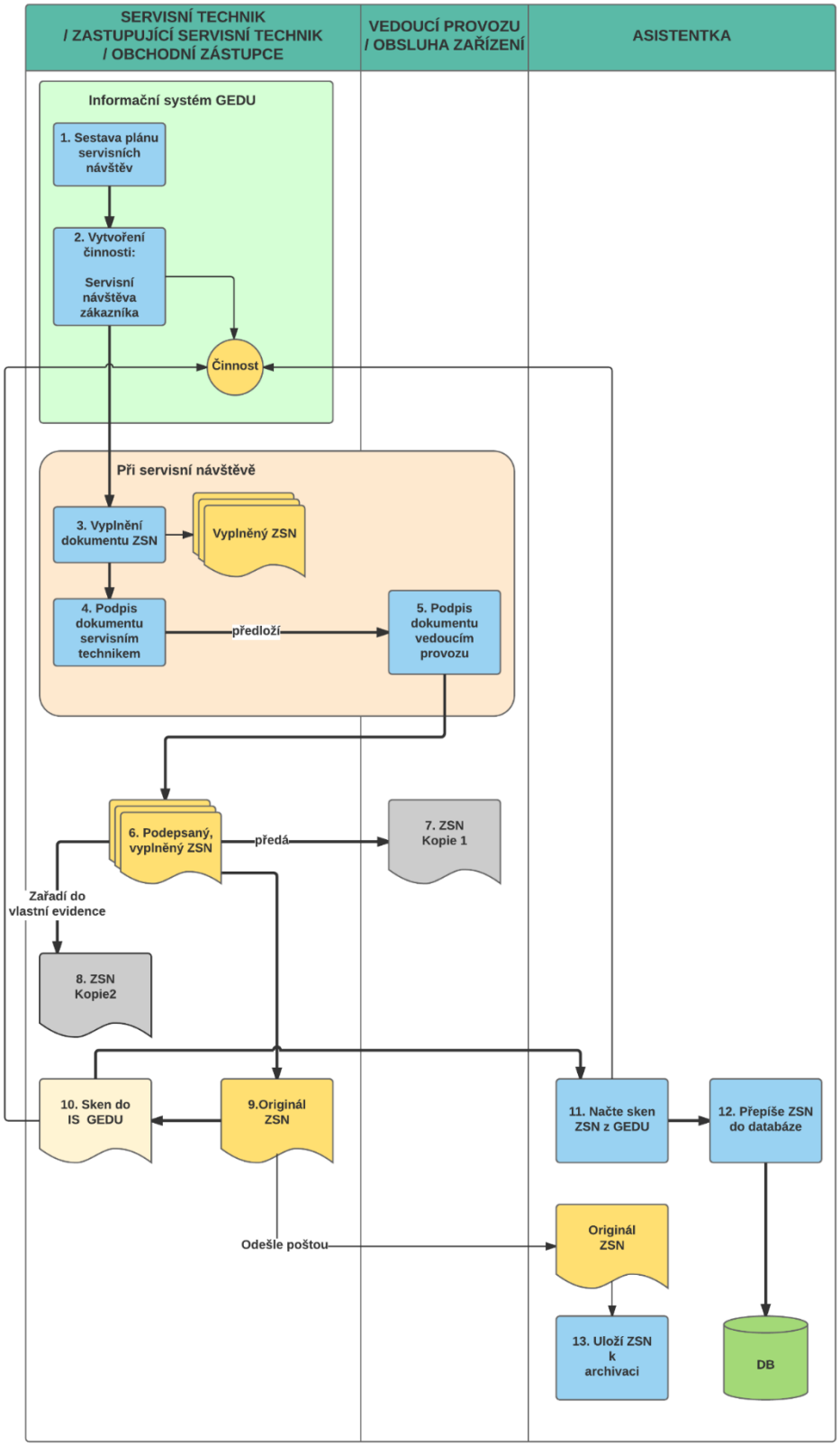
7 SEZNAM POUŽITÝCH TABULEK A OBRÁZKŮ

7.1 Seznam použitých tabulek

7.2 Seznam použitých obrázků

8 PŘÍLOHY

Příloha 1 – Diagram procesu Záznamu o servisní návštěvě



Příloha 2 – Záznam o servisní návštěvě

Chemická obchodní společnost s.r.o.
Pražská 1207
379 01 Třeboň
Držitel certifikátu ČSN EN ISO 9001:2009

Telefon: 384 721 560
Telefax: 384 721 561
E-mail: chos@chos.cz
http: www.chos.cz

Záznam o servisní návštěvě

datum:

Firma: **Zástupce:**

Zařízení:

Minulý návrh opatření:

Výsledek:

Vizuální stav:

Stav vodoměru v m^3

Analýza vod:

Voda	pH	p-alk mmol/l	m-alk mmol/l	Tvrd. mmol/l	Vodiv. µS/cm	Cl^- mg/l	Fe mg/l	Fe po filtraci	PO_4^{3-} mg/l		

Nastavení dávkovacích čerpadel:

Název přípravku	MAN CONT	zd./ min. zd./ imp.	FREQ.	ZDVIH %	N celkem zdvihů

Zásoba přípravku

Hodnocení, návrh opatření:

Vypracoval: .....
(jméno, příjmení, podpis)

Převzal: .....
(jméno, příjmení, podpis)

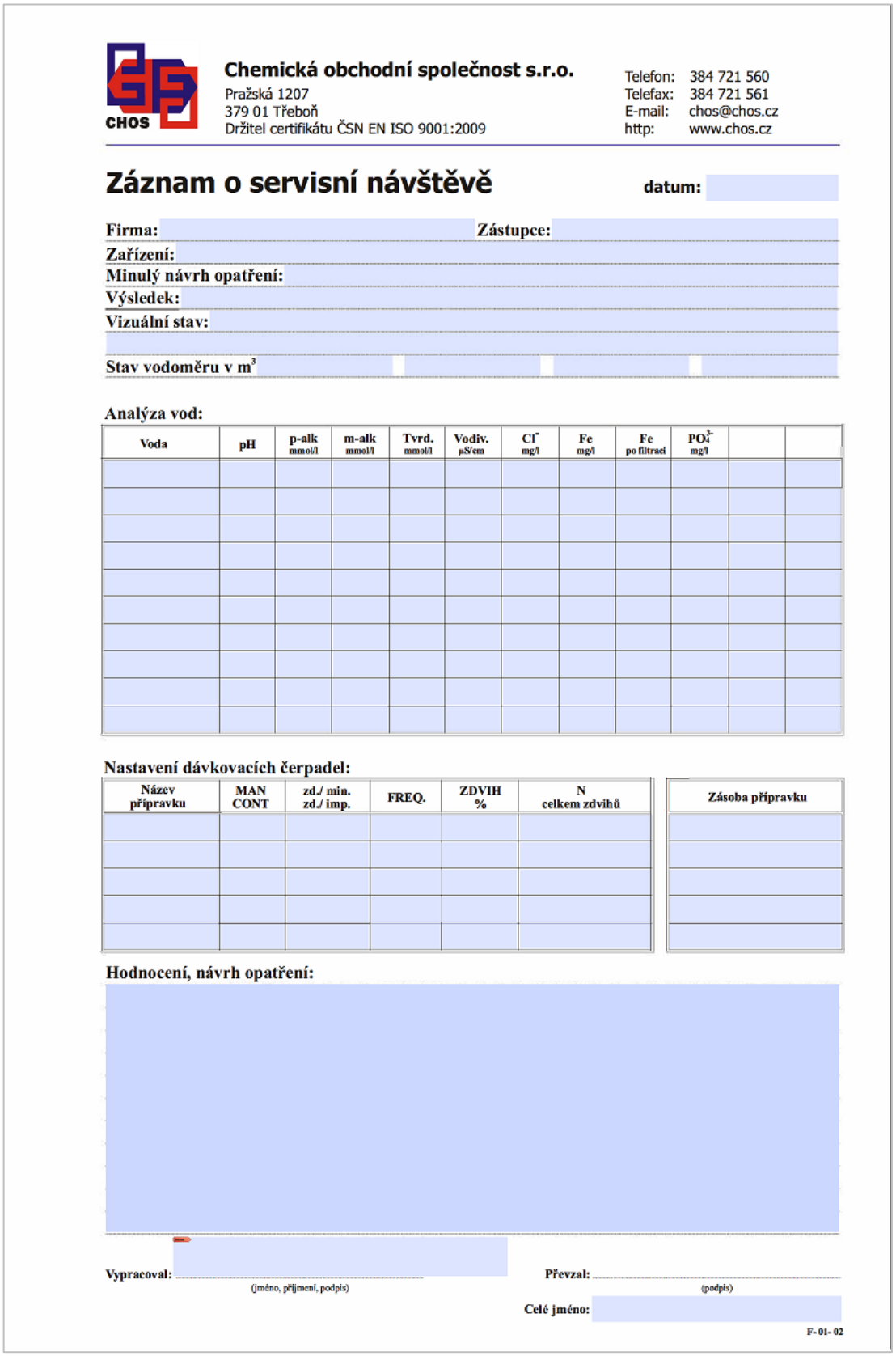
F- 01- 02

Příloha 3 – Doplnění servisní smlouvy

Obě smluvní strany se dohodly, že pro potřeby elektronického zpracování ZoSN budou vzájemně akceptovat elektronický podpis:

1. uznávaný elektronický podpis zástupce firmy CHOS jako poskytovatele zboží a služeb;
2. vlastnoruční podpis zástupce odběratele nasnímaný bez biometrických údajů, přičemž grafická podoba vlastnoručního podpisu může být nasnímána pomocí dotykového displeje, grafického tabletu či podpisového padu. Autenticita druhého podpisu bude podpořena doplněním čitelné podoby jména autora podpisu a tím, že dokument ZoSN bude ihned po podepsání oběma stranami automaticky odeslán na kontaktní e-mail zákazníka (odběratele) a bude vyžadováno potvrzení o přečtení. Datum odeslání e-mailu se bude shodovat s datem vyplněným v záhlaví ZoSN a s datem obsaženým v uznávaném elektronickém podpisu zaměstnance CHOS (poskytovatele).

Příloha 4 – Náhled formulářové verze ZoSN



Chemická obchodní společnost s.r.o.
Pražská 1207
379 01 Třeboň
Držitel certifikátu ČSN EN ISO 9001:2009

Telefon: 384 721 560
Telefax: 384 721 561
E-mail: chos@chos.cz
http: www.chos.cz

Záznam o servisní návštěvě

datum:

Firma: **Zástupce:**
Zařízení:
Minulý návrh opatření:
Výsledek:
Vizuální stav:
Stav vodoměru v m^3

Analýza vod:

Voda	pH	p-alk mmol/l	m-alk mmol/l	Tvrd. mmol/l	Vodiv. µS/cm	Cl^- mg/l	Fe mg/l	Fe po filtraci	PO_4^{3-} mg/l		

Nastavení dávkovacích čerpadel:

Název přípravku	MAN CONT	zd./ min. zd./ imp.	FREQ.	ZDVIH %	N celkem zdvihů

Zásoba přípravku

Hodnocení, návrh opatření:

Vypracoval: .....
(jméno, příjmení, podpis)

Převzal: .....
(podpis)

Celé jméno:

F- 01- 02

Příloha 5 – Ukázka vyplněného a podepsaného formuláře ZoSN

Chemická obchodní společnost s.r.o.
Pražská 1207
379 01 Třeboň
Držitel certifikátu ČSN EN ISO 9001:2009

Telefon: 384 721 560
Telefax: 384 721 561
E-mail: chos@chos.cz
http: www.chos.cz

Záznam o servisní návštěvě

datum: 13. 5. 2016

Firma: NovakSpol s.r.o. **Zástupce:** Josef Novák

Zařízení: 3 x UCHO; Kotelna

Minulý návrh opatření:

Výsledek:

Vizuální stav: 1 - F + H čiré, bezbarvé; 2 - čirá, žlutá; Kotelna - kalná, černá, silně zabarvená

Stav vodoměru v m³ 1 - 325 2 - 3417 Kotelna - 434,8 -

Analýza vod:

Voda	pH	p-alk mmol/l	m-alk mmol/l	Tvrd. mmol/l	Vodiv. µS/cm	Cl^- mg/l	Fe mg/l	Fe po filtraci	PO_4^{3-} mg/l		
1 Doplňková OSMO	6,63	0,0	0,8	0,0	25	2					
Formy	7,47	0,0	8,4	1,0	1028	2	2,5				
1 Hydraulika	8,08	0,0	4,8	0,8	554	2	0,8				
2 Doplňková SV+ZV	7,01	0,0	5,6	1,4	691	32	0,1				
2 Formy	7,78	0,0	5,9	1,1	617	25	30,0				
2 Hydraulika	8,39	0,4	5,8	1,1	610	25	20,0				
Kotelna	9,03	0,6	4,2	0,2	560	15	75,0				
Změkčená před RO				0,6							

Nastavení dávkovacích čerpadel:

Název přípravku	MAN CONT	zd./ min. zd./ imp.	FREQ.	ZDVIH %	N celkem zdvihů	Zásoba přípravku
1 Corsiheld MD4103		5,4	180	100	52420	14 kg
1 Spectrus NX1100						
Gengard GN7004			180	100	19276	0
SpectrusNX1100						20 kg

Hodnocení, návrh opatření:

Strojovna 1 - Formy + Hydraulika - O.K. bez opatření
- nadávkován SPECTRUS 1512 - 0,4 l + SPECTRUS NX110 - 0,5 l

Strojovna 2 - F + H - vysoké množství železa přetrvává, doporučení úrava vody RO + změna chem. přípravku
- zavzdušněné D. Č. GENGARDU GN 7004, v současné době v kanystru voda!, prosím o výměnu kanystru po podání GENGARDU GN7004
- nadávkován SPECTRUS BD 1512 - 0,5 l + SPECTRUS NX1422 - 1 l

Kotelna - vysoké množství železa, zabarvení, zákal, doporučuji zapůjčit filtraci dle návrhu p. Kubaly

Vypracoval: Digitálně podepsal Jakub Řeřicha Datum: 2017.11.17 14:45:40 +01'00'
(jméno, příjmení, podpis)

Převzal: Jan Novotný
(podpis)

Celé jméno: Jan Novotný

F-01-02