EKONOMICKÁ FAKULTA TUL

Bakalářská práce

Zajištění dokumentů pomocí digitálního podpisu

Studijní program: B0688P140002 Informační management
Autor práce: **Filip Šourek**
Vedoucí práce: doc. Ing. Klára Antlová, Ph.D.
Katedra informatiky

Liberec 2024

EKONOMICKÁ FAKULTA TUL

Zadání bakalářské práce

Zajištění dokumentů pomocí digitálního podpisu

Jméno a příjmení:	**Filip Šourek**
Osobní číslo:	E21000236
Studijní program:	B0688P140002 Informační management
Zadávající katedra:	Katedra informatiky
Akademický rok:	2023/2024

Zásady pro vypracování:

1. Softwarové a hardwarové řešení zajištění digitálního podpisu
2. Metody šifrování využívané v rámci digitálního podpisu
3. Návrh postupu implementace digitálního podpisu (pomocí případové studie)
4. Vyhodnocení daného řešení
5. Ekonomický přínos daného řešení

Rozsah grafických prací:
Rozsah pracovní zprávy: 30 normostran
Forma zpracování práce: tištěná/elektronická
Jazyk práce: čeština

Seznam odborné literatury:

- BURDA, Karel, 2019. *Kryptografie okolo nás*. Praha: CZ.NIC, z.s. p.o. ISBN 978-80-88168-49-2.
- KUROSE, James a Keith ROSS, 2014. *Počítačové sítě*. Brno: Computer Press. ISBN 978-80-251-3825-0.
- STAPLETON, Jeffrey a Clay EPSTEIN, 2016. *Security without obscurity. A guide to PKI operations*. CRC Press Boston: Taylor & Francis Group. ISBN 978-1-4987-0747-3.
- OULEHLA, Milan a Roman JAŠEK, 2017. *Moderní kryptografie*. Praha: IFP Publishing s.r.o. ISBN 978-80-87383-67-4.
- ZIMMER, Jan et al. 2021. The challenge of comparing digitally captured signatures registered with different software and hardware. online. *Forensic Science International*. vol. 327, no.3, s.103-120. ISSN 1872-6283. Dostupné z: https://doi.org/10.1016/j.forsciint.2021.110945.

Konzultant: Jakub Zezula, Systémový analytik, Škoda-auto, a.s.

Vedoucí práce: doc. Ing. Klára Antlová, Ph.D.
Katedra informatiky

Datum zadání práce: 1. listopadu 2023
Předpokládaný termín odevzdání: 31. srpna 2025

L.S.

doc. Ing. Aleš Kocourek, Ph.D.
děkan

Mgr. Tereza Semerádová, Ph.D.
garant studijního programu

V Liberci dne 1. listopadu 2023

Prohlášení

Prohlašuji, že svou bakalářskou práci jsem vypracoval samostatně jako původní dílo s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Jsem si vědom toho, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu Technické univerzity v Liberci.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti Technickou univerzitu v Liberci; v tomto případě má Technická univerzita v Liberci právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Současně čestně prohlašuji, že text elektronické podoby práce vložený do IS/STAG se shoduje s textem tištěné podoby práce.

Beru na vědomí, že má bakalářská práce bude zveřejněna Technickou univerzitou v Liberci v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

Jsem si vědom následků, které podle zákona o vysokých školách mohou vyplývat z porušení tohoto prohlášení.

2. května 2024 Filip Šourek

Zajištění dokumentů pomocí digitálního podpisu

Anotace

Bakalářská práce je zaměřena na problematiku zajištění dokumentů pomocí digitálních podpisů. Po uvedení do problematiky jsou stanoveny cíle, kterých bude následně dosaženo. V teoretické části jsou popsána především technická specifika související s digitálními podpisy a certifikáty. Dále je uveden princip fungování digitálních podpisů, jejich aplikace a bezpečnost, a je představen podnik a oddělení, kde byla zajištěna implementace podpisové technologie pro zajištění dokumentů digitálním podpisem. Následně jsou vysvětleny postupy a důvody při rozhodování pro zvolení vhodné technologie. V poslední části jsou shrnuty přínosy, výsledky a doporučení pro postup obdobné implementace podobné technologie. Poté se jedna kapitola věnuje ekonomickému přínosu a návratnosti investice do podpisového zařízení. Závěrem jsou shrnuty klíčové informace a nejzajímavější poznatky bakalářské práce.

Klíčová slova

Adobe Sign, certifikační autorita, digitální podpis, elektronický podpis, podpisové destičky, Signotec, Škoda Auto

Securing documents using a digital signature

Annotation

The bachelor thesis focuses on the issue of document security using digital signatures. After introducing the problematics, objectives are set, which will be then achieved. The theoretical part primarily describes the technical specifics related to digital signatures and certificates. Furthermore, the functioning principle of digital signatures, their applications, and security are outlined. Then, the company and department where the signature technology for securing documents was implemented, are introduced. Procedures and reasons for choosing suitable technology are explained thereafter. In the final section, the benefits, results, and recommendations for a similar technology implementation process are summarized. Subsequently, one chapter addresses the economic benefits and return on investment in signature equipment. Finally, key information and the most interesting findings of the bachelor thesis are summarized.

Key Words

Adobe Sign, certification authority, digital signature, electronic signature, signature pads, Signotec, Škoda Auto

Poděkování

Chtěl bych poděkovat vedoucí bakalářské práce doc. Ing. Kláře Antlové, Ph.D. za všestrannou pomoc, množství cenných rad a podmětů při zpracování této práce. Dále mé poděkování patří vedoucímu stáže ve firmě Škoda Auto a.s. Ing. Michalovi Bímovi a konzultantovi Jakubovi Zezulovi za jejich drahocenné zkušenosti v tématech zabývajících se praktickou stránkou bakalářské práce.

Obsah

Seznam ilustrací (obrázků)

Seznam tabulek

Seznam použitých zkratek, značek a symbolů

CA	Certifikační autorita
ETUL	Důvěryhodný seznam Evropské unie (European Union Trusted Lists of Trust Service Providers)

Úvod

Digitální transformace v posledních letech přinesla významné změny v tom, jak vnímáme každodenní náplň práce. Spolu s velkým důrazem na téma klima a životní prostředí se spousta firem věnuje digitalizaci zbytečných papírových dokumentů a snižování tisků papírů. Jeden z klíčových aspektů této transformace je rostoucí využívání digitálních podpisů jako efektivního nástroje pro zajištění bezpečnosti a autentičnosti digitálně podepsaných dokumentů. Tato bakalářská práce se zaměřuje na problematiku digitálního podpisu a jeho využití pro zabezpečení dokumentů v digitálním prostředí.

Cílem této práce je poskytnout čtenáři komplexní pohled na digitální podpisy včetně teoretických základů, technických aspektů, a i právního rámce v České republice. Dále se práce zaměřuje na praktickou stránku implementace digitálních podpisů pomocí případové studie ve firmě Škoda Auto, která popisuje konkrétní postup nasazení podpisových destiček Signotec v organizačním prostředí v souladu s požadavky daného oddělení. Následně jsou shrnuty požadavky, doporučení a důležité poznatky získané během případové studie. Poslední část bakalářské práce je zaměřena na ekonomický přínos vybraného řešení pro digitální podpisy. Zde je vysvětlen doporučený postup výpočtu návratnosti investice z hlediska nákladů na provoz tiskárny a nákladů na zajištění podpisového hardwaru.

Stanovení cílů

Cílem této práce je porozumět fungování digitálních podpisů a navrhnout vhodné řešení pro jejich implementaci. Nejprve je zkoumáno prostředí firmy a následně i samotné oddělení, které řešení digitálních podpisů vyhledává. Práce se zde zaměřuje na politiku a možnosti firmy o implementaci různých řešení. V této části jsou shromažďovány požadavky a očekávání od oddělení a na jejich základě jsou navrhnuta možná řešení. Z těch je následně vybráno optimální řešení.

Další část práce se věnuje implementaci vybraného optimálního řešení, jeho konfiguraci a hladké integraci do existující infrastruktury firmy. Vybrané řešení je zde podrobně popsané jak po softwarové stránce, tak i po hardwarové stránce. Dále je v této části poukázáno na fungování řešení ze strany IT administrátora, uživatele a podepisujícího se klienta.

Poslední část práce se zaměřuje na přínosy a výsledky implementace řešení, případné výzvy a jejich řešení, doporučení, a na ekonomický přínos daného řešení. Je zde znázorněný pohled na finanční stránku věci a zároveň vysvětlen postup měření návratnosti investice.

1. Digitální podpis

Digitální podpis představuje elektronický mechanismus, díky kterému je umožněné ověření identity odesílatele digitálního dokumentu nebo zprávy. Je to digitální bezpečnější způsob tradičního ručního podpisu používaného v papírové formě. Digitální podpis využívá moderní technologie a matematických principů, aby zajistil autentizaci, nedopustitelnost odmítnutí, integritu dat a nezpochybnitelnost času. (Dostálek et al., 2009)

1.1 Rozdíl mezi digitálním podpisem a elektronickým podpisem

Elektronický podpis je nadřazeným (obecnějším) termínem pro digitální podpis. Zahrnuje různé metody pro ověření identity a schválení dokumentu. Digitální podpis je tedy forma elektronického podpisu, která využívá matematické algoritmy a je založená na algoritmech asymetrické kryptografie. Elektronický podpis může být například ruční podpis v naskenované podobě, biometrický identifikátor (např. otisk prstu), PIN kód apod. Jeho jednoduchost implementace a praktičnost může být vhodná v situacích, kde není vyžadována vysoká úroveň bezpečnosti. (Peterka, 2011)

1.2 Rozdíl mezi digitálním a klasickým (ručním) podpisem

Klasický podpis je vytvářen fyzickým zápisem jména nebo jiného identifikačního prvku na fyzický dokument. Často je spojen s osobním fyzickým aktem a má psychologický aspekt spojený s identitou a závazkem. (Peterka, 2011)

Digitální podpis je vytvářen kryptografickým procesem, kdy se používá soukromý klíč k šifrování informací, čímž vzniká jedinečný kód, který slouží jako digitální podpis. Digitální podpis tak klade důraz na bezpečnost a elektronickou autenticitu. Je odvozen od matematických operací a poskytuje větší úroveň jistoty ohledně toho, kdo dokument podepsal. (Dostálek et al., 2009)

Ověření klasického podpisu může probíhat vizuálně nebo prostřednictvím grafologické analýzy. Což v praxi znamená, že ověření ručního podpisu závisí na expertním posouzení podpisu a může být náchylné k lidské chybě. Klasický podpis může být zpochybněn s poukazem na nedostatečnou grafologickou analýzu nebo tvrzením o nuceném podpisu. Existuje i možnost, že jednotlivec může

popřít platnost svého ručního podpisu. Jako další nevýhodu je nutno podotknout, že vlastnoruční podpisy se ověřují až v moment, kdy dojde k pochybení o pravosti podpisu. (Peterka, 2011)

Na druhou stranu ověření digitálního podpisu je matematický proces, kde je použit veřejný klíč ke kontrole podpisu. Digitální podpis poskytuje možnost automatizovaného a matematicky spolehlivého ověření autenticity, což snižuje riziko chyb spojených s lidským posuzováním. Pokud je vytvořen pomocí soukromého klíče, nelze ho popřít, protože matematické postupy zajišťují jednoznačnou identifikaci autora podpisu. V praxi, na rozdíl od klasického podpisu, se každý digitální podpis ověřuje. Digitální podpis tedy poskytuje vyšší úroveň nezpochybnitelnosti a nemožnosti popření. (Peterka, 2011)

1.3 Funkce digitálního podpisu

Digitální podpis může sloužit k několika klíčovým funkcím, které přispívají k jeho důležitosti a efektivitě při zajišťování dokumentů. Tyto funkce zahrnují:

- **Autentizace:** Digitální podpis umožňuje autentizaci identity odesílatele dokumentu. To znamená, že příjemce může s jistotou ověřit, že dokument pochází od skutečného odesílatele.
- **Nedopustitelnost odmítnutí:** Odesílatel nemá možnost popřít, že dokument podepsal. Jakmile je digitální podpis vytvořen, poskytuje nezpochybnitelný důkaz o autorství a souhlasu odesílatele.
- **Integrita dat:** Digitální podpis zaručuje, že obsah dokumentu zůstal nezměněn od doby jeho podepsání. Pokud by došlo ke změně v obsahu, digitální podpis by se stal neplatným.
- **Nezpochybnitelnost času:** Některé digitální podpisy mohou obsahovat časové razítko, což dodává další úroveň důvěry k tomu, že dokument byl vytvořen nebo podepsán v určitém časovém okamžiku.
- **Šifrování:** Při tvorbě digitálního podpisu je používána asymetrická kryptografie, což znamená, že veřejný a soukromý klíč jsou propojeny. Veřejný klíč slouží k ověření podpisu, zatímco soukromý klíč je používán k jeho vytvoření. Tímto způsobem je zajištěno šifrování dokumentu a zároveň umožněna jeho ověřitelnost. (Dostálek et al., 2009)

Tyto funkce společně vytvářejí pevný základ pro digitální podpis jako nástroj pro zajištění dokumentů. Jsou klíčové pro zvyšování důvěryhodnosti elektronických transakcí, elektronického obchodování a dalších online aktivit, které vyžadují spolehlivý způsob ověření identity a integrity dokumentů. (Peterka, 2011)

1.4 Princip fungování digitálního podpisu

Digitální podpis využívá matematické principy asymetrické kryptografie a hashovacích funkcí k zajištění autentizace, integrity a nezpochybnitelnosti digitálních dokumentů. (Dostálek et al., 2009)

1.4.1 Asymetrická kryptografie

Asymetrická kryptografie, známá také jako veřejný klíčový systém, je kryptografický mechanismus, který využívá dvojici klíčů, kde každý z těchto klíčů má svou specifickou roli a funkci. Veřejný klíč je distribuován volně a slouží k šifrování zpráv. Každý uživatel má svůj vlastní veřejný klíč, který může sdílet s ostatními. Na druhou stranu soukromý klíč je chráněn a uchováván pouze uživatelem, který ho vytvořil. Slouží k dešifrování zpráv, které byly zašifrovány pomocí odpovídajícího veřejného klíče. Soukromý klíč je považován za důvěrný a je důležité zajistit jeho ochranu proti neoprávněnému přístupu. (Dostálek et al., 2009; Peterka, 2011)

Princip asymetrické kryptografie spočívá v tom, že šifrování provedené pomocí veřejného klíče nemůže být snadno zpětně dešifrováno bez použití odpovídajícího soukromého klíče. To poskytuje bezpečný způsob komunikace a zabezpečení dat mezi různými uživateli, aniž by bylo nutné sdílet soukromé klíče. (Oulehla a Jašek, 2017)

Asymetrická kryptografie je klíčovým prvkem pro různé bezpečnostní mechanismy, jako jsou digitální podpisy, šifrování e-mailů, bezpečné spojení přes internet a mnoho dalších. Asymetrická kryptografie není bezpečná pouze díky složitosti algoritmů, ale také díky těžkému až nemožnému úkolu odhalení soukromého klíče z veřejného klíče. (Stinson, 1995)

1.4.2 Hashování

Hashování je kryptografická technika, která transformuje vstupní data libovolné délky (zprávu, dokument, …) na fixní délku dat, nazývanou has. Tato hash hodnota má obvykle fixní délku a má několik klíčových vlastností, zde jsou ty nejdůležitější:

- Pro stejný vstup je vždy vygenerovaná stejná hodnota hash. Tato vlastnost se nazývá determinismus.
- Hodnota hash je odolná vůči změnám. I malá změna, například jeden rozdílný bit, musí mít za následek změnu většiny bitů hodnoty hash. Díky této vlastnosti není možné digitálně podepsané dokumenty či transakce jakkoliv změnit.
- Odolnost proti kolizím je také důležitá pro chod jakékoliv aplikace. Kolize nastává v případě, kdy 2 různé zprávy budou mít za výsledek stejný hash. Ideální hashovací funkce by tedy měla mít minimální pravděpodobnost vzniku takovéto kolize. (Burda, 2019)

Pro zajištění bezpečnosti je potřeba držet krok s dobou a zvolit vhodný a moderní hashovací algoritmus. Některé z nejznámějších algoritmů jsou:

- **MD5 (Message Digest Algorithm 5)** je jedním z nejstarších a jeho doby nejpoužívanějších hashovacích algoritmů, který produkuje 128bitovou hodnotu. Kvůli známým bezpečnostním chybám a kolizím se však nedoporučuje jeho používání v nových aplikacích.
- **SHA-1 (Secure Hash Algorithm 1)** je další ze zastaralejších algoritmů. SHA-1 vyprodukuje 160bitovou hash hodnotu, byl navržen Národním institutem pro standardy a technologie (NIST) a v minulosti byl používán pro digitální podpisy a zabezpečení dat. Stejně jako předchozí MD5 algoritmus se ani SHA-1 nedoporučuje z bezpečnostních důvodů využívat pro aktuální aplikace.
- **SHA-2 (Secure Hash Algorithm 2)** patří do rodiny algoritmů, která zahrnuje SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Tyto algoritmy produkují hodnoty hash o různých délkách (224 bitů – 512 bitů). I přes to, že tato rodina algoritmů nepatří mezi nejnovější, SHA 256 je nejvíce využívaný hashovací algoritmus. Díky rychlosti výpočtu, standardizaci a bezpečnosti je velmi často preferovanou volbou vývojářů.
- **SHA-3 (Secure Hash Algorithm 3)** je nejnovější verze rodiny algoritmů SHA-2 a byl vyvinut z důvodu snahy nahradit SHA-2. Jednou z hlavních vlastností SHA-3 algoritmu je rozdílná struktura SHA-2, díky čemuž by měl být ještě odolnější vůči různým útokům. I přes jeho

bezpečnost jeho užívání roste pozvolně, a to hlavně kvůli tomu, že SHA-256 poskytuje dostatečnou bezpečnost pro většinu potřeb.

- **BLAKE2** je moderní a velmi rychlý hashovací algoritmus, který nabízí vyšší výkon než mnoho jiných algoritmů, včetně SHA-3. I přes maximální důraz na bezpečnost, rychlost a flexibilitu není využíván tak, jak by se čekalo. Dá se předpokládat, že je to hlavně z důvodu zpětné komptability – tedy v případě přechodu z SHA algoritmu na BLAKE2 by byl potřeba velký zásah do funkční infrastruktury. Vývojáři také dávají přednost standardizovaným algoritmům (například SHA-256), což BLAKE2 není. (Jose, 2015)(Aumasson et al., 2013)

1.4.3 Podepsání dokumentu digitálním podpisem a jeho sdílení

Sdílení dokumentu s digitálním podpisem je proces, který umožňuje uživatelům bezpečně sdílet dokumenty a zároveň ověřit jejich autenticitu a integritu. Zde je obecný postup, jak funguje tento proces:

1. Uživatel, který chce podepsat dokument, použije svůj soukromý klíč k vytvoření digitálního podpisu. Tento podpis je vytvořený pomocí asymetrické kryptografie. Zároveň v tomto podpisu je obsažená hodnota hash podepsaného dokumentu, kterou uživatel vytvoří pomocí některého z algoritmů.
2. Po vytvoření digitálního podpisu je podpis připojen k dokumentu pomocí vložení podpisových dat do metadat souboru, nebo vytvořením samostatného souboru, který je však propojen s dokumentem.
3. Následně se dokument dá sdílet standardními způsoby, jako například e-mailem, přes cloudová úložiště, sdílené síťové složky apod. (Peterka, 2011; Dostálek et al., 2009)

Ověření pomocí veřejného klíče

Příjemce dokumentu získá veřejný klíč od odesílatele. S pomocí tohoto klíče dešifruje digitální podpis a získá původní hash dokumentu. Příjemce následně sám vytvoří hash ze staženého dokumentu a porovná ho s dešifrovaným hashem od odesílatele. Pokud se oba hashe shodují, dokument je považován za ověřený. Tímto způsobem digitální podpis potvrzuje, že dokument nebyl změněn od doby podpisu. V dešifrovaném podpisu jsou také obsáhlé informace o odesílateli, tedy podepisujícím uživateli, které svědčí o jeho identitě. V případě, že odesílatel pro podepsání využil

digitálního certifikátu od certifikační autority, dešifrováním získáte informace i o ní. Certifikační autorita je detailněji rozebrána v dalších kapitolách. (Stapleton a Epstein, 2016)

1.5 Bezpečnosti digitálního podpisu

Digitální podpis přináší řadu bezpečnostních opatření, která umožňují spolehlivé ověření identity, autenticity a integrity dokumentů. Nicméně je důležité si být vědom možných hrozeb a zajistit odpovídající opatření k jejich prevenci. Bezpečnost digitálního podpisu vyžaduje komplexní přístup, který zahrnuje technická opatření, správu klíčů, školení uživatelů a sledování bezpečnostních standardů. Pravidelná aktualizace bezpečnostních postupů a reakce na nové hrozby jsou klíčové pro udržení bezpečnosti digitálních podpisů v průběhu času. (A. Kropáčová, 2006)

V následujících bodech jsou zmíněny některé důležité bezpečností prvky:

Ochrana soukromých klíčů

Digitální podpisy jsou závislé na bezpečnosti soukromých klíčů, což jsou tajné kryptografické klíče používané k vytváření digitálních podpisů. Ochrana těchto klíčů je kritickým prvkem celkové bezpečnosti digitálního podpisu. Ztráta soukromého klíče nebo jeho kompromitace útočníkem by mohla umožnit neoprávněný přístup k vytváření legitimních digitálních podpisů. Jako opatření může sloužit silné heslo, ukládání soukromých klíčů na bezpečné úložiště a případně i šifrování samotných soukromých klíčů. Nespolehlivá správa soukromých klíčů může zahrnovat špatné zálohování, neaktualizované údaje nebo nejasné postupy pro přidělování přístupu. To může mít za následek dokonce i jejich ztrátu, což vede k nevratným následkům pro digitální podpisy a bezpečnost. Pro minimalizaci rizika ztráty by soukromé klíče měly být pravidelně zálohovány na bezpečné a odolné úložiště. V případě ztráty by měly být okamžitě odvolány a nahrazeny novými. (Stapleton a Epstein, 2016)

Nedodržování osvědčených postupů může vést k nedostatečnému zabezpečení soukromých klíčů a jejich zranitelnosti vůči útokům, což může mít za následek únik citlivých informací nebo neoprávněné užití digitálních podpisů. Proto je zapotřebí jasně definovat a vynucovat bezpečnostní politiky a postupy pro správu klíčů pro zajištění konzistentního a bezpečného přístupu k soukromým klíčům. (Dostálek et al., 2009)

Autentizace veřejného klíče

Útočník může předstírat, že jeho veřejný klíč patří legitimnímu uživateli, což by vedlo k přijímaní falešných digitálních podpisů. Proto je vhodné používat certifikáty od důvěryhodných certifikačních autorit pro zvýšení důvěryhodnosti veřejných klíčů a zabránit falešným identitám. (Dostálek et al., 2009)

Kybernetické útoky

Útočníci mohou provádět různé typy kybernetických útoků jako jsou phishing, malware nebo brute force útoky, s cílem získat přístup k soukromým klíčům. Užívání aktualizovaných antivirových programů, vyhýbání se neověřeným zprávám nebo e-mailům a pravidelné školení uživatelů o kybernetických hrozbách mohou přispět k ochraně. (Hiltgen et al., 2006)

Pravidelná auditace a sledování

Nedostatečné sledování a auditace mohou vést k nerozpoznání nebo nedostatečné reakci na bezpečnostní incidenty. Pravidelné audity bezpečnosti, sledování aktivit a reakce na bezpečnostní incidenty jsou klíčovými prvky správy bezpečnosti digitálního podpisu. (Dostálek et al., 2009)

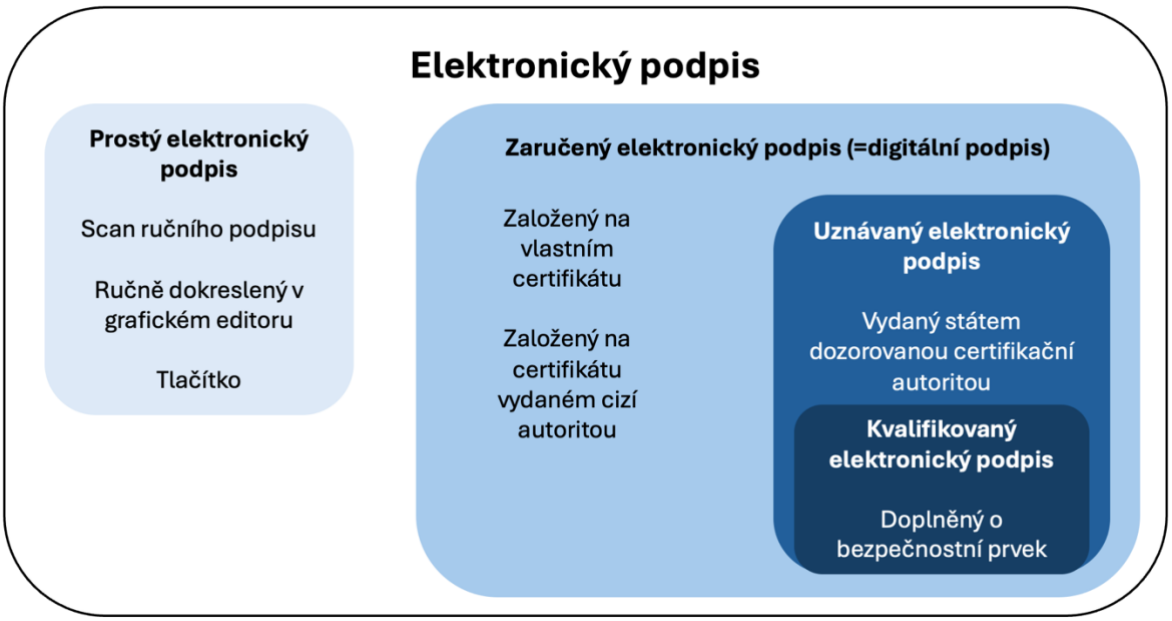
1.6 Právní aspekty digitálního podpisu v České republice

eIDAS (Electronic Identification, Authentication and Trust Services) je nařízení Evropské unie, které stanovuje pravidla pro elektronickou identifikaci a autentizaci, elektronické pečetění, elektronické časové razítko a další elektronické důvěryhodné služby v rámci jednotného digitálního trhu EU. Cílem eIDAS je podpora elektronického obchodu a posílení důvěry v elektronické transakce napříč všemi členskými státy EU. (Generální ředitelství pro komunikační sítě, obsah a technologie, 2023)

V České republice je eIDAS implementován prostřednictvím zákona č. 297/2016 Sb., o službách vytvářející důvěru pro elektronické transakce. Tento zákon stanovuje pravidla pro elektronický podpis, elektronickou identifikaci a další elektronické služby v souladu s eIDAS nařízením. Zákon definuje elektronický podpis jako datový záznam, který je spojen s jinými daty, slouží k autentizaci těchto dat a stanoví, že elektronický podpis má stejnou právní hodnotu jako ruční podpis, pokud splňuje požadavky na jeho bezpečnost a autentizaci. Zákon upravuje proces vydávání certifikátů pro

elektronické podpisy a stanovuje pravidla pro certifikační autority, které tyto certifikáty vydávají. Certifikační autority jsou pověřeny ověřením totožnosti osob a vydáváním certifikátů, které potvrzují platnost elektronických podpisů. Zákon také stanovuje podmínky pro používání elektronického podpisu v rámci veřejné správy a stanovuje, že elektronické podpisy jsou přijatelné pro všechny úřední dokumenty. (ČESKO, 2016)

Elektronický podpisů je více druhů. Zaručený elektronický podpis je podpis založený na certifikátech bez ohledu na to, kdo certifikáty vydá. Elektronický podpis při komunikaci občana s úřady musí být založený na kvalifikovaném certifikátu, což je certifikát vydaný státem dozorovanou certifikační autoritou. Takovému podpisu se říká uznávaný elektronický podpis. Je-li navíc tento certifikát doplněn o bezpečností prvek, tak podpis z něj vytvořený se nazývá kvalifikovaný elektronický podpis. Tímto podpisem musí komunikovat úřady s občanem. Příklad takového bezpečnostního prvku může být čipová karta s vydaným certifikátem zabezpečená PIN kódem. (ČESKO, 2016)



Obrázek 1 Druhy elektronických podpisů
Zdroj: vlastní zpracování dle (ČESKO, 2016)

1.7 Digitální certifikáty a certifikační autorita

Digitální certifikáty fungují na základě asymetrické kryptografie a principu důvěry v certifikační autoritu. (Dostálek et al., 2009)

Certifikační autorita

Certifikační autorita, dále jen CA, je důvěryhodná instituce, která vydává digitální certifikáty a provádí ověření identity a pro účely digitálního podepisování a šifrování dat v rámci internetových komunikací. Jejím hlavním úkolem je poskytovat důvěryhodné zabezpečené prostředí pro elektronické transakce a komunikace. (Peterka, 2011)

Zde je stručný přehled o funkcích a úlohách certifikační autority:

- Vydávání digitálních certifikátů,
- ověřování identity,
- správa o obnova certifikátů,
- odstoupení od certifikace. (Dostálek et al., 2009)

Získání digitálního certifikátu od CA

V následujících bodech je popsáno fungování a získání digitálního certifikátu od CA.

1. Žadatel si nejdříve musí nejdříve vygenerovat dvojici klíčů: soukromý a veřejný.
2. Žadatel následně požádá certifikační autoritu o vydání digitálního certifikátu. K žádosti připojí informace o své identitě a veřejný klíč, který chce začlenit do certifikátu.
3. CA si ověří identitu žadatele, aby se ujistila, že žadatel je skutečně ten, za koho se vydává (např. ověření dokladů, informací o společnost apod.)
4. Po ověření identity žadatele CA vydá digitální certifikát obsahující informace o identitě uživatele a jeho veřejný klíč. Následně je certifikát podepsán soukromým klíčem CA, což zajišťuje jeho důvěryhodnost a autentičnost. (Dostálek et al., 2009)

Po získání certifikátu od důvěryhodné CA může uživatel digitálně podepisovat dokumenty. Ověření digitálního podpisu vytvořeného pomocí takového certifikátu se provádí pomocí veřejného certifikátu podepisujícího a zároveň pomocí veřejného certifikátu CA. Pokud se podařilo ověřit všechny certifikáty, podpis se tak dá označit za důvěryhodný. (Peterka, 2011)

Důvěryhodný seznam Evropské unie (ETUL)

Důvěryhodný seznam Evropské unie (nebo také ETUL) je databáze, která obsahuje informace o důvěryhodných poskytovatelích služeb jako jsou například elektronické podpisy, elektronické

pečetě, časová razítka a další digitální služby v souladu s eIDAS nařízením. Díky EUTL mohou uživatelé jednoduše ověřit, zda poskytovatel služeb, který chtějí použít, splňuje stanovené bezpečnostní a důvěryhodností standardy EU. (Adobe, 2022)

Níže je seznam důvěryhodných poskytovatelů služeb v ČR:

- eIdentity
- I.CA
- PostSignum
- Správa základních registrů (Adobe, 2022)

1.8 Aplikace digitálního podpisu

Digitální podpis hraje klíčovou roli v mnoha odvětvích a oblastech, kde je potřeba zajišťovat bezpečnost, autenticitu a integritu elektronických dokumentů.

Zde jsou některé konkrétní aplikace digitálního podpisu v praxi:

- elektronický obchod (bezpečné uzavírání obchodních smluv online),
- bankovnictví (autentizace klientů, online bankovní transakce, elektronické podepisování úvěrových smluv atd.),
- právní dokumenty (nahrazení ručních podpisů ve smlouvách a notářských zápisech, urychlené ověřování platnosti podpisů),
- veřejná správa (elektronické podávání oficiálních dokumentů, formulářů a žádostí k různým úřadům),
- realitní odvětví (uzavření smlouvy o koupi, pronájmu nebo prodeji elektronicky),
- personalistika a HR (veškeré dokumenty spojené nejen s náborem zaměstnanců). (Chandrashekhara et al., 2021; Saurabh Bhausaheb Gawali, 2023)

Aplikace digitálního podpisu jsou rozmanité a zahrnují širokou škálu odvětví. Tento nástroj přináší efektivitu, bezpečnost a zjednodušení procesů v mnoha aspektech elektronické komunikace a transakcí. (Chandrashekhara et al., 2021)

1.9 Trendy a budoucnost digitálního podpisu

V následující kapitole jsou vysvětleny aktuální trendy a možná budoucnost týkající se digitálního podpisu.

Rostoucí poptávka v důsledku digitalizace

S postupující digitalizací společnosti a stále větším množstvím elektronických transakcí roste poptávka po digitálních podpisech. Očekává se, že s rostoucí digitalizací budou digitální podpisy stále více využívány v běžném každodenním životě, včetně interakcí s veřejnými institucemi, obchodem a dalšími oblastmi. (Khrykova et al., 2021)

Biometrická autentizace

Kombinace digitálních podpisů s biometrickou autentizací, jako jsou otisky prstů, rozpoznávání obličeje nebo hlasu, poskytuje další vrstvu bezpečnosti. Očekává se, že biometrická autentizace bude stále běžnější a poskytne větší bezpečnostní opatření pro digitální podpisy. (Ranashing et al., 2022)

Rozvoj mobilních aplikací

Rostoucí popularita mobilních zařízení vedla k vývoji mobilních aplikací pro digitální podpisy. Především v bankovním sektoru se můžeme setkat s aplikacemi pro potvrzování transakcí, které fungují na bázi digitálního podpisu a dvoufaktorové autentizace. (Sitorus a Chiudy, 2022)

Internetové bankovnictví a bankovní identita

Při komunikaci s bankou komunikuje klient převážně pomocí digitálního podpisu, aniž by o tom věděl. Uživatelem je nejdříve vytvořený požadavek (na přihlášení, převedení částky z bankovního účtu X na bankovní účet Y, potvrzení žádosti o úvěr apod.) a následně je uživatel vyzván k podepsání požadavku. Podpis může uživatel vytvořit heslem, nebo potvrzením požadavku v mobilní aplikaci. Požadavek je odeslaný spolu s podpisem směrem k bance, která ověří požadavek a elektronický podpis veřejným klíčem spojeným s klientem. (Hiltgen et al., 2006)

Aby banka zřídila občanovi přihlašovací údaje a s nimi i klientův vlastní soukromý klíč, tak musí nejdřív občan projít osobním ověřením na základě jeho občanského průkazu. Díky tomu státní

správa ve spolupráci s některými bankami povoluje přihlášení do určitých státních portálů přes tzn. bankovní identitu, kde může občan vyřídit spoustu věcí online. Využívání tohoto způsobu přihlášení se značně zvýšilo hlavně kvůli kovidové situaci mezi lety 2020 a 2022. (BANK ID, 2023)

Důraz na udržitelnost a ekologii

Snaha o snižování papírového odpadu a ekologický dopad vedou k přesunu k digitálním podpisům. Očekává se, že společnosti budou více upřednostňovat digitální podpisy z hlediska udržitelnosti a šetrnosti k životnímu prostředí. (Ranashing et al., 2022)

2 Historie a přechod k digitálním podpisům

V této kapitole jsou zmíněné první milníky historie a vývoje digitálních podpisů z hlediska softwaru, důvod přechodu od ručních k digitálním podpisům a softwarová využití digitálního podpisu.

2.1 Historie a vývoj digitálních podpisů

Už od prvních záznamů podpisu bylo jedno z největších rizik možnost jejich padělání. Jejich výhodou sice je vyžadování fyzické přítomnosti pro samotné podepsání dokumentu, ale i tak čelí omezené bezpečnosti. Takovéto podpisy je možné zfalšovat, nebo po podepsání upravit daný dokument, a to se velmi složitě a nákladně prokazuje. To je jeden z mnoha důvodů vzniků digitálních podpisů. (Scuola Forense di Grafologia (SFG et al., 2022)

První náznaky digitálních podpisů

S nástupem digitálního prostředí začaly vznikat potřeby pro elektronickou autentizaci, která by byla bezpečnější a efektivnější než tradiční ruční podpisy. První snahy se soustředily na využití fyzických tokenů nebo chytrých karet pro digitální podpisy spolu s experimenty s asymetrickou kryptografií a šifrovacími metodami jako prvním krokem k vytvoření bezpečných elektronických podpisů. (Dostálek et al., 2009)

Klíčové milníky ve vývoji digitálních podpisů

- 1976 – Whitfield Diffie a Martin Hellman – první zmínka o možnosti existence digitálních podpisů,
- 1977 – Ronald Rivest, Adi Shamir a Lewn Adleman – RSA algoritmus, který dokáže vyprodukovat první primitivní digitální podpis,
- 1988 – první veřejně dostupný software pro digitální podpisy na základně RSA - Lotus Notes 1.0,
- 1999 – možnost přiložení digitálního podpisu k PDF dokumentům,
- 2008 - standardizace PDF formátu dle ISO 32000. (Chandrashekhara et al., 2021)(Slayton, 2022)(Adobe, 2024)

2.2 Přechod od ručních podpisů k digitálním podpisům

S rozšiřováním informační technologie se dokumenty stále více přesouvají z fyzických forem do elektronických formátů. Digitalizace umožňuje snadnější sdílení, archivaci a ověření dokumentů, což vede ke zvýšení efektivity a urychlení pracovních procesů. S nárůstem elektronické komunikace a obchodu se zvýšila potřeba efektivních a bezpečných digitálních podpisů. Ruční podpisy se staly snadným cílem pro padělání, a tím se zvýšila potřeba spolehlivého digitálního způsobu ověření identity. (Chandrashekhara et al., 2021)

3 Softwarové a hardwarové řešení digitálních podpisů

Existuje celá řada softwarových produktů a aplikací, které umožňují vytváření a ověřování digitálních podpisů. Tyto produkty jsou rozdílné ve funkcionalitě, podporovaných formátech a úrovní zabezpečení. (Zimmer et al., 2021)

3.1 Software

Mezi nejběžnější typy softwaru pro digitální podpisy patří:

Digitální podpisové aplikace

Tyto aplikace umožňují uživatelům vytvářet a ověřovat digitální podpisy přímo na jejich zařízeních, jako jsou počítače, chytré telefony nebo tablety. Poskytují uživatelsky přívětivé rozhraní pro snadné vytváření podpisů a ověřování dokumentů. (Signotec GmbH, 2024)

Softwarové knihovny pro integraci digitálních podpisů

Tyto knihovny poskytují programátorské rozhraní (API), které umožňuje integrovat funkcionalitu digitálních podpisů do existujících softwarových aplikací. Tímto způsobem mohou vývojáři implementovat digitální podpisy do svých vlastních aplikací a systémů. (Khrykova et al., 2021)

Cloudové služby pro digitální podpisy

Tyto služby poskytují možnost vytvářet a ověřovat digitální podpisy prostřednictvím cloudových platforem. Uživatelé mohou nahrávat své dokumenty do cloudu, kde jsou podepisovány a ukládány v bezpečném prostředí. (Adobe, 2023)

3.2 Hardware

Hardwarové řešení digitálních podpisů je fyzické zařízení, které umožňuje uživatelům vytvářet, uchovávat a používat digitální podpisy s vysokou úrovní zabezpečení. Tato zařízení poskytují dodatečnou vrstvu bezpečnosti a jsou často preferována pro svou odolnost vůči kybernetickým hrozbám. (Peterka, 2011)

Zde je pohled na některé hlavní prvky hardwarových řešení digitálních podpisů:

Čtečky čipových karet

Čtečky čipových karet jsou zařízení umožňující uživatelům používat chytré karty s integrovaným čipem, který obsahuje digitální certifikáty a soukromé klíče, používané pro podpisování dokumentů. Pro zajištění ještě vyšší bezpečnosti jsou tyto karty standardně zabezpečeny PIN kódem. (Al-Khouri a Bal, 2007)

Biometrické podpisové destičky

Podpisové destičky jsou příslušenství, kter slouží k vytvoření digitálního podpisu pomocí biometrických údajů, jako jsou otisky prstů, nebo přítlaky a rychlosti při vytváření fyzického podpisu. Mimo jiné se s vytvořením digitálního podpisu šifrují právě tyto biometrické údaje a díky tomu takto vytvořený podpis má ještě další vrstvu bezpečnosti. (Al-Khouri a Bal, 2007)

USB Token

USB tokeny jsou malá paměťová zařízení, které se připojí k počítači a obsahují potřebné soubory pro vytvoření digitálního podpisu, tím je zejména soukromý klíč. Tato zařízení můžou být zabezpečeny ještě dalšími prvky, jako například potřeba PIN kódu pro přístup k těmto souborům. (Peterka, 2011)

4 Představení podniku

V následujících odstavcích bude představena firma, ve které autor navrhnul řešení zajištění dokumentů pomocí digitálního podpisu. Jedná se o automobilovou společnost Škoda Auto a.s., která je dlouhodobě největší českou firmou a největší exportér v České republice.

Právní forma podnikání firmy je akciová společnost, která spadá pod celosvětově působící koncern Volkswagen group, který vlastní 100 % akcií. Za spolehlivý chod firmy je nejvýše hierarchicky postavené představenstvo se současným předsedou představenstva Klausem Zellmerem. Každý z členů představenstva dohlíží na chod určité části podniku, základní rozdělení je následovné:

- Finance, IT a právní záležitosti
- Prodej a marketing
- Výroba a logistika
- Technický vývoj
- Lidé a kultura
- Nákup
- Komunikace, audit a produktová strategie

Každá ze zmíněných oblastí se dělí na další dvě až tři oblasti. Zajištění dokumentů pomocí digitálního podpisu má na starosti oblast IT služby spadající pod oblast Finance, IT a právní záležitosti.

4.1 Důvod potřeby digitalizace

Stejně jako spousta ostatních podniků, nejen stejného odvětví, se firma rozhodla k digitalizaci dokumentů a snížení spotřeby papíru ve všech možných procesech. Důvodů je k tomu spousta, například snížení negativního dopadu na planetu kvůli vysoké spotřebě papíru nebo také snížení nákladů na nákup a provoz tiskáren.

To jsou hlavní důvody, proč se začalo hledat elektronické řešení podpisů. Při hledání a představení různých technologií bylo ale zjištěno, že digitální podepisování dokumentů dokáže také ulehčit a zrychlit administrativní procesy, což oddělení motivuje na digitální podepisování přistoupit. Ulehčení procesů je detailněji popsáno v následujících kapitolách.

4.2 Výběrové řízení

Pro vstup externí firmy do projektu Škoda Auto musí být nejdříve vyhlášení tzn. tender (výběrové řízení). Škoda Auto zadá technické specifikace a případně další netechnické požadavky na dodavatele, následně se do tenderu přihlásí různí dodavatelé se snahou vyhovět požadavkům a stát se tak výhradním dodavatelem určité služby nebo technologie. Tímto způsobem byly Škoda Auto poskytnuté dva druhy technologií digitálních podpisů.

Signotec

Jedním typem je technologie německé firmy Signotec, která vysoutěžila řešení digitálních podpisů s biometrií. Jedná se o podpisové destičky, na které se dá speciálním perem vytvořit podpis stejně tak jako na papír. Rozdíl je však v tom, že podpisová destička zachycené biometrické údaje (rychlost psaní, přítlaky, naklonění pera atd.) zašifruje a vkládá do dokumentu spolu s podpisem.

Acrobat Sign

Druhým typem je technologie Adobe Sign, což je cloudové řešení digitálních podpisů, vhodné především pro podepisování na dálku, například zprostředkováním emailu. Odesílatel dokumentu nahraje do cloudové služby dokument, nastaví potřebné věci a protistraně, tedy podepisujícímu, odešle emailem pouze odkaz na dokument nahraný v cloudu. Pro potřeby autentizace může být před podepsáním požadováno heslo. Příjemce dokumentu dokument může podepsat na chytrém mobilu prsem nebo na počítači myší.

5 Případová studie

V praktické části této bakalářské práce je rozebraný návrh řešení implementace digitálního podpisu pomocí případové studie pro jedno z oddělení ve firmě Škoda Auto. V této kapitole jsou vysvětleny základní principy případové studie.

Případová studie popisuje konkrétní příklad nasazení a použití produktu nebo služby, v tomto případě podpisových destiček, v reálném prostředí. Případové studie jsou také důležitým způsobem, jak sdílet zkušenosti a znalosti o konkrétních projektech s organizací a širší komunitou. Tato studie obsahuje podrobné informace o tom, jakým způsobem jsou zavedeny a integrovány do existující infrastruktury a jaké přínosy či výzvy přineslo jejich nasazení. Níže jsou vypsány klíčové prvky, které byly brány v potaz při psaní případové studie. (Chrastina, 2019)

Případová studie nejdříve začíná popisem podnikového prostředí a oddělení, kde je chtěná implementace produktu nebo služby. V tomto případě tedy implementace podpisové technologie. V této části mohou být zahrnuty např. informace o velikosti podniku či oddělení, velikosti organizace, odvětví, ve kterém působí, případně jakékoliv specifické potřeby týkající se přímo nebo navrhovaného řešení. Na tuto část přímo navazuje potřeba získat od dané organizační jednotky požadavky, případně problémy, které vedly k potřebě hledání a integraci dané služby či produktu. Můžou zde být zmíněny jak potřeby a politické podmínky celé firmy, tak potřeby daného oddělení. Další část je zaměřená na výběr řešení potřebného produktu či služby. Zde je zaměřeno na analýzu dostupných možností, vyhodnocení výhod a nevýhod, porovnání nákladů na zavedení, zkoumání časové náročnosti na implementaci, zjištění komptability s existujícími postupy apod. Po rozhodnutí pro určité řešení je potřeba jej nasadit do existující infrastruktury podniku. V této části jsou popsány problémy a řešení propojení nového softwaru a hardwaru pro implementaci daného řešení. V neposlední řadě jsou shrnuty přínosy a výsledky. Případová studie by měla zhodnotit implementaci řešení v daném oddělení. To může zahrnovat například zlepšení bezpečnosti, zkrácení doby na schválení dokumentů, snížení nákladů, zlepšení uživatelského zážitků a podobně. V případové studii můžou být zmíněny i výzvy, se kterými si autor při implementaci řešení setkal, a jejich řešení. Takové výzvy mohou být např. technické, politické, morální, nebo právní. Poslední část případové studie slouží pro shrnutí postupů při implementaci řešení a shrnutí zajímavých poznatků a doporučení.(Chrastina, 2019)

6 Návrh postupu implementace pomocí případové studie

Firma Škoda Auto si je vědoma potřeby digitalizace, a to jak z pohledu ekologického, tak z pohledu nutnosti modernizace. Díky tomu se různá oddělení zasluhují o hladký přechod z papírové administrativy v digitální řešení. Díky centrálnímu systému SAP, se kterým je předávání informací mezi jednotlivými stanicemi a odděleními jednoduché, firma odbourala a zdigitalizovala ty nejobjemnější interní dokumenty. Ale digitalizaci dokumentů, které se podepisují především s externími subjekty, odkládala.

Důvodů obav z přechodu na digitální podepisování je více. V potaz je potřeba vzít právnický pohled na dokument a zda je vhodné a reálné ho digitalizovat. Další z důvodů může být pohodlí podepisujícího i administrativního pracovníka. Spousta pracovníků může mít obavy z přechodu na digitální řešení, protože se nepovažují za dostatečně technicky zdatné. Přechod na digitální podepisování s sebou také může nést nemalé náklady a je potřeba se dívat i na finanční stránku digitalizace.

Toto jsou některé aspekty, které je potřeba zvážit před rozhodnutím o zavedení digitálního podepisování dokumentů. V Servisním Centru Kosmonosy, které se zabývá servisováním vozidel Škoda pro interní zaměstnance i mimo firemní klienty, bylo rozhodnuto o hledání ideálního řešení pro zavedení digitálního podepisování dokumentů.

6.1 Popis organizačního prostředí

Servisní Centrum Kosmonosy je autorizovaný servis vozidel Škoda Auto. Digitální podepisování je chtěné vyřešit především pro deset pracovních míst, kde probíhá přímá komunikace mezi servisním poradcem a klientem. Zde je v rámci oprav podepisováno několik druhů dokumentů, nejčastější jsou GDPR, které se dělí na další dva dokumenty dle toho, zda dokument podepisuje interní zákazník nebo externí zákazník, dále interní doklad, daňový doklad a zakázkový list.

Při hledání adekvátního řešení je potřeba myslet především na pohodlí klientů, ale také na pohodlí servisních poradců a co nejvhodnějším způsobem zautomatizovat a ulehčit proces podepisování.

6.2 Původní požadavky a problémy

Vzhledem k povaze fungování firmy Škoda Auto není implementace nových technologií nejrychlejší a často z bezpečnostních důvodu ani možná. Proto je potřeba, aby se zájemci o určitý typ technologie snažili zaměřit na již dostupná a standardizovaná firemní řešení a vyvarovali se hledat nové možnosti mimo společnost. Implementace neozkoušených technologií bývá zdlouhavá, nákladná a je potřeba úzce spolupracovat s IT oddělením.

Servisní centrum v Kosmonosech má na implementaci digitálního podepisování hlavní požadavek a tím je úspora papíru. Jakožto všechna oddělení napříč firmou Škoda Auto i v Servisním centru se nyní klade velký důraz na limitování spotřeby papíru. Dalším hlavním požadavkem je snaha zefektivnit a ulehčit práci zaměstnancům pomocí vhodného řešení. Dále chce Servisní centrum poukázat na moderní prostředí, na snahu digitalizovat, na snahu zpříjemnit klientům jejich zkušenosti se servisním centrem a poskytnout vyšší bezpečnost.

6.3 Návrh možných řešení

Jak je již zmíněno výše, dodavatelé nástrojů pro zajištění dokumentů pomocí digitálního podpisu jsou již vysoutěženi. Díky tomu existují dvě řešení, která jsou možná Servisnímu centru nabídnout. Jedná se o cloudovou podepisující službu Acrobat Sign nebo o podpisové destičky a software firmy Signotec. Obě tato řešení jsou nástupci dosud jediného možného podepisování pomocí PKI certifikátu na zaměstnanecké MFA kartě. Hlavní důvod potřeby jiného řešení bylo to, že interně vydaný certifikát není pro externí subjekty považován za důvěryhodný. V následují části jsou popsány jednotlivé podpisové služby a jejich halvní rozdíly.

Tabulka 1 Porovnání podpisových metod

	Adobe Sign	Signotec destičky	PKI certifikát na MFA kartě
Místo podpisu:	Kdekoliv pomocí odkazu, který přijde na email (PC, mobil).	Osobně na místě na destičku.	Na přiděleném firemním laptopu zaměstnance.
Možnost podepisovat s externími subjekty?	ANO	ANO	NE
Potřebný hardware pro podepsání klientem:	Mobil / PC	Signotec podpisová destička	Firemní PC, MFA karta s aktivním PKI certifikátem

Zdroj: Vlastní

6.3.1 Acrobat Sign

Acrobat Sign je online služba pro elektronická a digitální podepisování dokumentů, která je součástí softwarového ekosystému Adobe Acrobat. V Adobe Sign je umožňováno uživatelům používat elektronické certifikáty pro ověření identity a autenticitu digitálních podpisů. V rámci této služby je nabídnuta uživatelům možnost spravovat a sledovat podepsané dokumenty, sledovat jejich aktuální stav, historii podpisů a získávat upozornění na aktivity související s dokumentem.

Celý postup zajištění dokumentu pomocí digitálního podpisu začíná nahráním dokumentu ve formátu PDF do online služby Adobe Document Cloud. Uživatelem je následně vybrána funkce pro přidání pole digitálního podpisu v místě dokumentu, kde to je potřeba. Případně je také možné přidat další pole pro vyplnění dodatečných informací. Dokument je poté odeslán na další uživatele, kteří ho mají podepsat. Ti obdrží oznámení e-mailem spolu s odkazem, který je přesměruje do prostředí Acrobat Sign. Zde je možné podepsat dokument různými způsoby – vložením obrázku, kreslením prstem/myší nebo vypsáním jména standardně na klávesnici. Po ukončení podepisujícího procesu je odesílateli dokumentu doručeno oznámení.

6.3.2 Podpisové destičky Signotec

Podpisové destičky jsou nástroj pro vytvoření digitálního podpisu s možností zachování i biometrických údajů, jako jsou například přítlaky pera na destičce nebo rychlost psaní. Biometrická data můžou sloužit jako další vrstva bezpečnosti. Tato technologie od firmy Signotec se skládá ze dvou komponent – hardwaru, tedy podpisové destičky jako takové a softwaru – podpisového programu, který zajišťuje chování dokumentu.

Hardware

Signotec nabízí široké portfolio destiček a dají se rozdělit do 3 kategorií. Do první skupiny spadají podpisové destičky, které mají monochromatický displej, anebo nemají žádný. Jejich hlavní výhoda je nízká pořizovací cena a malá velikost. Naopak nevýhodou je požitek z podepisování – podepisující nemusí vidět co podepisuje a odezva snímání podpisu je vysoká. Vhodné jsou především v situacích, kdy podepisující vidí na monitor, kde se zobrazí dokument, který bude podepisovat.

Obrázek 2 Podpisová destička Sigma
Zdroj: (Signotec GmbH, 2024)

Do další skupiny spadají destičky s barevným displejem. Jejich velikost není o moc větší v porovnání s destičkami z první skupiny, ale odezva snímání podpisu je značně nižší a destička dokáže zobrazit alespoň okolí místa dokumentu, kde se vytváří podpis, například část kupní s smlouvy s finální částkou.

Obrázek 3 Podpisová destička Gamma
Zdroj: (Signotec GmbH, 2024)

Do poslední skupiny spadá destička s barevným posuvným displejem. Při podepisování se na destičce zobrazí celý dokument, který si podepisující může přečíst. Nejen že disponuje nízkou odezvou a solidním rozlišením, ale tato destička se dá koupit i ve verzi s Ethernet portem. Díky tomu je možné se s destičkou spojit bezdrátově.

Obrázek 4 Podpisová destička Delta
Zdroj: (Signotec GmbH, 2024)

Software

Pro komunikaci s destičkou se využívá software Signosign/2. Jedná se o velmi výkonný program, pomocí kterého je možné nejen digitálně podepisovat PDF dokumenty, ale také automatizovat a usnadňovat práci uživateli. Některé z takových funkcionalit jsou: automatické odeslání podepsané kopie dokumentu emailem, pojmenování dokumentu na základě dat z dokumentu, vložení textu nebo obrázku, archivaci v přidělené složce a mnoho dalšího. Součástí tohoto softwaru je také MS Word doplněk, díky kterému je možné nejen lehce převést Word dokument do PDF, ale zároveň jej otevřít v Signosign/2 a zahájit podepisování na podpisové destičce.

6.4 Integrace do existující infrastruktury

Podpisové destičky značky Signotec je velmi lehké integrovat do existující infrastruktury téměř jakéhokoliv prostředí. Jejich integrace se dá rozdělit do čtyř kroků. Prvním krokem je zajištění dokumentu v PDF formátu. Dokumenty generované pro Servisní Centrum jsou již v tomto formátu generovány existujícím programem, díky tomu není potřeba podstupovat žádné další kroky.

Druhý krok souvisí se získáním softwaru. Zmiňovaný software Signosign/2 je potřeba nainstalovat na zařízení, kde probíhá vytváření digitálního podpisu. Instalační balíček lze získat z tzn. Centra Softwaru, kde se nachází všechny schválené programy firmou Škoda Auto.

Třetí krok zahrnuje výběr a nákup podpisové destičky. Destičku je možné mít připojenou USB-A kabelem přímo k pracovnímu počítači nebo dokovací stanici. V případě destičky s ethernetovým portem je možné ji mít připojenou k síti a k napájení.

Poslední krok se opět týká softwaru a z časového hlediska je nejnáročnější. Protože je chtěné, aby uživatelům podpisové destičky práci ulehčily a ne naopak, podpisový software Signosign/2 nabízí širokou škálu nastavení chování dokumentů a tím omezí zásah ze strany uživatelů na minimum. Některá z těchto nastavení jsou detailněji rozebrána v následující kapitole na příkladu dokumentů ze Servisního Centra.

6.4.1 Konfigurace Signosign/2

Jak je již zmíněno, podpisový software je možné přizpůsobit, aby uživatel měl s digitálním podpisem nejmenší námahu. Klíčovou vlastností je schopnost programu rozeznat jednotlivé typy dokumentů (např. GDPR souhlas se zpracováním osobních údajů, kupní smlouva, daňový doklad, interní doklad apod.). Rozeznání probíhá na základě nastavení identifikátoru vyskytujícím se v podpisovaném dokumentu. Jedná se tedy o nějaký textový řetězec, který je specifický pouze pro tento typ dokumentu. Při otevření dokumentu k podpisu v Signosign/2 program vyhledá, zda se některý z nastavených identifikátoru nachází v textu dokumentu a pokud ano, tak se k danému typu dokumentu chová tak, jak je pro daný dokumentový typ nastaveno.

Jedním ze základních nastavení je vytvoření podpisového pole. Každý typ dokumentů může mít místo pro podpis jinde, proto je potřeba pole vytvořit pro každý dokumentový typ zvlášť. Toto pole může mít absolutní polohu (například vždy 1 cm od pravého dolního rohu), nebo relativní (vždy vedle určitého textu).

Dalším z velmi důležitých nastavení je cílová složka pro archivaci. Zde je z bezpečnostních důvodu vhodné užití úložiště jiného než lokálního. Ve firmě Škoda Auto se nabízí možnost ukládání na OneDrive, Sharepoint nebo na síťové úložiště, které si Servisní Centrum zvolilo. Spolu s archivací souvisí nastavení pojmenování dokumentů, které může být nastavené pevně tak, že se vždy dokument pojmenuje přednastaveným textem. Nebo relativně, kdy se dokument pojmenuje na základě textu z podepisovaného dokumentu (např. jméno zákazníka) nebo datumem podpisu souboru (např. GDPR_<<jmeno_zakaznika>>). Případně je také možnost pojmenování kombinovat (např. GDPR_<<jmeno_zakaznika>>_<<dnesni_datum>>).

Vzhledem k digitalizaci dokumentů je potřeba aby i podepisující měl digitálně podepsaný dokument k dispozici. Z tohoto důvodu je možné využít nastavení e-mailové služby v Signosign/2. Nastavení emailové služby je jednoduché zejména díky součinnosti Signosign/2 a MS Outlooku. Pro dokumentový typ lze přednastavit základní parametry, jako je emailová adresa příjemce, další emailová adresa v kopii, předmět emailu a text emailu. Tyto údaje mohou být nastaveny podobně, jako výše zmíněné nastavení jména dokumentu. Lze nastavit pevně daný text, nebo potřebný text převzít z podepisovaného dokumentu. Pokud je, mimo jiné, na dokumentu emailová adresa příjemce, lze ji automaticky vyplnit před odesláním emailu. Stejně tak lze vložit např. jednotlivé položky z faktury a finální částku do textu samotného emailu, nebo vložit název firmy do předmětu emailu. Nastavení je možné přizpůsobit tak, aby se buď email automaticky odeslal bez zásahu uživatele, nebo aby se nejdříve otevřelo okno nového emailu v Outlook a uživatel případně mohl provést nutné změny. Podepsaný dokument je automaticky vložen do přílohy.

Spousta dokumentů je podepisovaných jak zákazníkem, tak zaměstnancem servisního centra. Řešením této situace může být buď přidání dalšího podpisového pole, nebo automatické vložení podpisu do dokumentu. S tím souvisí i jeden z požadavků Servisního centra, kde pod podpis zaměstnance Servisního centra je potřeba vložit razítko. Řešení je stejné pro oba požadavky, nejdříve je potřeba vytvořit si obrázek podpisu zaměstnance a obrázek razítka. Následně je potřeba u obou obrázků odebrat pozadí v některém z dostupných grafických editorů a nakonec v Signosign/2 nastavit místo, kam je potřeba tyto obrázky vložit. Vložení je opět možné buď na základě absolutního umístění, nebo relativního.

Správa a údržba

Řešení podpisových destiček od firmy Signotec spolu s podpisovým softwarem Signosign/2 je téměř bezproblémové a nejsou potřeba žádné velké zásahy ze strany uživatelů nebo administrátorů. Ze strany IT je zapotřebí v Centru Softwaru udržovat aktuální verzi Signosign/2, kterou je následně možné nainstalovat u jednotlivých uživatelů.

Certifikáty

Certifikát, který se použije pro šifrování digitálního podpisu, je možné změnit. Defaultně je certifikát nastavený od dodavatele, který splňuje eIDAS normy, a tak je možné jej využít i pro komunikaci s externími subjekty. V případě potřeby je certifikát možné změnit na interní, tedy vydaný interní

certifikační autoritou Škoda Auto. Digitální podpis zašifrovaný interním certifikátem může sloužit pouze pro interní účely.

6.5 Přínosy a výsledky

Celkový postup implementace řešení byl zdlouhavý, a to především kvůli specifickým potřebám servisního centra. Během snahy konfigurace Signosign/2 se autor setkal s chybami a situacemi, které byly nutné konzultovat a řešit s dodavatelem. Délka doby implementace se prodlužuje i z důvodů nutnosti spolupracovat s dalším IT oddělením ohledně nahrání opravené verze softwaru do Centra softwaru, což je také časově náročný proces. Dalším důvodem zdržení byly jiné rozpracované projekty Servisního oddělení, které měly vyšší prioritu. A v neposlední řadě celý proces prodlužuje nerozhodnost oddělení o vhodném řešení. Vzhledem k tomu, že na Servisní centrum není vytvářený žádný časový nátlak o nutnosti implementovat řešení co nejdříve, oddělení má možnost prozkoumat všechna možná řešení a případně zvážit i nějaké, které ještě není ve firmě implementované. Vzhledem ke všem těmto zdržením, oddalováním a potřebné doby pro testování je projekt již 4 měsíce rozpracovaný. Nicméně v případně potřeby zajistit funkční řešení co nejdříve by implementace obdobného řešení trvala méně než 1 měsíc. Díky flexibilitě podpisového softwaru je také možné řešit spoustu detailů za pochodu a není potřebné mít kompletní řešení při přechodu z ručních podpisů na digitální podpisy.

Autorova doporučení pro rychlejší nasazení řešení zahrnují pevně nastavené termíny, užší spolupráci s IT oddělením, předem nastavená očekávání a požadavky. Dále by bylo vhodné zajistit větší informovanost oddělení o možných řešení ve firmě a co vše taková řešení zahrnují.

V poslední části bakalářské práce je zahrnutý ekonomický pohled na implementaci řešení pro digitální podpisy zaměřený převážně na náklady a návratnosti investice. I přes to, že to jsou jedny z nejdůležitějších metrik pro měření implementace nového řešení, tak to nejsou jediné metriky. Je potřeba zaměřit se i na pohodlí servisních poradců, zda je pro ně určité řešení vhodným řešením, či nikoliv. Obecně se dá sledovat časová efektivita, jak rychle jsou schopni odbavit klienta prostým podpisem na papír a jak rychle pomocí podpisové destičky. Nicméně rychlost není vždy vhodné měřítko, zrovna v servisním centru není tak důležitá. Díky urychlení administrativy se ale může servisní poradce více věnovat klientovi a pracovat s ním na osobním sblížení. Zároveň je potřeba sbírat zpětnou vazbu od klientů, zda je pro ně nové moderní řešení zajímavé a pohodlné, či nikoliv.

V čase psaní bakalářské práce je v servisním centru podpisové destička v pilotním provozu, a tak ještě není možné uvést definitivní závěr a výsledky celého procesu implementace. Nicméně na základě dosavadní zpětné vazby pracovníků v servisním centru se dá říct, že na tuto technologii se dívá pozitivně. Nejen v rámci podepisování dokumentů s klienty servisního centra, ale i v rámci interních předávacích protokolů a dalších kroků, kde se stále tisknou dokumenty na papír. Hlavní výhodou je zmíněná lehkost implementace do existujících procesů.

Na následujícím obrázku je znázorněný příklad, jakým lze zjednodušit proces podepsání dokumentu. Nejen že jednotlivých kroků je méně, ale také jsou jednodušší, rychlejší a s menší pravděpodobností se mezi kroky udělá lidská chyba.

Obrázek 5 Porovnání procesů podepisování
Zdroj: Vlastní

Díky jednoduchosti vytvoření podpisu na destičce není třeba se obávat reakcí klientů, tedy podepisujících na destičce. K dispozici mají pero se speciálním hrotem, který není moc rozdílný od klasické kuličkové propisky a destičku, na kterou je potřeba vytvořit podpis, pod kterou se dá představit papír. Celý proces pro podepisujícího je tedy velmi intuitivní. Pomocí digitalizace podpisů je celý proces urychlený i z pohledu klientů a oddělením je tak poukázáno na snahu modernizovat procesy a také na zaměření se na snížení negativního dopadu na planetu.

6.6 Výzvy a řešení

Určitou výzvou na digitální podpisy jsou právnické záležitosti o tom, zda je možné daný dokument digitalizovat a v digitální formě jej i archivovat. Na takovéto otázky je ve firmě právní oddělení, se kterým je možné všechny situace konzultovat.

Další výzvou může být zajištění bezpečnosti podepsaných dokumentů a zabránění neoprávněnému přístupu k těmto datům. Díky propracovanému podpisovému softwaru je možné tyto dokumenty archivovat v existující infrastruktuře. Možná úložiště pro takováto data mohou být např. SharePoint, OneDrive, připojená síťová jednotka nebo i speciální úložiště jiného existujícího programu. Všechna tato úložiště mají zabezpečený způsob přístupu k datům a je možné se spolehnout na jejich zabezpečení.

Za zmínění také stojí výzva o přesvědčení uživatelů o přínosech podpisových destiček. Je potřeba budoucí uživatele řádně seznámit s podpisovými destičkami a motivovat k aktivnímu přestupu na tuto technologii. Standardní uživatele hlavně zajímá, co všechno bude muset dělat navíc, a proto je důležité řádně nakonfigurovat Signosign/2, aby naopak měl práce méně, než kdyby dokumenty tisknul a skenoval.

6.7 Závěr a doporučení

Digitalizace dokumentů je nezbytným krokem v každém prostředí, kde to legislativa dovoluje. A to jak z důvodů modernizace, tak kvůli snížení dopadu na přírodu. V mnoha případech digitalizace dokumentů může vést i ke snížení nákladů na administraci, provoz tiskáren, skladování dokumentů a nákup papírů jako takových. Díky digitálnímu podepisování je možné digitalizovat dokumenty bez obav jejich padělání po podepsání a kde je to nutné, tam je možné i sbírat údaje, které běžně není možné zachytit na klasickém ručním podpisu. Další výhodou je možnost podepsání dokumentu vzdáleně a stále mít jistotu o autentičnosti osoby.

Na začátku celého procesu implementace digitálních podpisů je potřeba řádně zmapovat nejen celý proces, kde se digitalizace zvažuje, ale také i procesy, které mu předcházejí nebo následují. Je nutné zamyslet se nad tím, zda se digitálním podepisováním nenaruší některý z procesů, nebo zda by nebylo výhodnější jiné řešení pro hladké předávání dokumentů mezi jednotlivými kroky.

6.8 Ekonomický přínos řešení

Z ekonomického pohledu na implementaci řešení podpisových destiček je možné zmínit úspory nákladů na provoz tiskáren vůči nákladům na pořízení potřebného hardwaru a licencím. Napříč firmou Škoda Auto se využívají tiskárny značky Canon, které má ve vlastnictví firma Canon a jsou pouze pronajímány na základě leasingové smlouvy. Za každou tiskárnu je placená určitá částka korespondující s daným typem tiskárny. Spolu s tímto nákladem je placená licence firmwaru pro vzdálenou správu tiskáren, která je jednotná pro všechny typy. Dále se společnosti Canon platí variabilní částka za každý vytisknutý papír za spotřebu inkoustu. Nakonec do nákladů spadá částka za spotřebovaný papír jako takový. V závislosti na barvě dokumentu, velikosti papíru a typu tiskárny se částka za jeden vytisknutý papír může pohybovat cca od 0,7 Kč/list až do 1,3 Kč/list. Průměr na jeden vytisknutý list papírů je ve firmě Škoda Auto 0,99 Kč/list.

Jak je již zmíněno výše, podpisových destiček je více druhů. Nejlevnějším je Signotec Sigma za 4`056 Kč, dále Signotec Gamma za 6`465 Kč a nejdražším řešením je Signotec Delta v ceně 10`776 Kč. Náklady za nákup hardwaru jsou provázeny i náklady za software Signosign/2. První nákup licence softwaru je zpoplatněný částkou 2`500 Kč za první rok. Každý další rok se platí tzn. maintanence poplatek 433 Kč za obnovení licence. Pomocí těchto údajů je možné vypočítat dobu návratnosti investice, tedy za jak dlouho se oddělení vrátí investovaná částka do podpisových destiček oproti nákladům na tiskárny.

Jednoduchý vzorec (1) vytvořený pro tento účel se na skládá z čitatele, který znázorňuje celkové náklady na nákup a provoz podpisových destiček a jmenovatele, který znázorňuje náklady na využívání tiskáren. Čitatel se skládá z jednorázové částky za nákup softwaru 2500 Kč, částky za maintanence 433 Kč vynásobenou Y lety, zohlednění, že první rok se maintanence neplatí -433 Kč a připočtením variabilní částky za destičku PAD, pro kterou se oddělení rozhodne. Jmenovatel se následně skládá z částky za jeden vytištěný list papíru 0,99 vynásobený předpokládaným ročním počtem tisků PT.

$$Y = \frac{2500 - 433 + 433Y + PAD}{0{,}99 * PT} \tag{1}$$

Y = počet let

PAD = náklady na podpisovou destičku

PT = předpokládaný počet tisků za 1 rok

Na základě těchto informací a vzorečku pro výpočet doby, za jak dlouho se podpisové destičky splatí, je zřetelné, že čím vyšší počet podepsaných papírů se očekává, tím dříve bude nákup a provoz technologie splacený a zároveň tím vyšší jsou očekávané úspory oproti tisknutí dokumentů.

Obdobným způsobem je možné spočítat ekonomický přínos i druhého možného řešení, tedy Adobe Sign. Ve firmě Škoda Auto stojí jeden podepsaný dokument v Adobe Sign 1 Kč. Spolu s touto částkou platí firma i za provoz v místním prostředí určitou fixní částku, nicméně ta není nijak ovlivněná počtem podepsaných dokumentů, nebo počtem oddělení, která toto řešení využívají. Z tohoto důvodu nebude s touto částkou počítáno. Z těchto informací je zřejmé, že rozdíl nákladů na jeden vytisknutý list papíru a nákladů na jeden podepsaný dokument v Adobe Sign je dodatečný náklad ve výši 0,01 Kč na každý digitálně podepsaný dokument.

Z čistě ekonomického hlediska se tedy dá říct, že implementace Adobe Sign je neekonomická a pro firmu se nevyplatí. Stejným způsobem by se dala konstatovat situace, kdy počet podepsaných dokumentů na podpisové destičce by byl nižší než 429 ks (při nižším počtu by se nezaplatila ani maintanence licence za 433 Kč ročně). Ovšem v některých situacích nelze sledovat pouze ekonomickou stránku věci, ale je nutné se zamyslet nad všemi aspekty přechodu na digitální podpisy. I přes to, že Adobe Sign by bylo v každém případě nákladnější, tak stojí za zamyšlení zvážit jeho ostatní výhody. Pro administrativní pracovníky by takové řešení mohlo být úlevou díky možnosti řešit digitální podepisování na dálku, sledovat proces podepisování, lehce přístupné digitální dokumenty apod. Další ekonomickou výhodou je to, že Adobe Sign je řešení, které nepotřebuje žádný dodatečný hardware, který by byl potřeba servisovat, nebo u kterého hrozí fyzické poškození či opotřebení.

Digitalizace dokumentů může ulehčit práci administrativním pracovníkům. Nejen že zde nejsou zohledněny náklady na archivaci, ale v potaz je potřeba vzít i lehčí přístup k digitálně archivovaným souborům. A v neposlední řadě je výhodou i snížení negativního dopadu na planetu.

Závěr

Digitální podpisy se stávají nedílnou součástí moderního digitálního prostředí a přináší řadu výhod v oblasti zabezpečení dokumentů a elektronických transakcí. Cílem této bakalářské práce bylo čtenáři poskytnout komplexní pohled na digitální podpisy a jejich využití pro zajištění dokumentů pomocí případové studie.

V rámci teoretické části byly prozkoumány rozdíly mezi elektronickým a digitálním podpisem a principy jejich fungování. Dále byl zmíněn vývoj a historické začátky digitálních podpisů a v neposlední řadě softwarová a hardwarová řešení. V této části bakalářské práce autor mimo jiné kladl důraz na bezpečnost a nutnost využívání digitálních podpisů, a to hlavně díky jejich vlastnostem, které zahrnují bezpečné ověření identity podepisujícího, časové razítko, nedopustitelnost odmítnutí podepisujícím, pečeť zajišťující neměnnost dokumentu a v neposlední řadě šifrování asymetrickou kryptografií.

Praktická část se nejdříve zaměřila na představení podniku a prostředí, dále nás provedla procesem výběru vhodného řešení a jeho nasazením. Případová studie se úzce soustředila na specifika prostředí Škoda Auto a spojení s již funkčními a implementovanými systémy. Nasazení elektronického podepisování zjednodušilo celý procesní tok, a to jak z hlediska časové úspory snížením jednotlivých kroků, tak z ekonomického pohledu snížením nákladů na provoz tiskáren. Dále implementace podpisových destiček zmodernizovala prostředí, ve kterém je firma v úzkém kontaktu se zákazníky a klienty a díky tomu i zlepšila své služby, které jim poskytuje.

Na závěr lze říct, že digitální podpisy představují klíčový nástroj pro modernizaci a zjednodušení procesů a bezpečné zajištění dokumentů, a to nejen v organizaci. Nasazení řešení pro digitální podepisování přináší řadu výhod z hlediska bezpečnosti, časové náročnosti a v některých případech i z hlediska nákladů. Je však důležité se zaměřit na zajištění souladu s právním rámcem a zajistit správné školení pro uživatele této technologie. Díky častějšímu využívání digitálních podpisů při komunikaci se zákazníky a klienty firma buduje povědomí o existenci této technologie a uživatelé s dobrými zkušenostmi mohou zvážit používání obdobné technologie i pro soukromé účely. V dnešní moderní době to nemusí být pouhé digitální podepisování dokumentů pro jednání se státní správou, ale v rámci projektu digitalizace Evropské Unie, do kterého je zapojené i Česko, je možné vyřídit většinu administrativních záležitostí bezpečně online a často i bez administrativních poplatků. Využívání digitálních podpisů jako digitálního prokázání identity se bude zajisté rozrůstat

a dříve nebo později se bez svého vlastního digitálního podpisu nikdo neobejde.

Seznam použité literatury

GENERÁLNÍ ŘEDITELSTVÍ PRO KOMUNIKAČNÍ SÍTĚ, OBSAH A TECHNOGLOIE, 2023. Nařízení eIDAS. Online. In: Evropská komise. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/eidas-regulation. [citováno: 2024-02-25].

ADOBE, 2022. Důvěryhodný seznam Evropské unie. Online. In: Adobe. Dostupné z: https://helpx.adobe.com/cz/document-cloud/kb/european-union-trust-lists.html. [citováno: 2024-02-25].

ADOBE, 2024. How to open, view and work with the PAdES format. Online. ©2024. In: Adobe. Dostupné z: https://www.adobe.com/uk/acrobat/resources/document-files/pdf-types/pades.html. [citováno 2024-02-25].

SIGNOTEC, 2024. PDF signature with signoSign/2. Online. ©2024. In: Signotec e-signature solutions. Dostupné z: https://en.signotec.com/software/pdf-signature-windows/signosign-2/. [citováno 2024-02-25].

BANK ID, 2023. Informace pro uživatele Bank iD. Online. 2023. In Bank iD. Dostupné z: https://www.bankid.cz/caste-dotazy. [citováno 2024-04-13]

ADOBE, 2023. Cloud-based digital signatures. Online. In: Adobe. Dostupné z: https://helpx.adobe.com/sign/config/send-settings/auth-methods/cloud-signature.html. [citováno: 2024-02-25].

ČESKO, 2016. Zákon č. 297 ze dne 24. srpna 2016 o službách vytvářejících důvěru pro elektronické transakce. In: *Sbírka zákonů České republiky*, částka 115, s.4466-4468. ISSN 1211-1244. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=61057

A. KROPÁČOVÁ, [s. a.]. Bezpečnost elektronických dat a elektronické komunikace. online. roč. 2006, č. 4. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/522.html.

AL-KHOURI, A.M. a J. BAL, 2007. Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics. online. *Journal of Computer Science*, roč. 3, č. 6, s. 361–367. Dostupné z: https://doi.org/10.3844/jcssp.2007.361.367.

AUMASSON, Jean-Philippe; Samuel NEVES; Zooko WILCOX-O'HEARN a Christian WINNERLEIN, 2013. BLAKE2: Simpler, Smaller, Fast as MD5. online. In: JACOBSON, Michael; Michael LOCASTO; Payman MOHASSEL a Reihaneh SAFAVI-NAINI (ed.). *Applied Cryptography and*

Network Security, s. 119–135. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg. Dostupné z: https://doi.org/10.1007/978-3-642-38980-1_8.

BURDA, Karel, 2019. *Kryptografie okolo nás*. 1. vydání. Praha: CZ.NIC, z.s. p.o. ISBN 978-80-88168-49-2.

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

HILTGEN, A.; T. KRAMP a T. WEIGOLD, 2006. Secure Internet banking authentication. online. *IEEE Security & Privacy Magazine*, roč. 4, č. 2, s. 21–29. Dostupné z: https://doi.org/10.1109/MSP.2006.50.

CHANDRASHEKHARA, J.; Anu V B; Prabhavathi H a Ramya B R, 2021. A COMPREHENSIVE STUDY ON DIGITAL SIGNATURE. online. *International Journal of Innovative Research in Computer Science & Technology*, roč. 9, č. 3. Dostupné z: https://doi.org/10.21276/ijircst.2021.9.3.7.

CHRASTINA, Jan, 2019. *Případová studie - metoda kvalitativní výzkumné strategie a designování výzkumu = Case study - a method of qualitative research strategy and research design*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-5373-6.

JOSE, Robin Thomas, 2015. A Comparative Study on Different Hashing Algorithms. online. *7*, č. 3. ISSN 2320-9801. Dostupné z: https://www.ijircce.com/special-issues/pdf/2015/october/30_212.pdf.

KHRYKOVA, Anastasia; Marina BOLSUNOVSKAYA; Svetlana SHIROKOVA a Andrey NOVOPASHENNY, 2021. Implementation of digital signature technology to improve the interaction in company. online. *E3S Web of Conferences*, roč. 244, s. 12023. Dostupné z: https://doi.org/10.1051/e3sconf/202124412023.

OULEHLA, Milan a Roman JAŠEK, 2017. *Moderní kryptografie*. Praha: IFP Publishing s.r.o. ISBN 978-80-87383-67-4.

PETERKA, Jiří, 2011. *Báječný svět elektronického podpisu*. Praha: CZ. NIC. ISBN 978-80-904248-3-8.

RANASHING, Om; Prateek HAJARE a Hussain SHEIKH, 2022. Future of Online Signatures: The One-Sign Feature. online. *International Journal of Research in Science and Technology*, roč. 12, č. 02, s. 06–11. Dostupné z: https://doi.org/10.37648/ijrst.v12i02.002.

SAURABH BHAUSAHEB GAWALI, 2023. A Comprehensive Study on Digital Signatures. online. *International Journal of Advanced Research in Science, Communication and Technology*. 2023-06-18. s. 37–39. Dostupné z: https://doi.org/10.48175/IJARSCT-11608.

SCUOLA FORENSE DI GRAFOLOGIA (SFG; Pàvlos KIPOURÀS; a SCUOLA SUPERIORE DI PERIZIE (SSP), 2022. THE EVOLUTION OF THE SIMULATED SIGNATURE BY THE FORGER. online. *International Journal of Law in Changing World*, roč. 1, č. 2, s. 60–72. Dostupné z: https://doi.org/10.54934/ijlcw.v1i2.25.

SITORUS, Rolib a Cathryn Aurora CHIUDY, 2022. The Effectiveness of Use of Electronic Signatures in Managing Banking Transactions Based on ITE Law. *LEGAL BRIEF*, roč. 12, č. 1. ISSN 2722-4643, 1979-522X.

SLAYTON, Rebecca (ed.), 2022. *Democratizing cryptography: the work of Whiteld Diffie and Martin Hellman*. First Edition. ACM books, #42. New York, NY, USA: Association for Computing Machinery. ISBN 978-1-4503-9828-2.

STAPLETON, Jeffrey James a W. Clay EPSTEIN, 2016. *Governance, risk, and compliance for PKI operations*. 1st vyd. Boca Raton: Auerbach. ISBN 978-1-4987-0748-0.

STINSON, Douglas R., 1995. *Cryptography: theory and practice*. The CRC Press series on discrete mathematics and its applications. Boca Raton: CRC Press. ISBN 978-0-8493-8521-6.

ZIMMER, J.; N. KALANTZIS; T. DZIEDZIC; J. HECKEROTH; E. KUPFERSCHMID et al., 2021. The challenge of comparing digitally captured signatures registered with different software and hardware. online. *Forensic Science International*, roč. 327, s. 110945. Dostupné z: https://doi.org/10.1016/j.forsciint.2021.110945.