ŠKODA AUTO VYSOKÁ ŠKOLA o.p.s.

Studijní program: Podniková ekonomika a manažerská informatika

Využití elektronických podpisů jako nástroje efektivní digitalizace ve ŠKODA AUTO a.s.

Bakalářská práce

Lukáš Horák

Vedoucí práce: Ing. Lukáš Herout, Ph.D.

Tento list vyjměte a nahraďte zadáním závěrečné práce s elektronickými podpisy.
Pozor, v tištěné verzi musí být zadání vytištěné oboustranně.

Prohlašuji, že jsem závěrečnou práci vypracoval samostatně a použité zdroje uvádím v seznamu literatury. Prohlašuji, že jsem se při vypracování řídil vnitřním předpisem ŠKODA AUTO VYSOKÉ ŠKOLY o.p.s. (dále jen ŠAVŠ) směrnicí Vypracování závěrečné práce.

Jsem si vědom, že se na tuto závěrečnou práci vztahuje zákon č. 121/2000 Sb., autorský zákon, že se jedná ve smyslu § 60 o školní dílo a že podle § 35 odst. 3 je ŠAVŠ oprávněna mou práci využít k výuce nebo k vlastní vnitřní potřebě. Souhlasím, aby moje práce byla zveřejněna podle § 47b zákona č. 111/1998 Sb., o vysokých školách.

Beru na vědomí, že ŠAVŠ má právo na uzavření licenční smlouvy k této práci za obvyklých podmínek. Užiji-li tuto práci, nebo poskytnu-li licenci k jejímu využití, mám povinnost o této skutečnosti informovat ŠAVŠ. V takovém případě má ŠAVŠ právo ode mne požadovat příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to až do jejich skutečné výše.

V Mladé Boleslavi dne 24.10.2022

Děkuji Ing. Lukáši Heroutovi, Ph.D. za odborné vedení závěrečné práce, poskytování rad a informačních podkladů. Dále děkuji společnosti ŠKODA AUTO a.s. za možnost stáže na toto téma a mému koordinátorovi Bc. Kamilu Veselému MBA. Mé poděkování patří také společnosti Signotec za poskytnutí interních informací ohledně jejich produktu a daného tématu.

Obsah

Úvod 8

1 Elektronický podpis a jeho vymezení 9

1.1 Co je elektronický podpis? 9

1.2 Nařízení eIDAS 9

1.3 Tři typy elektronických podpisů dle nařízení eIDAS 9

1.3.1 Prostý elektronický podpis 10

1.3.2 Zaručený elektronický podpis 10

1.3.3 Kvalifikovaný elektronický podpis 10

1.4 Elektronický a digitální podpis 11

1.5 Elektronické značky 12

1.6 Časová razítka 13

1.7 Biometrický podpis 15

1.8 Digitální podpis 16

2 Technologické aspekty elektronického podpisu 18

2.1 Hashování a hashovací funkce 18

2.2 Klíče a asymetrická kryptografie 19

2.3 Certifikáty 20

2.3.1 Komerční a kvalifikované certifikáty 21

2.3.2 Certifikační autority 22

2.4 PKI 22

2.5 Ověřování platnosti elektronických podpisů 23

3 Problematika využití elektronického podpisu v praxi 24

3.1 Náklady 24

3.2 Vnímání veřejnosti 25

3.3 Adopce uživatele 25

3.4 Zpoždění 25

3.5 Právní uznání 25

3.6 Kompabilita 25

4 Zhodnocení konkrétní implementace elektronických podpisů v rámci ŠKODA AUTO a.s. 26

4.1 Typy podpisů ve ŠKODA AUTO 26

4.1.1 DigiPodpisy 27

4.1.2 Adobe Sign 28
4.1.3 První Certifikační autorita (I. CA) 28
5 Návrh změn vedoucích ke zvýšení pozitivních aspektů využívání el. podpisů 30
5.1 Aktuální řešení ve ŠKODA AUTO a.s. 30
5.2 Navrhované řešení použití biometrických elektronických podpisů ve ŠKODA AUTO a.s. 31
5.2.1 Využití nového procesu – oddělení SO 32
5.2.2 IT Point – oddělení FIO 32
5.2.3 Oddělení SB 35
5.3 signoSign2 36
5.4 Shrnutí budoucnosti elektronického podpisu 36
Závěr 38
Seznam literatury 39
Webové stránky 39
Seznam obrázků a tabulek 41

Seznam použitých zkratek a symbolů

DNS	Hierarchický, decentralizovaný systém doménových jmen
eIDAS	Nařízení EU, které stanoví standardy pro elektronickou identitu, autentizaci a podpisy
EU	Evropská Unie
GDPR	Obecné nařízení o ochraně osobních údajů
ISDS	Informační systém datových schránek
PKI	Public Key Infrastructure (označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie)
RSA	Iniciály autorů Rivest, Shamir, Adleman. Jedná se o šifru s veřejným klíčem

Úvod

Společnosti se neustále snaží inovovat a zlepšovat své procesy, vzhlíží do budoucna a adaptují se podmínkám jak ve světě tak ale i podmínkám kolem nich. Zároveň ale k vzrůstající tendenci trendu digitalizace se snaží přejit z prostředí náročného na papír k prostředí bez papíru, pomocí digitalizace.

Organizace odcházejí od tradičních, časově náročných papírových procesů a hledají nové a inovativní technologie ke zvýšení efektivity. Elektronické a digitální podpisy jsou jednim z nich, mohou významně prospět organizacím tím, že odstraní poslední papír v obchodním cyklu. Schopnost okamžitě podepisovat a elektronicky zapečetit dokumenty a transakce má za následek mnohem kratší doby procesních cyklů a to má zá následek zrychlené služby zákazníkům a zároveň to přináší značné úspory nákladů a času. Elektronické a digitální podpisy poskytují vylepšené pohodlí jak pro zákazníka, tak pro organizaci a usnadňují tak chod společnosti.

Takové řešení je zároveň ale i environmentálně přátelské a dokáže tak pomoci omezit zbytečnou spotřebu papíru v organizaci. Toto řešení bude obzvláště výhodné pro jednu z největších společností v České republice, společnost ŠKODA AUTO a.s.. Obzvlášť když jeden z cílů které si stanovila je právě být environmentálně přátelska. A pomáhá k tomu například projektem vysazování nových stromů, kde už šestnáctým rokem vysazuje nový strom za každý prodaný vůz.

Hlavním cílem bakalářské práce je analyzovat možnosti a přístupy k využívání elektronických podpisů jako součásti digitalizace vnitropodnikových procesů. Na konkrétním případě v rámci vybraného oddělení/části ŠKODA AUTO a.s. zmapovat pozitivní a negativní aspekty využití el. podpisů a navrhnout případné změny vedoucí ke zvýšení očekávaných benefitů.

1 Elektronický podpis a jeho vymezení

1.1 Co je elektronický podpis?

Elektronický podpis, také známý jako e-podpis, je digitální ekvivalent vlastnoručního podpisu. Slouží k ověřování elektronických dokumentů a k prokázání totožnosti a úmyslu při elektronických transakcích. Elektronické podpisy lze používat v různých kontextech, jako jsou finanční transakce, smlouvy a právní dokumenty, a poskytují bezpečný a pohodlný způsob elektronického podepisování a ověřování dokumentů. Mnoho zemí uznává elektronické podpisy jako právně závazné a jejich používání je regulováno zákony a předpisy, jako je eIDAS v Evropské unii (Budiš, Petr; Štědroň, Bohumír, 2008).

1.2 Nařízení eIDAS

Nařízení eIDAS (Electronic IDentification, Authentication and trust Services) je nařízení Evropské unie, které stanovuje pravidla pro elektronickou identifikaci a ověřování osobnosti v Evropské unii. Cílem tohoto nařízení je poskytnout jednotný a spolehlivý rámec pro elektronickou identifikaci a ověřování osobnosti, aby se zajistilo, že elektronické služby a transakce jsou bezpečné a důvěryhodné. Nařízení eIDAS také stanovuje pravidla pro používání elektronických podpisů a dalších elektronických ověřovacích nástrojů. Nařízení eIDAS udává *„že elektronickému podpisu by neměly být upírány právní účinky na základě skutečnosti, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis.“* (Smejkal, 2019) Ačkoliv tedy že samotný elektronický podpis nemá nejvyšší úroveň zabezpečení *„měly by být v zvláštních případech, přijímány rovněž elektronické podpisy s nižší zárukou bezpečnosti.“* (Smejkal, 2019).

1.3 Tři typy elektronických podpisů dle nařízení eIDAS

„Nařízení eIDAS definuje tři úrovně elektronického podpisu: prostý elektronický podpis, zaručený elektronický podpis a kvalifikovaný elektronický podpis. Požadavky každé úrovně vycházejí z požadavků úrovně pod ní, takže nejvíce požadavků splňuje kvalifikovaný elektronický podpis a nejméně jednoduchý elektronický podpis.“ (Evropská komise, 2022).

1.3.1 Prostý elektronický podpis

Prostý elektronický podpis je nejjednodušší forma elektronického podpisu, která se používá k ověření identity osoby, která podepsala dokument. Tento typ podpisu nemusí být nutně garantován certifikační autoritou a nemusí být právně závazný. Pod daným elektronickým podpisem si můžeme představit něco tak jednoduchého, jako je napsání vašeho jménoa pod e-mail (Evropská komise, 2022).

1.3.2 Zaručený elektronický podpis

„Zaručený elektronický podpis je elektronický podpis, který je navíc:

- *jedinečně propojený a schopný identifikovat signatáře;*
- *vytvořené způsobem, který umožňuje signatáři zachovat si kontrolu;*
- *propojeny s dokumentem tak, aby byla zjistitelná jakákoli následná změna údajů.*

Nejčastěji používanou technologií schopnou zajistit tyto funkce je použití infrastruktury veřejného klíče (PKI), která zahrnuje použití certifikátů a kryptografických klíčů.“ (Evropská komise, 2022). Je to druh elektronického podpisu, který je garantován certifikační autoritou. To znamená, že certifikační autorita potvrzuje pravost a důvěryhodnost zaručeného elektronického podpisu. Tento typ elektronického podpisu je považován za právně závazný.

1.3.3 Kvalifikovaný elektronický podpis

Kvalifikované elektronické podpisy, známé také jako zaručené elektronické podpisy, jsou nejbezpečnější formou elektronického podpisu. Jsou garantovány certifikační autoritou a jsou právně závazné. K vytvoření kvalifikovaného elektronického podpisu je zapotřebí zařízení pro vytváření kvalifikovaného podpisu a kvalifikovaný certifikát pro elektronické podpisy. Tato zařízení mohou mít podobu čipových karet, SIM karet, USB klíčů nebo zařízení pro vzdálenou tvorbu podpisů, které spravuje poskytovatel. Kvalifikované certifikáty poskytují kvalifikovaní poskytovatelé uvedení v národních „důvěryhodných seznamech“ každého členského státu EU. V celé EU jsou uznávány pouze kvalifikované elektronické podpisy, které mají stejný právní účinek jako vlastnoruční podpisy. (Evropská komise, 2022).

1.4 Elektronický a digitální podpis

Zásadní je ale také vysvětlit rozdíl mezi elektronickým a digitálním podpisem. Tyto pojmy se často používají zaměnitelně, ale ve skutečnosti jsou odlišné. Elektronický podpis je jakýkoli typ označení, které může sloužit jako ekvivalent vlastnoručního podpisu na elektronickém dokumentu. To se může pohybovat od napsaného jména ve spodní části e-mailu až po biometrický podpis zachycený specializovaným zařízením pro elektronický podpis.

Digitální podpisy jsou na druhé straně pokročilejší formou elektronického podpisu, který využívá šifrování a další bezpečnostní opatření k zajištění pravosti a integrity podepsaného dokumentu. Na rozdíl od elektronických podpisů jsou digitální podpisy jedinečné pro každého podepisujícího a vyžadují použití digitálního certifikátu, což je druh elektronického identifikačního dokumentu vydaného důvěryhodnou třetí stranou. Digitální certifikát slouží jako spojení mezi podepisujícím a podepsaným dokumentem, ověřuje identitu podepisujícího a umožňuje mu bezpečně podepsat dokument.

Pro lepší pochopení tohoto konceptu můžeme digitální certifikát přirovnat k řidičskému průkazu nebo pasu. Stejně jako tyto dokumenty je digitální certifikát jedinečný pro jednotlivce a slouží jako doklad totožnosti pro konkrétní účel. Cestovní pas například ověřuje totožnost jednotlivce ve vztahu k jeho státní příslušnosti a umožňuje mu legálně cestovat do určité země s řádným oprávněním. Obdobným způsobem se digitální certifikát používá k elektronickému prokazování totožnosti.

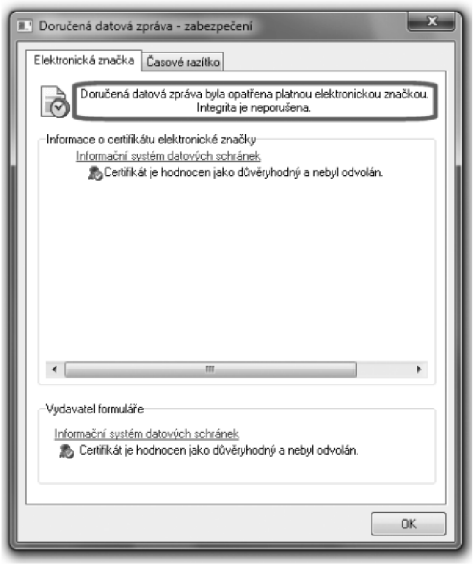
Jednou z klíčových výhod používání digitálního podpisu je, že jsou zaznamenány jakékoli změny podpisu nebo dokumentu, což znemožňuje jeho padělání. Tato přidaná vrstva zabezpečení a důvěry zajišťuje, že s dokumentem nebylo manipulováno a že podepisující osoba je tím, za koho se vydává.

Závěrem, hlavní rozdíl mezi těmito dvěma typy podpisů je ten, že digitální podpis se používá k zabezpečení dokumentu, zatímco elektronický podpis se používá k ověření dokumentu. I když elektronické podpisy mohou poskytnout určitou úroveň jistoty, nejsou tak bezpečné nebo spolehlivé jako digitální podpisy a neměly by se používat v situacích, kdy má pravost nebo integrita dokumentu zásadní význam.

(Rybka, Michal; MALÝ, Ondřej, 2002)

1.5 Elektronické značky

Elektronické značky jsou druh elektronického podpisu, které se používají k ověření identity organizace nebo právnické osoby. Jedná se o digitální ekvivalent fyzické pečeti, která se používá k ověření legitimity dokumentu nebo transakce. Elektronické značky se typicky používají v kontextu veřejné správy, kde poskytují vyšší úroveň bezpečnosti a důvěry ve srovnání s jinými typy elektronických podpisů. Elektronické značky jsou vytvářeny pomocí zařízení pro bezpečné vytváření podpisů a kvalifikovaného certifikátu pro elektronické pečeti. Uznává se, že mají stejný právní účinek jako vlastnoruční podpisy v kontextu nařízení Evropské unie eIDAS (Štědroň, 2007).



Zdroj: (Peterka, 2011)

Obr. 1 Příklad (uznávané) elektronické značky na datové zprávě v ISDS

Používání elektronických podpisů se rozrostlo v reakci na potřeby jednotlivých uživatelů a organizací. To vedlo k vývoji systémů elektronického podpisu, které mohou využívat právnické osoby, jako jsou společnosti, k podepisování dokumentů bez přímé účasti osoby. Tyto systémy napodobují proces vlastnoručního podpisu a jsou právně závazné, přičemž důsledky jakéhokoli podpisu dopadají na osobu, která systém zřídila. To umožňuje organizacím používat elektronické podpisy jako pohodlnou a bezpečnou alternativu k tradičním papírovým podpisům (Štědroň, 2007).

1.6 Časová razítka

Časové razítko je typ elektronického podpisu, který obsahuje informaci o době, kdy byl vytvořen. To poskytuje bezpečný způsob sledování vytváření a úprav dokumentu a zajišťuje, že nemůže být narušena jeho integrita. Časová razítka se vytvářejí pomocí specializovaného softwaru nebo služeb a připojují se k dokumentu spolu s elektronickým podpisem.

Jednou z klíčových výhod používání časových razítek je, že poskytují digitální pečeť, která zvyšuje důvěryhodnost dokumentu a podpisu k němu připojeného. Časové razítko totiž slouží jako nezávislé ověření času, kdy byl podpis vytvořen, a znemožňuje dodatečnou změnu dokumentu nebo podpisu nebo s nimi manipulovat.

Kromě běžných časových razítek existují i kvalifikovaná časová razítka, která vytváří kvalifikovaný poskytovatel služby. Ty jsou považovány za „silnější“ než běžná časová razítka, protože poskytují další úroveň zabezpečení a důvěry. Kvalifikovaná časová razítka jsou vytvářena pomocí kvalifikovaných zařízení pro vytváření podpisů a kvalifikovaných certifikátů a jsou garantována certifikační autoritou.

Celkově použití časových razítek ve spojení s elektronickými podpisy nabízí výkonné řešení pro sledování vytváření a úprav dokumentů a pro poskytování další vrstvy zabezpečení a důvěry. To může být užitečné zejména v situacích, kdy má pravost a integrita dokumentu zásadní význam, například při právních nebo finančních transakcích.(Peterka, 2011)

Zdroj: (Peterka, 2011)

Obr. 2 Příklad (kvalifikovaného) časového razítka na datové zprávě v ISDS

Shrnutí označení daných forem elektronického podpisu, včetně připomenutí jaký daný uživatel může daný podpis použít:

elektronický podpis	*„bez přívlastku“*	podepsanou osobou může být pouze fyzická osoba
	zaručený	
	uznávaný	
elektronická značka	*„bez přívlastku“*	označující osobou může být jak fyzická osoba, tak i právnická osoba či organizační složka státu
	uznávaná	
časové razítko	*„bez přívlastku“*	
	kvalifikované	

Zdroj: (Peterka, 2011)

Obr. 3 Klasifikace podpisů, značek a razítek

1.7 Biometrický podpis

Biometrický podpis není úplně klasický elektronický podpis, nicméně sdílí s ním společnou autentizační vlastnost.

Je založen zejména na biomotorických/biometrických vlastnostech konkrétního člověka.

Biometrické atributy jsou fyzické nebo behaviorální charakteristiky, které lze použít k identifikaci jednotlivce. V kontextu biometrického podpisu se tyto atributy používají k zachycení a ověření jedinečnosti podpisu jednotlivce.

Některé běžné biometrické atributy používané v systémech biometrických podpisů zahrnují tvar a velikost podpisu, tlak aplikovaný na pero nebo jiný psací nástroj, rychlost a směr podpisu a načasování a trvání podpisu. Tyto atributy jsou měřeny a zaznamenávány systémem biometrických podpisů a poté porovnávány s referenčním podpisem pro ověření identity podepisujícího.

Další biometrické atributy, které mohou být použity v systémech biometrických podpisů, zahrnují charakteristiky otisků prstů, rozpoznávání obličeje a skenování duhovky nebo sítnice. Tyto atributy se běžněji používají v jiných typech biometrických identifikačních systémů, ale lze je také použít v kombinaci s biometrickými systémy založenými na podpisu, aby poskytly další vrstvu zabezpečení a přesnosti.

Daný podpis tudíž musí proběhnout na nějaké konkrétní podpisové destičce se specializovaným perem s použitím podpisového softwaru umožňující sběr těchto dat, protože né každá podpisová destička má tuto možnost a pokud se tato možnost dá na daném zařízení využít tak bývá nastavitelná a nemusí se tudíž vždy používat. Vzhledem k tomu že samotný podpis na takovém zařízení je sám o sobě, šifrovaný tak se né vždy tato možnost využívá. Také pro využití takového nastavení pro sběr těchto dat je potřeba souhlas podepisujícího uživatele vzhledem k GDPR, protože se jedná o citlivé osobní údaje, i když konkrétně biometrický podpis není definován žádnou legislativou. Zároveň díky tomu, že se v podepsaném dokumentu uchovávají jedinečné charakteristiky daného podepisujícího, umožňuje daný podpis jednoznačné spojení podepisujícího se dokumentem a tudíž nabízí nejvyšší možnost prokazatelnosti. Je tedy jasné, že v porovnání s klasickým tradičným podpisem obyčejným perem na papíře je biometrický podpis bezpečnější. Po samotném podpisu je daný dokument šifrován proti manipulaci. Jakkýkoliv pokus

o změnu informací či podpisu v daném dokumentu, daný podpis automaticky zneplatní. Hlavním benefitem oproti ostatním formám podpisu je jeho přirozenost bez nároku na zaškolení podepisujícího uživatele. Přece jenom jakmile se naučíme psát tak se zároveň naučíme i jak se podepisovat, proto je to pro nás přirozené. Nikdo se nikdy ale nepodepíše dvakrát úplně stejným způsobem, protože ale ověření biometrického podpisu může sledovat přirozené výkyvy každého člověka v průběhu času, tak může snadno určit i padělání (Budiš, Petr; Štědroň, Bohumír, 2008).

1.8 Digitální podpis

Digitální podpis je elektronický podpis, který je podložen digitálním certifikátem. Digitální podpisy vyhovují předpisům po celém světě a poskytují nejvyšší úroveň zabezpečení identity při práci s digitálními dokumenty.

„*Proces (nebo procedura) ověřování digitálního podpisu se skládá z ověřovacího algoritmu spolu s metodou pro obnovu dat ze zprávy*." (Menezes, Oorschot, vanstone, 1997) jedná se o takzvaný matematický algoritmus který pomáhá ověřovat autentičnost a integritu daného dokumentu. Svým způsobem vytváří digitální stopu která je jedinečná k danému podepisujícímu a tudíž zajišťuje aby při přenosu mezi podepisujícím a příjemcem daného dokumentu nedocházelo k žádnému vnějšímu ovlivnění už podepsaného dokumentu. V případě že by k takovému ovlivnění došlo bude daný podpis zněplatněn.

Digitální podpis pracuje s několika zabezpečovacími funkcemi, jsou to: hašovací funkce, asymetrická kryptografie, PKI, certifikační autorita, digitální certifikát. V kapitole 2 se podrobněji ponoříme do technologických aspektů elektronického podpisu.

Digitální podpisy fungují pomocí kryptografie veřejného klíče, kde jsou generovány dva klíče: veřejný klíč a soukromý klíč. Tyto klíče jsou matematicky propojené dvojice, které se navzájem ověřují. Osoba vytvářející podpis používá svůj soukromý klíč k zašifrování dat spojených s podpisem, zatímco příjemce podpisu používá veřejný klíč podepisujícího k dešifrování dat. Pokud příjemce nemůže otevřít dokument pomocí veřejného klíče podepisujícího, je problém buď s dokumentem, nebo se samotným podpisem.

Tento systém však není bez nedostatků. Pokud osoba vytvářející podpis neuchová svůj soukromý klíč v tajnosti, je možné, že někdo, kdo získá přístup k soukromému

klíči, vytvoří podvodné digitální podpisy jménem držitele soukromého klíče. Je to proto, že soukromý klíč se používá k zašifrování nebo podepsání dokumentu a jeho uzamčení, zatímco veřejný klíč se používá pouze ke čtení dokumentu. Vlastní generování kódu a šifrování dokumentů probíhá v procesorové jednotce počítače, takže uživatel nevidí proces tak, jak k němu dochází (Rybka, Michal; MALÝ, Ondřej, 2002).

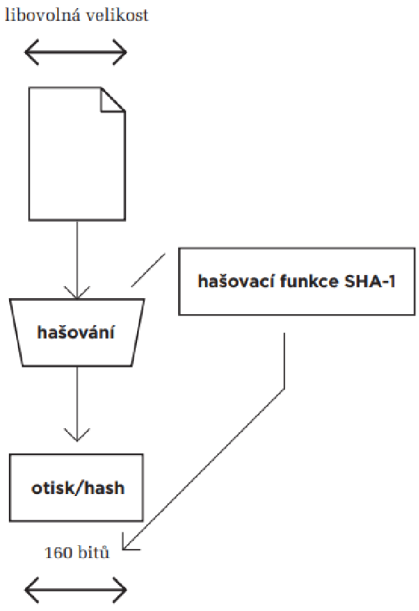
2 Technologické aspekty elektronického podpisu

2.1 Hashování a hashovací funkce

Digitální podpis je matematická technika používaná k ověření identity odesílatele digitální zprávy nebo dokumentu. Je založena na konceptu hashovací funkce, což je matematická funkce, která bere vstup libovolné velikosti a mapuje jej na výstup s pevnou velikostí. Výstup, známý jako hodnota hash, je jedinečný otisk původního vstupu.

Chcete-li vytvořit digitální podpis, odesílatel nejprve vytvoří hodnotu hash digitální zprávy nebo dokumentu pomocí funkce hash. Odesílatel poté zašifruje hodnotu hash pomocí svého soukromého klíče a vytvoří digitální podpis. Digitální podpis je poté připojen k původní zprávě nebo dokumentu a odeslán příjemci.

Příjemce poté použije veřejný klíč odesílatele k dešifrování digitálního podpisu, čímž odhalí původní hodnotu hash. Příjemce pak pomocí stejné hashovací funkce vytvoří vlastní hash hodnotu přijaté zprávy nebo dokumentu. Pokud se dvě hodnoty hash shodují, příjemce si může být jistý, že se zprávou nebo dokumentem nebylo během přepravy manipulováno a že byly skutečně odeslány odesílatelem, který tvrdí, že je odeslal. Tímto způsobem je hashovací funkce nezbytnou součástí digitálního podpisu a poskytuje bezpečný a spolehlivý způsob ověření pravosti digitální zprávy nebo dokumentu.



Zdroj: (Peterka, 2011)

Obr. 4 Představa hašování (s hašovací funkcí SHA-1)

Hlavním důvodem pro potřebu hashování je také to, že při daném podpisu(ale i při označování, neboli při vytváření elektronických značek, stejně jako při vytváření časových razítek, při šifrování apod.) pracujeme s bloky dat o pevné velikosti. Technologie(metody a algoritmy), která se k podepisování používá, to zkrátka vyžaduje. Zmenšením dat na menší, stanovenou velikost nám pomáha s rychlejším zpracováním elektronického podpisu a jeho zašifrováním(Peterka, 2011).

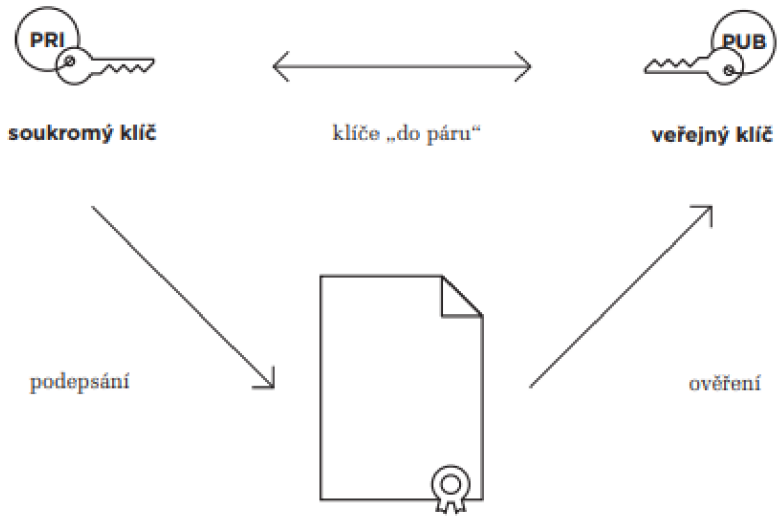
2.2 Klíče a asymetrická kryptografie

Klíče a asymetrická kryptografie v kontextu elektronických podpisů označují použití dvojice doplňkových klíčů za účelem ověření pravosti digitálního podpisu. Jednou z klíčových technologií elektronických podpisů je asymetrická kryptografie, která používá k vytváření a ověřování podpisů dvojici doplňkových klíčů. Soukromý klíč, který podepisující osoba uchovává v tajnosti, se používá k vytvoření podpisu, zatímco veřejný klíč slouží k ověření podpisu. Tento přístup se nazývá asymetrický, protože klíče mají různé vlastnosti a slouží různým účelům.

Použití asymetrické kryptografie v elektronických podpisech poskytuje několik důležitých výhod. Za prvé, zajišťuje bezpečnost podpisu tím, že znesnadňuje neoprávněným stranám podpis padělat nebo pozměnit. Za druhé, umožňuje efektivní ověřování podpisů, protože veřejný klíč může být snadno distribuován a použit kýmkoli k ověření pravosti podpisu. Konečně umožňuje neodmítnutí, což znamená, že podepisující nemůže popřít, že podepsal dokument, jakmile byl podpis ověřen.

Jedním z nejpoužívanějších typů asymetrické kryptografie je algoritmus RSA, který je založen na výpočetní složitosti faktorizace velkých celých čísel. V tomto přístupu se veřejný klíč skládá ze dvou čísel, která jsou součinem dvou velkých prvočísel, zatímco soukromý klíč je odvozen ze stejných prvočísel. Bezpečnost šifrování přímo souvisí s velikostí klíče, přičemž větší klíče poskytují silnější šifrování. Kvůli pokroku v technologii se od používání 1024bitových klíčů upustilo, protože se očekává, že budou v blízké budoucnosti zranitelné vůči útoku.

Celkově je použití asymetrické kryptografie v elektronických podpisech zásadní pro zajištění bezpečnosti a integrity digitální komunikace. Tím, že poskytuje robustní prostředky pro ověřování pravosti elektronických dokumentů, pomáhá budovat důvěru a důvěru v digitální svět(Algoritmus RSA, 2022).



Zdroj: (Peterka, 2011)

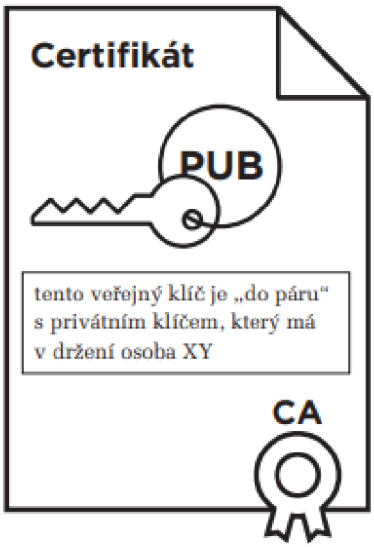
Obr. 5 Představa využití soukromého a veřejného klíče

2.3 Certifikáty

Klíčovou roli ve světě elektronických podpisů hrají certifikáty, které poskytují prostředek k ověření identity podepisujícího a pravosti podpisu. Certifikát je digitální dokument, který obsahuje informace o podepisující osobě, jako je její jméno a kontaktní údaje, a také veřejný klíč, který lze použít k ověření podpisu. Obsahuje také informace o vydavateli certifikátu, jako je certifikační autorita, což je důvěryhodná entita, která je odpovědná za vydávání a správu certifikátů.

Použití certifikátů nabízí několik významných výhod, včetně možnosti pro příjemce podepsaného dokumentu ověřit identitu podepisujícího a integritu podpisu, zajištění bezpečnosti elektronických podpisů prostřednictvím prevence proti padělaným nebo falešných certifikátů a umožnění efektivní ověřování podpisů pomocí veřejného klíče obsaženého v certifikátu.

Celkově je používání certifikátů zásadním aspektem technologie elektronického podpisu, protože pomáhá budovat důvěru v digitální svět. Poskytováním robustních prostředků pro ověření identity podepisujícího a pravosti podpisu hrají certifikáty zásadní roli při zajišťování bezpečnosti a integrity elektronické komunikace (Peterka, 2002).



Zdroj: (Peterka, 2011)

Obr. 6 Představa certifikátu

Certifikáty se můžou udělat jak fyzickým tak také i právnickým osobám či organizačním složkám státu. Těmto certifikátům říkáme systémové certifikáty, které mohou být vytvářeny jak například pro elektronické značky (ve smyslu předešlé zmíněné kapitoly 1.6) tak i pro vytváření časových razítek (zmíněno v kapitole 1.7) či další účely jako je identifikace a šifrování komunikace serverů. (Peterka, 2011)

2.3.1 Komerční a kvalifikované certifikáty

Existuje několik kategorií certifikátů, včetně komerčních a kvalifikovaných certifikátů. Požadavky a obsah kvalifikovaných certifikátů stanoví zákon, zatímco obsah komerčních certifikátů zákon nestanoví. V praxi se pro podepisování a ověřování podpisů, značek a razítek používají kvalifikované certifikáty (osobní i systémové). Pro jiné účely, jako je šifrování, přihlašování, prokazování identity a ověřování, by se měly používat komerční certifikáty (Peterka, 2011).

Vydávání kvalifikovaných certifikátů je upraveno nařízením EU č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na trhu (eIDAS) a zákonem č.297/2016 Sb., o službách vytvářejících

důvěru pro elektronické transakce.(I.CA. O společnosti I.CA., 2022). Jedna z prvních takových českých firem která získala akreditaci poskytovatele certifikačních služeb ve smyslu původního zákona č. 227/2000 Sb., o elektronickém podpisu byla právě společnost I.CA.

Nejzásadnějším rozdílem mezi kvalifikovaným a komerčním certifikátem je, že komerční certifikát je totiž vydáván bez jakýchkoliv legislativních záruk a není na tento druh certifikátu kladen žádný požadavek ze strany zákona, svým způsobem je dána volnost v jejich využití zatímco bezpečnost a důvěryhodnost kvalifikovaný certifikat je kontrolovaná a standardizována příslušnými úřady. Kvalifikovaným certifikátem tudíž vytvoříme zaručený elektronický podpis a dokážeme jim zajistit integritu a auntencitu dat. (Jaký je rozdíl mezi kvalifikovaným a komerčním certifikátem? (Hájková, 2010)

2.3.2 Certifikační autority

Certifikační autorita (CA) je entita, která vydává a spravuje digitální certifikáty. Tyto certifikáty se používají k ověření identity jednotlivců nebo organizací a k navázání kryptografických klíčů na ně. CA vystupuje jako důvěryhodná třetí strana, ověřuje identitu předmětu certifikátu a zajišťuje, že s certifikátem nebylo manipulováno. Když je podepsaný certifikát předložen třetí straně, může tato strana použít digitální podpis CA k ověření pravosti certifikátu. Tímto způsobem hraje CA zásadní roli při zajišťování bezpečnosti a integrity digitálních certifikátů.

2.4 PKI

Jedním z nejdůležitějších atributů každého certifikátu je jeho důvěryhodnost neboli míra, do jaké můžeme důvěřovat informacím obsaženým v certifikátu. Každý certifikát obsahuje veřejný klíč ve kterém je uvedena identita osoby spojená s tímto klíčem. Tato osoba také vlastní odpovídající soukromý klíč. Důvěryhodnost každého certifikátu lze hodnotit individuálně.

Použití digitálních podpisů ve spojení s infrastrukturou veřejných klíčů (PKI) zvyšuje bezpečnost těchto podpisů a snižuje potenciální bezpečnostní problémy spojené s přenosem veřejných klíčů a ověřováním jejich vlastnictví. Zabezpečení digitálního podpisu do značné míry závisí na ochraně soukromého klíče. Bez PKI není možné prokázat něčí identitu nebo zrušit kompromitovaný klíč, což by mohlo umožnit

zlomyslným aktérům vydávat se za někoho jiného bez toho aniž by zde byla možnost jakýchkoli prostředků ověření.

PKI lze považovat za digitální ekvivalent voskové pečeti, která se v minulosti používala k zabezpečení citlivých zpráv. V této analogii funguje PKI jako pečeť, která ověřuje pravost odesílatele a integritu zprávy. Stejně jako pečeť na fyzickém dopise potvrzuje PKI identitu odesílatele a zajišťuje, že se zprávou během přepravy nebylo manipulováno. I když se zprávy již neposílají na koních, stále cestují sítí serverů, routerů a dalších zařízení, než dosáhnou svého cíle. Bez ochrany PKI by tyto zprávy mohly být snadno pozměněny nebo zmanipulovány kyberzločinci.

Chcete-li uvést konkrétnější příklad, představte si odeslání zprávy příteli nebo kolegovi. Když příjemce obdrží zprávu, je doprovázena voskovou pečetí, která potvrzuje totožnost odesílatele a integritu zprávy. Neporušená pečeť naznačuje, že zpráva je legitimní dvěma zásadními způsoby. Za prvé, design pečeti potvrzuje totožnost odesílatele, protože pouze odesílatel by měl mít přístup k této konkrétní pečeti. Když příjemce uvidí pečeť, může si být jistý, že zpráva je od odesílatele. Za druhé, neporušená pečeť také naznačuje, že se zprávou během přepravy nebylo manipulováno. Příjemce si může být jistý, že zpráva byla chráněna před jakýmikoli pokusy o změnu jejího obsahu. PKI funguje na stejném principu a zajišťuje, že zpráva je chráněna před manipulací a že lze ověřit identitu odesílatele (Adams, Lloyd, 2003)

2.5 Ověřování platnosti elektronických podpisů

Validace elektronického podpisu zahrnuje ověření pravosti podpisu a integrity dokumentu. To se provádí pomocí veřejného klíče podepisujícího, který je obsažen v digitálním certifikátu. Veřejný klíč slouží k ověření podpisu na dokumentu, a pokud je podpis platný, je považován za účinný elektronický podpis.

Existuje několik různých metod ověřování elektronických podpisů a konkrétní použitá metoda bude záviset na typu použité technologie. Některé systémy mohou například používat centrální úložiště digitálních certifikátů, kde jsou uloženy veřejné klíče podepisujících a lze k nim přistupovat za účelem ověření. Jiné systémy mohou používat decentralizovaný přístup, kdy jsou veřejné klíče distribuovány mezi strany zapojené do procesu podepisování.

Celkově je ověřování elektronických podpisů důležitou součástí zajištění bezpečnosti a integrity elektronických dokumentů. Pomocí důvěryhodné technologie a osvědčené metody ověřování mohou organizace zajistit, že jejich elektronické podpisy jsou právně závazné a lze se na ně u soudu spolehnout (BUDIŠ, Petr; ŠTĚDROŇ, Bohumír, 2008).

Při ověřování platnosti elektronických podpisů jsou možné tyto tři možné výstupy:

- *„zjištěním, že elektronický podpis je platný: jsme schopni ověřit a prokázat platnost podpisu*
- *zjištěním, že elektronický podpis je neplatný: jsme schopni ověřit a prokázat neplatnost podpisu.*
- *zjištěním, že „nevíme" (že platnost podpisu nedokážeme posoudit, že nejsme schopni ověřit, zda podpis je či není platný)*" (Peterka, 2011).

3 Problematika využití elektronického podpisu v praxi

V této kapitole prozkoumáme problematiku používání elektronického podpisu v praxi se zaměřením na výzvy a potenciální problémy, které mohou při implementaci této technologie nastat.
Kromě toho prozkoumáme potenciální rizika a zranitelná místa spojená s používáním elektronických podpisů a poskytneme doporučení pro řešení těchto problémů, abychom zajistili bezpečné a efektivní používání této technologie. Celkově tento příspěvek poskytne ucelený přehled problematiky používání elektronických podpisů v praxi a upozorní na potenciální výzvy jejich bezpečného a efektivního používání.

3.1 Náklady

Jednou z nevýhod elektronických podpisů je jejich cena. K zašifrování souboru digitálním podpisem je vyžadován ověřovací software a podpisové certifikáty od certifikačních autorit. Používání podpisových destiček také znamená dodatečné náklady, které mohou být značné v závislosti na potřebném počtu. Může být také nutné proškolit zaměstnance a další osoby o správném používání elektronických podpisů. Celková hodnota elektronických podpisů je závislá na úsporách dosažených v jiných oblastech, jako je tisk a ukládání souborů.

3.2 Vnímání veřejnosti

V některých případech mohou být elektronické podpisy vnímány jako méně důvěryhodné nebo spolehlivé než fyzické podpisy. To může vést ke nedůvěře a může ztížit jednotlivcům a organizacím přesvědčit ostatní o platnosti a zákonnosti jejich elektronických podpisů.

3.3 Adopce uživatele

Někteří jedinci se mohou bránit používání elektronických podpisů kvůli nedostatečné znalosti nebo nedostatečnému pohodlí s danou technologií. To může znesnadnit účinné zavádění a používání elektronických podpisů a může to vyžadovat školení a podporu, která podpoří přijetí a používání.

3.4 Zpoždění

Dalším problémem je možnost technických problémů nebo poruch. Systémy elektronického podpisu se spoléhají na komplexní technologii, a pokud selžou nebo nefungují, může to vést ke zpožděním nebo narušení obchodních procesů.

3.5 Právní uznání

Použití elektronických podpisů nemusí být v některých situacích právně uznáno. Zatímco mnoho zemí a jurisdikcí má zákony, které uznávají platnost elektronických podpisů, mohou existovat určité typy dokumentů nebo transakcí, pro které je fyzický podpis stále vyžadován. To může způsobit zmatek a nejistotu pro jednotlivce a organizace, které používají elektronické podpisy.

3.6 Kompabilita

S používáním elektronických podpisů mohou být spojeny technické problémy, jako je kompatibilita s různými softwarovými a hardwarovými systémy a potřeba zajištění bezpečného přenos a ukládání elektronických dokumentů.

4 Zhodnocení konkrétní implementace elektronických podpisů v rámci ŠKODA AUTO a.s.

Používání elektronických podpisů je v posledních letech stále běžnější a organizace napříč různými odvětvími tuto technologii zavádějí, aby zefektivnily své procesy podepisování a zlepšily bezpečnost svých dokumentů. V tomto zhodnocení se zaměříme na konkrétní implementaci elektronického podpisu v rámci ŠKODA AUTO as, předního výrobce automobilů.

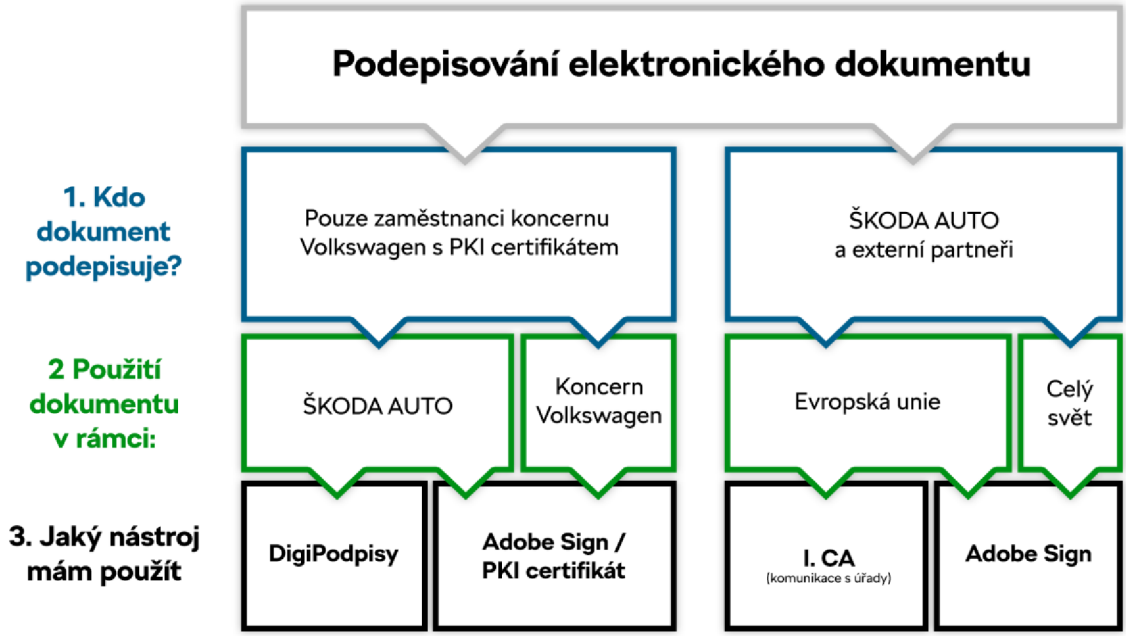
Prozkoumáme různé způsoby podepisování elektronických dokumentů, které ŠKODA AUTO as využívá, včetně digitálních podpisů a dalších typů elektronických podpisů. Probereme také technologii a procesy, které se používají pro ověřování elektronických podpisů, abychom zajistili pravost a integritu podepsaných dokumentů.

Dále prozkoumáme výhody a potenciální výzvy používání elektronického podpisu v rámci organizace a poskytneme doporučení pro zlepšení implementace této technologie ve ŠKODA AUTO a.s. Celkově toto hodnocení poskytne komplexní přehled o používání elektronických podpisů v rámci organizace a upozorní na výhody a potenciální oblasti ke zlepšení.

4.1 Typy podpisů ve ŠKODA AUTO

Ve ŠKODA AUTO a.s. existuje několik různých způsobů podepisování elektronických dokumentů. Tyto metody zahrnují použití digitálních podpisů, což je typ elektronického podpisu, který využívá specifickou technologii k zajištění pravosti a integrity dokumentu. Tato technologie, která je často založena na infrastruktuře veřejných klíčů (PKI), zahrnuje použití digitálního certifikátu, který vydává důvěryhodná třetí strana, jako je certifikační úřad (CA). Certifikát obsahuje veřejný klíč podepisujícího, který se používá k ověření podpisu na dokumentu (Rybka, Michal; MALÝ, Ondřej, 2002).

Celkově používání elektronického podpisu ve ŠKODA AUTO a.s. umožňuje efektivnější a bezpečnější způsob podepisování dokumentů, protože eliminuje potřebu fyzických podpisů a zajišťuje pravost a integritu dokumentů. To nejen zrychluje a zjednodušuje proces podepisování, ale také pomáhá snížit riziko podvodu a zajistit soulad s právními požadavky.



Zdroj: (Portál ŠKODA AUTO a.s., 2022)

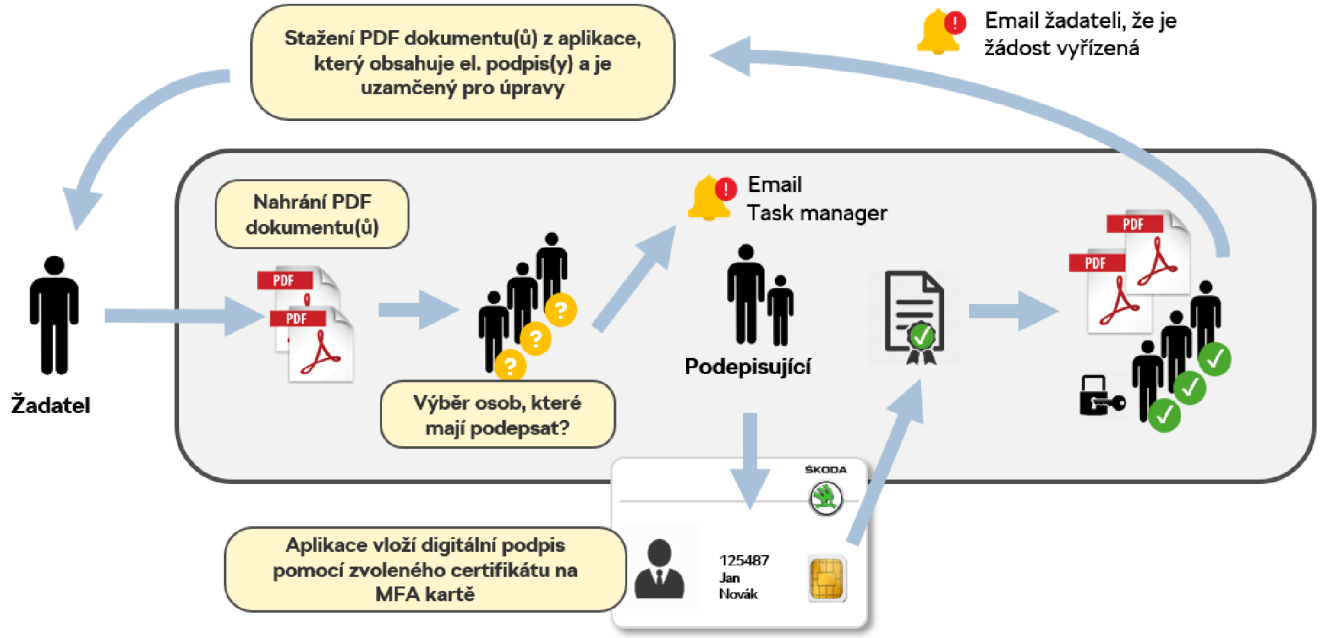
Obr. 7 ***Podepisování elektronického dokumentu v rámci ŠKODA AUTO a.s.***

Kromě digitálních podpisů ŠKODA AUTO a.s. také umožňuje použití jiných typů elektronických podpisů, jako jsou biometrické podpisy a vlastnoruční podpisy, které jsou zachyceny elektronicky. Tyto podpisy lze použít na řadě různých dokumentů, včetně smluv, dohod a dalších právních dokumentů.

4.1.1 DigiPodpisy

Webová aplikace DigiPodpisy slouží výhradně zaměstnancům ŠKODA AUTO a.s. pro elektronické podepisování PDF dokumentů několika uživateli najednou. Aplikaci může využívat každý zaměstnanec ŠKODA AUTO a.s., který má MFA kartu s aktivovaným PKI čipem a současně aktivní firemní emailovou schránku ve tvaru: xxx.yyy@skoda-auto.cz.

DigiPodpisy lze použít na dokumentech v rámci koncernu Volkswagen. Zde se můžeme podívat na následující proces fungování DigiPodpisu ve firmě ŠKODA AUTO a.s.:



Zdroj: (Portál ŠKODA AUTO a.s., 2022)

Obr. 8 Fungování DigiPodpisu ve firmě ŠKODA AUTO a.s.

4.1.2 Adobe Sign

Adobe Sign je jedním z nástroju ve ŠKODA AUTO a.s. sloužící pro elektronické podepisování jakýchkoliv dokumentů či smluv bez potřeby složitého zajišťování fyzických podpisů a posílání tištěných dokumentů. Využívá se ve ŠKODA AUTO a.s. zejména v rámci dodavatelských vztahů a obchodních činnosti. Hlavní výhodou je že přes jeden dokument se může podepsat více osob, přičemž tyto podepisující osoby nemusí být zaměstnanci ŠKODA AUTO a.s., ale mohou to být právě i osoby druhé smluvní strany. Jediné co musí daný zaměstnanec mít pro použití tohohle nástroje je funkční MFA karta přes kterou se přihlásí do interní sítě ŠKODA AUTO a.s. a dále musí mít přidělené externí jednatelské oprávnění (Portál ŠKODA AUTO a.s., 2022).

4.1.3 První Certifikační autorita (I. CA)

Certifikační autorita (CA) je entita, která vydává digitální certifikáty, které se používají k určení vlastnictví veřejného klíče. Digitální certifikáty jsou elektronické

dokumenty, které používají digitální podpis ke spojení veřejného klíče s identitou. Tato vazba umožňuje použití certifikátu pro ověření pravosti elektronického podpisu.

Aby mohl CA vydat digitální certifikát, musí nejprve ověřit identitu subjektu, který certifikát požaduje. To se obvykle provádí prostřednictvím procesu známého jako registrace certifikátu, kdy CA shromažďuje identifikační informace a ověřuje je proti autoritativnímu zdroji, jako je státem vydaný průkaz totožnosti. Jakmile je identita ověřena, CA vytvoří digitální certifikát a použije svůj vlastní soukromý klíč k podepsání certifikátu, čímž vytvoří digitální podpis.

Digitální certifikát je poté vydán subjektu a lze jej použít k vytvoření elektronického podpisu na elektronických dokumentech. Když je dokument podepsán digitálním certifikátem, podpis je vytvořen pomocí soukromého klíče, který odpovídá veřejnému klíči v certifikátu. To umožňuje každému, kdo má certifikát, ověřit pravost podpisu pomocí veřejného klíče certifikátu.

Stručně řečeno, certifikační autorita hraje klíčovou roli v procesu vytváření a ověřování elektronických podpisů vydáváním digitálních certifikátů, které vážou veřejný klíč k identitě. To umožňuje subjektům bezpečně podepisovat elektronické dokumenty způsobem, který mohou ostatní ověřit. (Peterka, 2002).

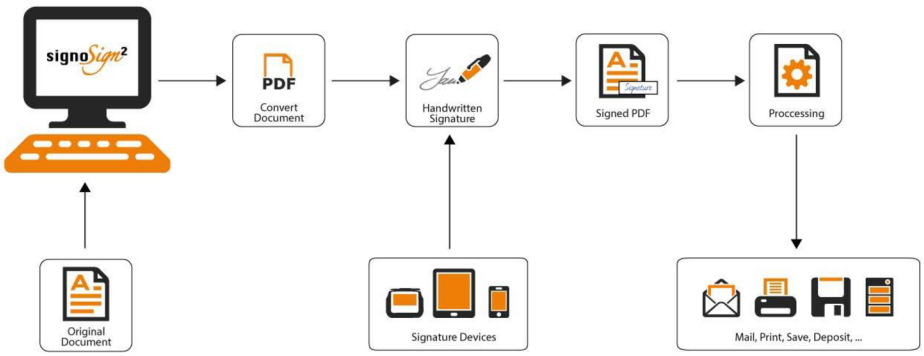
Kvalifikovaný certifikát vydávaný I. CA splňuje veškeré požadavky dané zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce a nařízením č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS). Kvalifikovaný certifikát je určeny pro komunikaci s orgány veřejné moci, současně jej lze využít také pro komerční účely. Ve ŠKODA AUTO a.s. se jedná zejména například o mzdovou, celní, lékařskou dokumentaci (Portál ŠKODA AUTO a.s., 2022).

5 Návrh změn vedoucích ke zvýšení pozitivních aspektů využívání el. podpisů

Elektronické podpisy se v digitálním věku staly stále oblíbenější metodou pro usnadnění bezpečných a pohodlných transakcí. Stejně jako u jakékoli technologie však existuje potenciál pro zlepšení, aby se maximalizovaly pozitivní aspekty elektronických podpisů a zároveň se minimalizovaly jakékoli negativní účinky. V této kapitole se popíše několik změn, které by mohly vést ke zvýšení výhod elektronických podpisů, včetně strategií pro zlepšení bezpečnosti a zefektivnění procesu podpisu. Implementace těchto změn může zajistit, že další používání elektronických podpisů zlepší schopnost uživatelů provádět transakce bezpečným a efektivním způsobem.

5.1 Aktuální řešení ve ŠKODA AUTO a.s.

V současné době ŠKODA AUTO a.s. hodně spoléhá na používání MFA karty pro řízení přístupů a oprávnění zaměstnanců a podepisování dokumentů. Toto řešení sice efektivně slouží potřebám pro interní zaměstnance, ale není vhodné pro externí uživatele, kteří chtějí podepisovat dokumenty, ale nemají přístup k MFA kartě. K řešení tohoto problému je ideální jako alternativní řešení použití biometrických elektronických podpisů prostřednictvím podpisových destiček. To by ve shrnutí zahrnovalo otevření podpisového softwaru na počítači nebo notebooku a vytvoření pole pro podpis v dokumentu, který má být podepsán. Uživatel pak může dokument podepsat pomocí specifického podpisového pera které je u podpisové destičky. Řešení biometrického elektronického podpisu umožňuje bezpečné a pohodlné podepisování dokumentů externími uživateli bez potřeby MFA karty.



Zdroj: (signotec, 2022)

Obr. 9 Ilustrace daného procesu přes podpisové zařízení od firmy signotec

Postup podepsání je tudíž stejný jak při běžném podpisu na papíře, akorát jedinou změnou je, že se daný uživatel podepisuje na podpisové destičce či jiném podpisovém zařízení.

5.2 Navrhované řešení použití biometrických elektronických podpisů ve ŠKODA AUTO a.s.

Řešení použití biometrických elektronických podpisů se dá ještě více zefektivnit a to právě s využitím podpisové destičky která bude vybavena ethernet připojením. Tato možnost ethernetového připojení je volitelná u podpisových destiček Signotec Delta. Toto připojení umožňuje integraci podložky do firemní sítě a její ovládání přes IP adresu. Například pro použití zařízení z několika pracovních stanic současně. Ale také použití na větší vzdálenost, může být realizováno tímto způsobem. Režim lze změnit z USB na Ethernet nebo naopak v servisním menu podložky.

Při využití možnosti ethernetového připojení u podpisových destiček lze omezit počáteční náklady na jednotlivé destičky. Využitím tohoto řešení se omezí počáteční náklady, nebude nutná potřeba kupovat jednu podpisovou destičku na každou pracovní stanici na které se bude pracovat s dokumenty, které bude daný uživatel chtít podedpsat, ale jednoduše si takhle sdílí podpisovou destičku s vícero uživateli, když bude potřeba. Změny v procesu podepsání na podpisové destičce oproti běžnému podepsání na papíře by byly následující:

Původní proces tisku papírového předávacího protokolu:

- Odeslání tisku na tiskárnu
- Tisk dokumentu
- Podání dokumentu zaměstnanci
- Výzva k prostudování a podpisu
- Založení papíru.

Nový proces s podpisovou destičkou:

- Odeslání tisku protokolu do PDF
- Vygenerování dokumentu a zobrazení na podpisové destičce
- Pokyny uživateli, prostudování a podpis na destičku.
- Uložení na sdílený disk.

5.2.1 Využití nového procesu – oddělení SO

Nový proces podpisu byl implementován na oddělení SO(Bezpečnost společnosti ŠKODA AUTO a.s.), kde nahradil běžný předešlý proces podpisu dokumentu na papíře. Zaměstnanci oddělení SO následně provedli časové vypočty s oběma podpisovými procesy. Pří výpočtech obou podpisových procesů bylo zjištěno, že v propočtu vyšla časová dotace u papírového formuláře na 4 minuty, jedná se o kompletní čas, kde je zahrnuto zajištění papíru, archivace, likvidace, tiskové služby atd..,. U nového procesu podpisu s podpisovou destičkou pak vyšla časová dotace na 2 minty (uložení dokumentu atd..). Při samotném měření se zjistilo, že proces podpisu na papíru trval 20 sekund zatímco proces podpisu na destičku trval 23 sekund. Největší časová úspora byla u nového podpisového procesu na podpisové destičce v následných krocích před podpisem a následně po něm. Zaměstnanci při novém procesu nemuseli zajišťovat papír nebo vyměňovat toner, tisknout, skenovat, archivovat. Například samotná archivace je automatizovaná v novém procesu, tudíž se v porovnání s původním procesem daný proces zkrátí a ušetří se tím zaměstnancům čas. Dále byla zjištěna úspora tisku při využití nového procesu. Od listopadu 2020 až do prosince 2021 v rozmezí 1 roku bylo ušetřeno následující počet papíru:

- Mladá Boleslav – 15 816
- Kvasiny - 1948
- Vrchlabí – 401

Celkem: 18 165 kusů papíru

Roční přínos úspor při využití nového procesu s podpisovou destičkou byl v hodnotě **16.887€**. Výpočty úspor provedla Lucie Ulipova(SVP expert – nepřímá oblast S) za oddělení S(Lidé a kultura).

5.2.2 IT Point – oddělení FIO

Oddělení FIO už v IT Pointu využívalo podpisové destičky od společnosti Wacom. Nicméně oddělení FIO v IT Pointu plánovalo využít nové pracovní zařízení (notebooky) vybavené operačním systémem macOS. Nicméně na macOS operačním systému podpisové destičky nefungují, tudíž se muselo najít jiné řešení. Řešení se nalezlo ve využití ethernetového připojení kterým podpisové destičky od společnosti signotec mohou být vybaveny.

Připojení přes ethernet by se využilo ke vzdálenému připojení na VDI (virtuální stroje) přes Citrix. Virtuální počítače se v ničem neliší od jiných fyzických počítačů, jako jsou notebooky nebo desktopy. Jedná se o plnohodnotné operační systémy provozované na serverech společnosti ŠKODA AUTO a.s., a ke kterým je možný vzdálený přístup odkudkoliv a kdykoliv. Jednou z hlavních výhod VDI je že díky sjednocené a standardizované instalaci operačního systému a softwarových nástrojů, dokáží virtuální počítače plně nahradit standardní fyzické počítače v síti ŠKODA AUTO a. s..

Propojení ethernetového připojení podpisové destičky s VDI umožní využívat podpisovou destičku odkudkoliv a z jakéhokoliv zařízení. Tudíž i ze zařízení ze kterého by například podpisový software nešel ani spustit.

Než se ale začne ethernetové připojení na podpisových destičce používat, musí v rámci ŠKODA AUTO a.s. projít několika interními formuláři a být odsouhlaseno.

Celý proces funguje následovně:

1. Převzetí podpisových destiček
2. Zjištění MAC a sériového čísla podpisových destiček
3. Poslání daného označení Videoteamu pro registraci daných podpisových destiček do SAPu (podnikový informační systém) a zažádání o vyjímku z bezpečnosti
4. Po úspěšném zaevidování v SAPu, registrace podpisových destiček v DNS přes elektronické a zadání MAC adresy
5. Zjištění informací ohledně konkrétních uživatelů, kteří je chtějí používat (uživatelské jméno)
6. Nastavení pravidel pro průchod firewallem pro podpisové destičky přes elektronické formuláře
7. Vyzkoušení funkčnosti u uživatelů

Po úspěšném nastavení veškerých náležitostí a přiřazení virtuálních zařízeních jednotlivým uživatelům se musí na VDI zařízeních nainstalovat podpisový software signoSign2 z centra pro software kde se nachází všechen který lze nainstalovat pro interní používání na interních zařízení. signoSign2 se objeví všem uživatelům v centru pro software ke kterým byla přiřazena zakoupená licence. Dále se na VDI zařízeních musí nainstalovat Check Point Identity Agent, který pak běží v pozadí a pomocí kterého se rozpozná konkrétní uživatel pro kterého byla vystavena vyjímka průchodu firewallem v síti pro připojení se na podpisovou destičku. V signoSign2 by

pak již měla být aktivovaná licence, pokud ne tak se zadá manuálně dle obdrženého klíče. Následně se v signoSign2 dle preference uživatele dá nastavit automatizace konkrétních procesů jako je například předem nastavení daného místa uložení po úspěšném podpisu, či předem definování podpisového pole v určitých typech dokumentů na určitém místě. Kokrétně byly objednány 4 podpisové destičky. Vzhledem k novější verzi podpisové destičky oproti té používané oddělením SO, jsou počáteční náklady o trochu vyšší a celkově se dá předpokládat i nižší efektivita úspor vzhledem k nižší návštěvnosti v porovnání s oddělením SO, vzhledem k daným lokací kde budou podpisové destičky signotec Delta využity. Ethernet připojení jednotlivých podpisových destiček se využije zejména na vzdálené připojení na jednotlivé pracovní stanice a neplánuje se jejích sdílení.

Předmět	Cena 1 ks ŠKODA AUTO	Množství	Cena celkem
Signotec Delta Pad Ethernet/USB	12 263,00 Kč	4	49 052,00 Kč
Recyklační příspěvek	4,00 Kč	4	16,00 Kč
Dopravné, balné, pojištění 4 ks	155,00 Kč	1	155,00 Kč
Cena celkem			**49 223,00 Kč**

Zdroj: (signotec, 2022)

Obr. 10 Cenová nabídka signpadů pro oddělení FIO

Aplikace je dodávána spolu s virtuální PDF tiskárnou, díky které je možné v aplikaci otevřít dokument z libovolné aplikace, která umožňuje tiskový výstup. V signoSign/2 podporuje definici dokumentových tříd a k nim odpovídající chování jako je např. automatické generování podpisových polí, nebo automatizované ukládání na předem definované úložiště.

Předmět	Cena 1 ks	Cena ŠKODA AUTO a.s. 1 ks	Množství	Cena celkem
signoSign2 SW	3 547,00 Kč	2 164,00 Kč	4	8 656,00 Kč
SW maintenance 1 rok	709,-00 Kč	433,00 Kč	4	1732,00 Kč
Cena celkem	**4 256,00 Kč**	**2 597,00 Kč**		**10 388,00 Kč**

Zdroj: (signotec, 2022)

Obr. 11 Cenová nabídka softwaru (licence) pro oddělení FIO

SW licence jsou podporovány po dobu využívání aplikace prostřednictvím tzv. SW maintenance. SW maintenance zahrnuje vydání nových verzí softwaru. Roční maintenance je splatná vždy předem na následující rok.

5.2.3 Oddělení SB

Dalším místo kde se dá zlepšit proces podepisování je oddělení SB(operativní HR péče, digitalizace, HR). Oddělení SB se zabývá především otázkami týkajících se oblasti lidských zdrojů. Zde se konkrétně projevil zájem o 14 podpisových destiček kde se primárně bude cílit na využití ethernetového připojení podpisových destiček a sdílení destiček mezi vícero uživateli a tím snížení nákladů na pořízení.

Předmět	Cena 1 ks ŠKODA AUTO	Množství	Cena celkem
Signotec Delta Pad Ethernet/USB	11 845,00 Kč	14	165 830,00 Kč
Recyklační příspěvek	4,00 Kč	14	56,00 Kč
Síťový adaptér ST-SPARE -DEL-019	379,00	14	5 306,00 Kč
Dopravné, balné, pojištění 4 ks	155,00 Kč	1	500,00 Kč
Cena celkem			**171 692,00 Kč**

Zdroj: (signotec, 2022)

Obr. 12 Cenová nabídka signpadů pro oddělení SB

Předmět	Cena 1 ks	Cena ŠKODA AUTO a.s. 1 ks	Množství	Cena celkem
signoSign2 SW	3 547,00 Kč	2 164,00 Kč	54	116 856,00 Kč
SW maintenance 1 rok	709,-00 Kč	433,00 Kč	54	23 382,00 Kč
Cena celkem	**4 256,00 Kč**	**2 597,00 Kč**		**140 238,00 Kč**

Zdroj: (signotec, 2022)

Obr. 13 Cenová nabídka softwaru (licence) pro oddělení SB

Objednávalo se 54 licencí. Na každou podpisovou destičku vychází v průměru 4(54/14=3,86) uživatelé. Při výpočtu se pořizovací náklady se sníží na čtvrtinu (11 845 / 4 = 2961,- Kč). Nicméně když se připočtou náklady za 1 licenci na uživatele. Tak celkové pořizovací náklady na 1 uživatele budou: **7217,- Kč.**

V porovnání s využitím řešení bez ethernetu by celkové pořizovací náklady na 1 uživatele byly: 11 845 + 3547 + 709 = **16 101,- Kč**. Rozdíl je v ceně dvojnásobný. Je výhodné zvolení podpisové destičky která je vybavena ethernetovým připojením oproti podpisové destičce která jim není. I když časová náročnost implementace ethernetového připojení bude náročnější oproti běžnému USB připojení, tak z hlediska počátečních úspor je tato volba vhodnější.

5.3 signoSign2

Použití programu signoSign2 umožňuje automatizaci procesu podepisování dokumentů na podpisové destičky. Prostřednictvím programu je možné přednastavit nastavení podpisového pole tak, aby se nemuselo ručně zadávat při každém podepisování dokumentu. Toto řešení by bylo užitečné zejména v administrativě, konkrétně v oddělení lidských zdrojů, kde by mohlo vést ke snížení nákladů na spotřebu a vytížení jednotlivých skenerů a tiskáren. Implementaci tohoto řešení však brání překážky jako jsou počáteční investice do podpisových destiček a školení zaměstnanců v jejich používání. Navzdory těmto výzvám se dlouhodobé výhody tohoto řešení vyplatí.

Zdroj: (signotec, 2022)

Obr. 14 signotec Delta bez držáku pera (boční pohled)

5.4 Shrnutí budoucnosti elektronického podpisu

Budoucnost elektronických podpisů bude pravděpodobně zahrnovat pokračující růst a inovace v této oblasti. Vzhledem k tomu, že technologie postupuje vpřed a stále více podniků a jednotlivců začíná používat elektronické podpisy, poptávka po nových a vylepšených řešeních elektronického podpisu pravděpodobně poroste.

Jednou z potenciálních oblastí růstu elektronických podpisů je používání biometrických technologií. Biometrické podpisy, které využívají jedinečné fyzické nebo behaviorální charakteristiky k identifikaci jednotlivce, mají potenciál poskytnout bezpečnější a spolehlivější formu elektronického podpisu. Systém biometrického podpisu může například používat otisk prstu nebo rozpoznávání obličeje k ověření identity podepisujícího.

Další potenciální oblastí růstu elektronických podpisů je využití technologie blockchain. Blockchain je distribuovaná decentralizovaná databáze, která umožňuje

bezpečné a transparentní zaznamenávání transakcí. Použitím blockchainu k ukládání a ověřování elektronických podpisů může být možné vytvořit záznam o podepsaných dokumentech, který je zabezpečený proti neoprávněné manipulaci a je auditovatelný.

Jednou z dalších potenciálních oblastí budoucího vývoje elektronických podpisů je využití umělé inteligence (AI) a strojového učení. Začleněním těchto technologií do systémů elektronického podpisu může být možné automatizovat proces ověřování podpisu a zlepšit jeho přesnost a rychlost. Systém elektronického podpisu s umělou inteligencí by například mohl být schopen se časem naučit podpis jednotlivce a použít tyto informace k přesnějšímu ověření budoucích podpisů.

Další potenciální oblastí rozvoje elektronických podpisů je využití technologií virtuální reality (VR) a rozšířené reality (AR). Pomocí VR a AR může být možné vytvořit působivější a intuitivnější zážitek z elektronického podpisu. Například systém elektronického podpisu poháněný AR může uživateli umožnit podepsat dokument pouhým napsáním svého podpisu ve vzduchu prstem.

Další potenciální oblastí rozvoje elektronických podpisů je využití technologie inteligentních smluv. Inteligentní smlouvy jsou samovykonatelné smlouvy, přičemž podmínky dohody mezi kupujícím a prodávajícím jsou přímo zapsány do řádků kódu. Použitím chytrých smluv ve spojení s elektronickými podpisy může být možné automatizovat uzavírání smluv a zefektivnit proces podepisování a ověřování dohod.

Celkově lze říci, že budoucnost elektronických podpisů bude pravděpodobně zahrnovat pokračující inovace a přijímání nových technologií pro zlepšení bezpečnosti, spolehlivosti a pohodlí. Vzhledem k tomu, že se elektronické podpisy stále více používají a přijímají, můžeme očekávat průběžný vývoj v této oblasti. (Research and Markets, 2022)

Závěr

Digitální podpisy poskytují organizacím konkurenční výhodu prostřednictvím vyšší efektivity, zkrácení doby rozhodování, odstranění papírování, lepší transparentnosti a lepšího zabezpečení. Tato vylepšení vedou k výraznému snížení nákladů.

Stojí za zmínku, že používání digitálních podpisů není omezeno na určité typy podniků nebo pouze na produkty a služby související s technologiemi. Digitální podpisy lze použít na jakýkoli aspekt operací organizace, včetně marketingu, prodeje, nákupu, logistiky, výroby, designu a inženýrství. Organizace mohou používat digitální podpisy pro různé funkce, jako je zabezpečený prodejní kanál, zabezpečená komunikace s partnery a klienty a bezpečné provádění dalších transakcí elektronického obchodování. Digitální podpisy nabízejí potenciál pro mnoho vylepšení v rámci obchodních procesů.

Organizace by měly přejít od tradičních, časově náročných procesů papírového podpisu k novým a inovativnějším technologiím, aby zvýšily efektivitu. Digitální podpisy mohou významně prospět organizacím, protože eliminují poslední kus papíru v obchodním cyklu a poskytují zvýšené pohodlí jak pro zákazníka, tak pro organizaci.

Přechod od papírových k plně elektronickým obchodním procesům a od fyzického oddělení k digitální integraci přináší organizacím významné úspory nákladů, výhody produktivity a konkurenční výhodu na trhu. Otázkou tedy není, zda používat digitální podpisy, ale spíše jak je efektivně implementovat.

Seznam literatury

MASON, S. -- SENG, D. Electronic Evidence and Electronic Signatures. United Kingdom: University of London Press, Institute of Advanced Legal Studies, 2021. 422 s. ISBN 978-1-911507-24-6.

PETERKA, J. Báječný svět elektronického podpisu. Praha: CZ.NIC, 2011. 438 s. ISBN 978-80-904248-3-8.

VANSTONE, S. -- MENEZES, A. -- OORSCHOT, P. Handbook of Applied Cryptography. 6000 Broken Sound Parkway NW, Suite 300: CRC Press, 1996. 816 s. ISBN 0-8493-8523-7.

BUDIŠ, Petr; ŠTĚDROŇ, Bohumír. Elektronické komunikace. 1. vyd. Slovakia: Magnet Press, 2008. 110 s. ISBN 978-80-89169-11-5.

RYBKA, Michal; MALÝ, Ondřej. Jak komunikovat elektronicky. 1. vyd. Praha: Grada, 2002. 92 s. ISBN 80-247-0208-8.

ADAMS, C. LLOYD, S. Understanding PKI: Concepts, Standards, and Deployment Considerations. Second Edition, Addison-Wesley Professional, 2003, ISBN 978-0-672-32391-1, s. 11-12

ŠTĚDROŇ, Bohumír. Úvod do eGovernmentu: právní a technický průvodce. Praha: Úřad vlády české republiky, 2007, ISBN 978-80-87041-25-3

ŠKODA AUTO a.s. interní zdroj, 2022

Webové stránky

Co byste měli vědět o rostoucím trhu s elektronickými podpisy [online]. Forbes, 2021 [cit. 2022-12-02].
URL: https://www.forbes.com/sites/forbestechcouncil/2021/07/28/what-to-know-about-the-growing-electronic-signature-market/?sh=2d2ce5723b90

Elektronický podpis. *První certifikační autorita, a.s. (I.CA)* [online]. [cit. 2022-12-03].
URL: https://www.ica.cz/elektronicky-podpis

I.CA. O společnosti I.CA. [online]. [cit. 2022- 11-28].
URL: https://www.ica.cz/o-nas

SMEJKAL, V. Kryptografický a dynamický biometrický podpis podle platné právní úpravy. [online]. 2019. [cit. 2022-11-26]
URL: https://www.researchgate.net/publication/334279726_Kryptograficky_a_dynamicky_biometricky_podpis_podle_platne_pravni_upravy

What is eSignature. Evropská komise [online]. [cit. 2022-11-26].
URL: https://ec.europa.eu/digitalbuildingblocks/wikis/display/DIGITAL/What+is+eSignature

Algoritmus RSA. [online]. [cit. 2022-11-26].
URL: https://www.algoritmy.net/article/4033/RSA

PETERKA, J. Kvalifikovaný certifikát pro elektronický podpis.[online]. [cit. 2022-11-26].
URL: https://www.ica.cz/kvalifikovany-certifikat-pro-ePodpis

Portál ŠKODA AUTO a.s. [online]. [cit. 2022-11-26].
URL: https://eportal.skoda-auto.cz/skodaspace/group/b2eportal/home-page

Research and Markets [online]. [cit. 2022-11-27].
URL: https://www.globenewswire.com/en/news-release/2022/08/19/2501529/28124/en/Digital-Signature-Global-Market-Report-2022-Implementation-of-Blockchain-Technology-a-Key-Facet-for-Future-Growth.html

Seznam obrázků a tabulek

Seznam obrázků

Obr. 1 Příklad (uznávané) elektronické značky na datové zprávě v ISDS 12
Obr. 2 Příklad (kvalifikovaného) časového razítka na datové zprávě v ISDS 13
Obr. 3 Klasifikace podpisů, značek a razítek 14
Obr. 4 Představa hašování (s hašovací funkcí SHA-1) 18
Obr. 5 Představa využití soukromého a veřejného klíče 20
Obr. 6 Představa certifikátu 21
Obr. 7 Podepisování elektronického dokumentu v rámci ŠKODA AUTO a.s. 27
Obr. 8 Fungování DigiPodpisu ve firmě ŠKODA AUTO a.s. 28
Obr. 9 Ilustrace daného procesu přes podpisové zařízení od firmy signotec 30
Obr. 10 Cenová nabídka signpadů pro oddělení FIO 34
Obr. 11 Cenová nabídka softwaru (licence) pro oddělení FIO 34
Obr. 12 Cenová nabídka signpadů pro oddělení SB 35
Obr. 13 Cenová nabídka softwaru (licence) pro oddělení SB 35
Obr. 14 signotec Delta bez držáku pera (boční pohled) 36

ANOTAČNÍ ZÁZNAM

AUTOR	**Lukáš Horák**		
STUDIJNÍ PROGRAM/OBOR/SPECIALIZACE	**Podniková ekonomika a manažerská informatika**		
NÁZEV PRÁCE	**Využití elektronických podpisů jako nástroje efektivní digitalizace ve ŠKODA AUTO a.s.**		
VEDOUCÍ PRÁCE	**Ing. Lukáš Herout, Ph.D.**		
KATEDRA	**KI - Katedra informatiky**	**ROK ODEVZDÁNÍ**	**2022**

POČET STRAN	**43**
POČET OBRÁZKŮ	**14**
POČET TABULEK	**1**
POČET PŘÍLOH	**0**

STRUČNÝ POPIS	**Závěrečná práce se věnuje oblasti elektronického podpisu, popisuje se v ní detailně jak vlastně funguje a jak se dělí. Je zde popsaný využití elektronického podpisu ve ŠKODA AUTO a.s., budoucnost elektronického podpisu a jsou zde zmíněný i jeho kladné i záporné stránky. Cílem bakalářské práce je analyzovat možnosti a přístupy k využívání elektronických podpisů jako součásti digitalizace vnitropodnikových procesů. Na konkrétním případě v rámci vybraného oddělení/části ŠKODA AUTO a.s. zmapovat pozitivní a negativní aspekty využití el. podpisů a navrhnout případné změny vedoucí ke zvýšení očekávaných benefitů.**
KLÍČOVÁ SLOVA	**Digitalizace, elektronický podpis, digitální podpis**

ANNOTATION

AUTHOR	**Lukáš Horák**		
FIELD	**Business Informatics**		
THESIS TITLE	**Využití elektronických podpisů jako nástroje efektivní digitalizace ve ŠKODA AUTO a.s.**		
SUPERVISOR	**Ing. Lukáš Herout, Ph.D.**		
DEPARTMENT	**KI - Department of Informatics**	**YEAR**	**2022**

NUMBER OF PAGES	**43**
NUMBER OF PICTURES	**10**
NUMBER OF TABLES	**1**
NUMBER OF APPENDICES	**0**

SUMMARY	**The bachelor thesis is devoted to the field of electronic signature, it describes in detail how it actually works and how it is divided. The use of electronic signatures in ŠKODA AUTO a.s., the future of electronic signatures and its positive and negative aspects are also described here. The aim of the bachelor's thesis is to analyze the possibilities and approaches to the use of electronic signatures as part of the digitization of internal company processes. In a specific case within the selected department/part of ŠKODA AUTO a.s. to map the positive and negative aspects of the use of electricity signatures and propose any changes leading to an increase in the expected benefits.**
KEY WORDS	**Digitization, electronic signature, digital signature**