UNICORN VYSOKÁ ŠKOLA S.R.O.

BAKALÁŘSKÁ PRÁCE

2025 Milan Lysák

UNICORN VYSOKÁ ŠKOLA S.R.O.

Softwarový vývoj

BAKALÁŘSKÁ PRÁCE

Změny v elektronické identifikaci a autentizaci eIDAS, dopady zavedení Evropské digitální identity v podnikových systémech a dopady legislativy na vývoj těchto systémů v ČR

Autor BP: Milan Lysák
Vedoucí BP: Mgr. František Korbel, Ph.D.

Čestné prohlášení

Prohlašuji, že jsem svou závěrečnou práci na téma Změny v elektronické identifikaci a autentizaci eIDAS, dopady zavedení Evropské digitální identity v podnikových systémech a dopady legislativy na vývoj těchto systémů v ČR vypracoval samostatně pod vedením vedoucího závěrečné práce a s použitím výhradně odborné literatury a dalších informačních zdrojů, které jsou v práci všechny citovány a jsou také uvedeny v seznamu použitých zdrojů. Prohlašuji, že nástroje umělé inteligence byly využity pouze pro podpůrné činnosti a v souladu s principem akademické etiky.

Jako autor této závěrečné práce dále prohlašuji, že v souvislosti s jejím vytvořením jsem neporušil autorská práva třetích osob a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.

Dále prohlašuji, že odevzdaná tištěná verze závěrečné práce je shodná s verzí, která byla odevzdána elektronicky.

V Praze, dne 10. 07. 2025. ……

Milan Lysák

Poděkování

Děkuji vedoucímu závěrečné práce Mgr. Františku Korbelovi, Ph.D. za trpělivost, metodickou, pedagogickou a odbornou pomoc a cenné rady při zpracování této práce.

Změny v elektronické identifikaci a autentizaci eIDAS, dopady zavedení Evropské digitální identity v podnikových systémech a dopady legislativy na vývoj těchto systémů v ČR

UNICORN
UNIVERSITY

Abstrakt

Tato práce se zabývá změnami, které přináší implementace nařízení eIDAS a nově i její aktualizace eIDAS 2 do české legislativy a jejími dopady v podnikových systémech.

V první části bude vysvětlen vznik nařízení, jeho legislativní rámec a budou vysvětleny základní používané pojmy.

Ve druhé části bude popsáno několik praktických aplikací, které využívají služby vytvářející důvěru dle nařízení eIDAS a na jejichž vývoji jsem se podílel nebo jsem tyto služby využíval.

Ve třetí části budou shrnuty dosavadní zkušenosti z hlediska přínosů a rizik implementace služeb vytvářejících důvěru dle nařízení eIDAS v podnikových systémech a nastíněny možnosti využití novinek přicházejících s novelizací eIDAS 2.

Cílem práce je na základě platné legislativy a dostupných znalostí identifikovat dopady vznikajících služeb vytvářejících důvěru eIDAS na podnikové systémy.

Klíčová slova: eIDAS, digitální identita, Peněženka digitální identity EU, elektronické potvrzování atributů, eGovernment, kyberbezpečnost.

Abstract

This thesis deals with the changes brought about by the implementation of the eIDAS regulation and its new update eIDAS 2 to Czech legislation and its impacts on corporate systems.

The first part will describe the origin of the regulation, its legislative framework and explain the basic terms used.

The second part will describe several practical applications that use trust services according to the eIDAS regulation and in whose development I participated or used these services.

The third part will summarize the experience to date in terms of the benefits and risks of implementing trust services according to the eIDAS regulation in corporate systems and outline the possibilities of using the innovations coming with the amendment of eIDAS 2.

The aim of the thesis is to identify the impacts of emerging eIDAS trust services on corporate systems based on the current legislation and available knowledge.

Keywords: eIDAS, digital identity, EU Digital Identity Wallet, electronic attestations of attributes, eGovernment, cybersecurity.

Obsah

Úvod

Každé období lidské historie je charakterizováno určitými znaky nebo lépe řečeno vynálezy a inovacemi, které vedly k viditelným změnám ve struktuře společnosti, životního stylu a ke změnám ve vymáhání moci a práva. Tyto znaky nebo inovace nemusí být nutně na první pohled viditelné a zřejmé pro současníky, ale jsou zcela jasně rozeznatelné zpětně následujícími generacemi. Ve škole se učíme, co to byla doba bronzová nebo proč se 19. století říká století páry. Může se nám to nelíbit, můžeme s tím nesouhlasit, ale všechny důležité vynálezy měly přímý nebo nepřímý dopad i na vymáhání práva a moci. V době feudální byl hlavním dopravním prostředkem kůň a moc panovníka se (zjednodušeně řečeno) omezovala na území, které byl schopen obsáhnout osobní přítomností nebo dosahem vojenských posádek. Stejně rychle putovaly i informace o událostech, které byly pro panovníka relevantní.

Byla to doba, kdy dané slovo (ústní) mělo svou platnost a bralo se jako závazné. Ještě vyšší platnost mělo psané slovo, jehož průkaznost byla zajištěna tím, že málo lidí dokázalo číst, ještě méně psát a zároveň nejdůležitější listiny byly spravovány důvěryhodnými institucemi - například Zemské desky spravovaly soudy a zemští písaři/notáři. Bylo velmi obtížné takovéto písemnosti změnit či dodatečně upravovat, a proto můžeme hovořit o dostatečné průkaznosti a důvěryhodnosti těchto listin.

Každá doba potřebuje mít pro fungování veřejné správy nebo smluvních vztahů (zejména vymáhání vlastnických práv, smluvních závazků nebo trestních záležitostí) k dispozici takové nástroje, které jsou pro současníky dostatečně důvěryhodné a zajistí uchování relevantních informací.

Důvěryhodnost dokumentu v sobě zahrnuje tři základní roviny: důvěryhodnost vlastního dokumentu, důvěryhodnost zúčastněných stran a třetí rovina je transportní, neboli přenositelnost dokumentu.

Zatímco dříve se lidé spoléhali na to, že listinu posel nepozměnil, protože to prostě neuměl nebo neměl čas ji nechat nějakému písaři přepsat (padělání se vždy tvrdě trestalo, což ale dokazuje, že se tak i někdy dělo), tak v dnešní době se musíme spoléhat na nové nástroje, které vykazují stejné znaky - pozměnění dokumentu musí být velmi obtížně nebo ideálně nemožné.

Během 20. století díky novým vynálezům, jako např. fotografie či daktyloskopie, byly takovými dokumenty rodný list, občanský průkaz, cestovní pas nebo úřední záznamy opatřené razítkem a podpisy.

V dnešní době, kdy pokročila digitalizace veškerých dokumentů a díky rychlému internetu máme veškeré informace téměř na dosah ruky, tak zároveň vyvstává potřeba mít záchytné body, na které se můžeme spolehnout, že zde nalezneme ověřené a ověřitelné zdroje informací.

Podnikové intranety byly schopny si udržet vysokou míru spolehlivosti díky uzavřenému ekosystému, nicméně s větším rozvojem internetových služeb nebo zavedením homeoffice se tyto vnitřní podnikové systémy začaly otevírat, což přineslo nemalé bezpečnostní nástrahy a úskalí.

Zde bych podotknul zajímavou věc, že zatímco dosud byl nositelem pokroku v oblasti digitalizace a internetových služeb především průmysl, obchod a mladá generace nadšenců, nyní důležité změny a standardy zavádí úřady a vlády, které byly zatím spíše považovány (a stále jsou považovány) spíše za brzdy pokroku a udržovatele tradičních postupů.

Nicméně, přestože je eIDAS na první pohled doménou státní správy a jejího vztahu k občanům a firmám, přináší platformu a nástroje, která se postupně propisují i do vnitřního fungování firem.

První část této bakalářské práce se bude věnovat legislativnímu rámci eIDAS, výkladu některých termínů, autoritám a poskytovatelům služeb vytvářejících důvěru.

Druhá část práce se bude věnovat několika praktickým aplikacím využívaných v podnikových systémech se zaměřením na elektronickou identifikaci. Jedním z prezentovaných příkladů je projekt, na kterém jsem se podílel jako vývojář a měl tak možnost získat cenné zkušenosti, které jsem využil nejen pro tuto bakalářkou práci.

Třetí část práce se bude věnovat zhodnocení přínosů zavádění eIDAS pro podnikové systémy a poukáže na možná rizika s tím spojená.

1 Teoretická část

V teoretické části práce se budu věnovat nejprve myšlence vzniku a zavedení eIDAS jako celku, vysvětlením základních pojmů spojených s oblastmi, kterých se eIDAS dotýká, což jsou například občané, státní instituce nebo hospodářské subjekty. Dále se budu zabývat novelizací eIDAS, tzv. "eIDAS 2" a novým službám, které přináší.

1.1 Základní pojmy

1.1.1 eIDAS

eIDAS je NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č.910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES [1]. Cílem tohoto nařízení bylo, mimo jiné, zřízení jednotného digitálního trhu v rámci členských států EU., zjednodušení přeshraniční elektronické komunikace nebo vytvořit právní jistoty pro používání elektronických podpisů a elektronické identifikace.

1.1.2 Elektronická identita

Elektronická identita je elektronický ekvivalent "standardní" identity jedinečné osoby v reálném světě. Slovo standardní je potřeba brát s velkou rezervou, protože k termínu identity je možno přistupovat různými způsoby. Například v humanistické psychologii je identita chápána jako schopnost "být tím, čím člověk opravdu je, tedy sám sebou" [2]. Nicméně ve vztahu k eIDAS a pro potřeby identifikace a autentizace v elektronických systémech se postupně prosazuje koncept identity jako souboru atributů, které popisují jednoznačně konkrétní osobu (viz. kapitola 1.3.1 Evropská digitální identita).

Pro eGovernment je pojem e-identita vnímán jako "druh uživatelského účtu, který je svázaný s jednoznačně identifikovanou osobou, která prostřednictvím tohoto účtu může dále komunikovat zejména se státní správou. Prostřednictvím e-identity je možné mít dálkový přístup k údajům konkrétního uživatele/občana" [3].

Nutno dodat, že identita se vyvíjí a může se měnit. Proto je i u elektronické identity umožněna změna atributů na základě změny atributů identity občana.

1.1.3 Elektronická identifikace

Elektronickou identifikací se dle eIDAS rozumí "postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu" [1]. K tomu, aby mohla proběhnout elektronická identifikace jsou potřeba identifikační prostředky, systém elektronické identifikace, do kterého se subjekt přihlašuje a s tím spojená autentizace. Identifikační prostředky jsou nástroje, které má občan k dispozici (občanský průkaz, mobilní klíč eGovernmentu, apod.), který použije pro proces autentizace. Procesem autentizace se rozumí určitá činnost za použití identifikačních prostředků (přihlášení do webové služby, potvrzení v mobilní aplikaci apod.), jejímž výsledkem je potvrzení

identity a to v jedné ze tří základních úrovní záruky: nízká, značná a vysoká.

1.1.4 Záruky

Záruka představuje úroveň zabezpečení systému elektronické identifikace. Její výše zabezpečení je dána použitými identifikačními prostředky a způsobem autentizace. Pro každou službu vytvářející důvěru se vyžaduje minimální úroveň záruky, aby se uživatel mohl přihlásit a službu použít.

- Nízká úroveň - v této úrovni nedošlo k zaručenému ověření identity, často jde pouze o zvolení přihlašovacího jména a hesla.
- Značná úroveň - v této úrovni je již potřeba použít dvoufaktorovou autentizaci, tedy použití dvou nezávislých prostředků pro ověření identity. Například jméno+heslo a k tomu zaslání SMS. U této úrovně je již potřeba, aby identita byla ověřena před vydáním identifikačních prostředků. Například předložením osobních dokladů v bance, kontaktním místě Czech POINT či na jiném kontaktním místě a to prostředkem stejné nebo vyšší úrovně důvěry.
- Vysoká úroveň - v této úrovni je již vyžadován HW prostředek s bezpečně uloženými údaji, jako je například občanský průkaz s aktivovaným čipem nebo čipová karta. Platí zde, stejně jako pro úroveň Značná, že byla identita osoby zaručeně ověřena před vydáním elektronických identifikačních prostředků.

Tabulka 1: Úroveň záruky

úroveň záruky	příklad z praxe	požadavky	cíl (.... riziko zneužití nebo změny totožnosti)
Vysoká (High)	nová eOP 	nutný HW (čipová karta/token)	předejít ....
Značná (Substantial)	„jméno, heslo, SMS“, bankovní identita, ...	nutná 2-faktorová autentizace	značně snížit ....
Nízká (Low)	přihlašování k ISDS	stačí 1-faktorová autentizace	snížit ....
..... (nulová)	jméno a heslo	stačí 1- faktorová autentizace	.....

Zdroj: https://www.earchiv.cz/papers/p85/gifs/p85.pdf

1.1.5 Identifikační prostředky

Podobně, jako v reálném světě se pro identifikaci osoby používají předem určené identifikační prostředky různého stupně záruky (například občanský průkaz, průkazka městské hromadné dopravy či průkazka do knihovny), tak se obdobným způsobem vydávají a používají elektronické identifikační prostředky různého stupně záruky. Pro přístup do emailu nebo na webové stránky často stačí znát pouze přihlašovací jméno a heslo, naopak pro komunikaci s úřady jsou vyžadovány mnohem vyšší nároky na zabezpečení.

Identifikační prostředky ve vztahu k eIDAS a pro přístup ke službám vytvářejících důvěru

(jako je eGovernment) se považují takové, které byly vydány v souladu se zákonem č.250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů, jsou v současné době vydávány státem i soukromoprávními kvalifikovanými poskytovateli. Takové identifikační prostředky posuzuje pověřená osoba, což je nyní Digitální a informační agentura. Ta také udržuje seznam identifikačních prostředků.

Tabulka 2: Aktuální seznam identifikačních prostředků

Kvalifikovaný správce			**Elektronický identifikační prostředek**	
Název	IČO	Adresa sídla	Prostředek	Úroveň záruky prostředku
Digitální a informační agentura	17651921	Na Vápence 915/14, 130 00 Praha	Mobilní klíč eGovernmentu	značná
			NIA ID	značná
Ministerstvo vnitra České republiky	00007064	Nad štolou 936/3, 170 00 Praha 7	Občanský průkaz s čipem (eObčanka)	vysoká
První certifikační autorita a.s.	26439395	Podvinný mlýn 2178/6, 190 00 Praha 9	Čipová karta STARCOS 3.5 ID ECC C1R s příslušným komerčním certifikátem pro systém elektronické identifikace.	vysoká
CZ.NIC, z.s.p.o.	67985726	Milešovská 1136/5, 130 00 Praha 3	MojeID – úroveň „značná“ (standardní přístup)	značná
			MojeID – úroveň „vysoká“	vysoká
Československá obchodní banka, a. s.	00001350	Radlická 333/150, 150 57 Praha 5	ČSOB Identita (jméno a heslo)	nízká
			ČSOB Identita (jméno, heslo a ověřovací kód)	značná
Česká spořitelna, a. s.	45244782	Olbrachtova 1929/62, 140 00 Praha 4	Bankovní IDentita	značná
Komerční banka, a. s.	45317054	Na Příkopě 969/33, 114 07 Praha 1	Bankovní identita KB	značná
Air Bank, a. s.	29045371	Evropská 2960/17, 160 00 Praha 6	Bankovní Identita	značná
MONETA Money Bank, a. s.	25672720	Vyskočilova 1442/1b, 140 28 Praha 4	Bankovní Identita	značná
Raiffeisenbank, a.s.	49240901	Hvězdova 1716/2b, 140 78 Praha 4	Bankovní Identita	značná
Fio banka, a.s.	61858374	V Celnici 1028/10, 117	Fio bankovní identita	značná

Kvalifikovaný správce			Elektronický identifikační prostředek	
		21, Praha 1		
UniCredit Bank Czech Republic and Slovakia, a.s.	64948242	Želetavská 1525/1, Michle, 14000 Praha 4	Bankovní identita	značná
Banka CREDITAS a.s.	63492555	Sokolovská 675/9, 186 00, Praha 8	Bankovní identita	značná
mBank, S.A.,Prosta 18 00-850 Varšava, Polská republika, zapsaná ve vnitrostátním soudním rejstříku, sč. zápisu 0000025237, a identifikačním číslem – REGON 001254524, vykonávající činnost na území České republiky prostřednictvím odštěpného závodu	27943445	Pernerova 691/42, 186 00, Praha 8	Bankovní identita	značná
Partners Banka, a. s.	9727094	Türkova 2319/5b, 149 00 Praha 4	Bankovní identita	značná

Zdroj: https://info.identita.gov.cz/KvalifikovaniSpravci.aspx

1.1.6 Kvalifikovaný systém elektronické identifikace

Kvalifikovaný systém elektronické identifikace je konkrétní systém provozovaný jedním z kvalifikovaných správců. Takový systém zajišťuje elektronickou identifikaci a tedy umožňuje přístup k elektronickým službám vytvářejících důvěru, například k službám eGovernmentu. Systém elektronické identifikace musí splňovat kritéria dle par. 3 zákona č. 250/2017 Sb., o elektronické identifikaci [4] a být schválen pověřenou osobou. Aktuálně je touto pověřenou osobou Digitální a informační agentura, která udržuje seznam těchto systémů.

Členský stát oznamuje Evropské komisi takový systém a po posouzení a schválení je zařazen do seznamu systémů elektronické identifikace oznámené podle čl. 9 odst.1 nařízení Evropského parlamentu a Rady (EU) a je uznávám ostatními členskými státy EU.
Seznam je dostupný na adrese: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

1.1.7 Kvalifikovaný správce systému elektronické identifikace

Kvalifikovaným správcem může být pouze státní orgán nebo osoba, které byla udělena akreditace pro správu kvalifikovaného systému. Do roku 2023 udělovalo akreditace pro kvalifikované správce Ministerstvo vnitra ČR a od roku 2023 je tímto, dle zákona 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, pověřena Digitální a informační agentura.

Kvalifikovaný správce spravuje systém elektronické identifikace, zajišťuje jeho provoz a bezpečnost v souladu s platnou legislativou. Vydává a spravuje identifikační prostředky, které umožňují osobám přístup do jím spravovaného systému. Podléhá dohledu pověřené osoby, kterou

je nyní Digitální a informační agentura. Mezi hlavní povinnosti kvalifikovaného správce systému elektronické identifikace patří, dle par.16 zákona č.250/2017 Sb. [4]:

- zajištění dostupnosti jím spravovaného kvalifikovaného systému pro spoléhající se stranu způsobem umožňujícím dálkový přístup prostřednictvím národního bodu a pro národní bod způsobem umožňujícím dálkový přístup,
- vedení evidence jím vydaných prostředků pro elektronickou identifikaci,
- před prvním použitím prostředku pro elektronickou identifikaci v rámci kvalifikovaného systému ověří totožnost držitele prostřednictvím národního bodu,
- zapsání identifikátoru jím vydaného prostředku pro elektronickou identifikaci a úroveň záruky tohoto prostředku do národního bodu,
- aktualizování údajů v evidenci vydaných prostředků pro elektronickou identifikaci na základě upozornění správce národního bodu na změny údajů,
- po ukončení své činnosti předání evidence vydaných prostředků pro elektronickou identifikaci ministerstvu,
- bez zbytečného odkladu zneplatnění prostředku pro elektronickou identifikaci držitele, o kterém se prokazatelně dozvěděl, že zemřel, nebo byl prohlášen za mrtvého,
- bez zbytečného odkladu zneplatnění prostředku pro elektronickou identifikaci na základě žádosti držitele, nebo na základě ohlášení držitele o zneužití nebo hrozícím nebezpečí zneužití prostředku pro elektronickou identifikaci,
- při ukončení činnosti zneplatnění jím vydaných prostředků pro elektronickou identifikaci,
- oznámení správci národního bodu zneplatnění prostředku pro elektronickou identifikaci,
- vedení a aktualizace plánu ukončení činnosti a při ukončení své činnosti postupování podle plánu ukončení činnosti,
- kvalifikovaný správce zajistí, aby fyzické osoby, které vykonávají řídící činnosti při správě kvalifikovaného systému, a fyzické osoby, které ověřují totožnost držitele, byly bezúhonné.

1.1.8 Národní identitní autorita (NIA)

Národní identitní autorita, nebo také Portál národního bodu pro identifikaci a autentizaci, je státní instituce spadající pod Digitální a informační agenturu, která je ústředním bodem pro elektronickou identifikaci a autentizaci. NIA zajišťuje bezpečné ověření identity uživatelů při přístupu k elektronickým službám, především eGovernmentu. Umožňuje při tom použití různých elektronických identifikačních prostředků (eObčanka, NIA ID, Bankovní identita, apod.), které provozují různí kvalifikovaní správci. Do oblasti působnosti NIA patří:

- **Národní bod pro identifikaci a autentizaci** jako centrální bod systému, který zajišťuje komunikaci a registraci účastníků tohoto systému. Zajišťuje současně vždy jednoznačné ztotožnění osoby, která prokazuje svoji totožnost s využitím autentizačních prostředků (prostředků pro elektronickou identifikaci). Je definován v zákoně č. 250/2017 Sb. jakožto

informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace. Zajišťuje orgánům veřejné správy státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity.

- **Kvalifikovaný správce,** který vydává jednoznačně identifikovaným fyzickým osobám prostředky pro vzdálenou autentizaci (prokázání totožnosti) a provádí veškeré činnosti spojené se správou těchto prostředků a s prokazováním totožnosti fyzické osoby, tj. spravuje kvalifikovaný systém elektronické identifikace.
- **Kvalifikovaný poskytovatel online služeb,** který připojuje k Národnímu bodu online služby, ke kterým je vyžadováno přihlášení prostředky vydanými kvalifikovanými správci.
- **Základní registry,** které poskytují jednoznačnou identifikaci osoby a zajištění vazeb této osoby vůči referenčním údajům o osobě.
- **Národní uzel eIDAS,** který je samostatnou součástí Národního bodu a zajišťuje přijímání vzdáleného prokázání totožnosti z ohlášených systémů dle nařízení eIDAS a předávání vzdálené identifikace a autentizace z České republiky ostatním státům EU. Ostatní státy EU musí akceptovat české identity od 13. 9. 2020, kdy vypršela roční lhůta pro zavedení akceptace ohlášeného prostředku.

1.1.9 Digitální a informační agentura (DIA)

Dle eIDAS článku č. 17 určí členské státy orgány dohledu, udělí jim nezbytné pravomoci a zdroje. Tyto orgány dohledu mají plnit zejména následující úkoly:

- Vykonávat dohled nad kvalifikovanými poskytovateli služeb vytvářejících důvěru a zajistit, aby jimi poskytované služby splňovaly požadavky nařízení eIDAS.
- Přijmout opatření ve vztahu k nekvalifikovaným poskytovatelům služeb vytvářejících důvěru, pokud je orgán informován, že tito poskytovatelé nebo jimi nabízené služby vytvářející důvěru nesplňují požadavky eIDAS.
- Informovat ostatní orgány dohledu a veřejnost o případech narušení bezpečnosti nebo ztráty integrity.
- Udělovat poskytovatelům služeb vytvářejících důvěru a jimi poskytovaným službám status kvalifikovaného poskytovatele nebo kvalifikované služby a odnímat tento status.
- Informovat subjekt odpovědný za vnitrostátní důvěryhodný seznam podle čl. 22 odst. 3 dle eIDAS o svých rozhodnutích udělit nebo odejmout status kvalifikovaného poskytovatele nebo kvalifikované služby, pokud tento subjekt není rovněž orgánem dohledu.

V České republice je dohledovým orgánem Digitální a informační agentura (DIA).

Digitální a informační agentura byla zřízena na základě Zákona č. 471/2022 Sb. ze dne

23. prosince 2022, kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony [5].

Digitální a informační agentura (dále jen DIA) je ústředním správním úřadem pro elektronickou identifikaci a služby vytvářející důvěru a pro informační systémy veřejné správy. Dle tohoto zákona (§ 2a odst. 3) má tyto úkoly:

- plní koordinační úlohu v oblasti digitálních služeb a digitálních úkonů podle zákona o právu na digitální služby,
- plní koordinační úlohu pro informační technologie,
- plní koordinační úlohu v oblasti evidence a sdílení dat,
- zajišťuje systém podpory centrálních způsobů komunikace veřejné správy,
- zajišťuje odborný rozvoj, školení, sdílení znalostí, osvětu a vzdělávání v oblasti své působnosti,
- provozuje kompetenční centra.

DIA byla zřízena novelou zákona o právu na digitální služby a její politická nezávislost by měla být dána tím, že má nadresortní postavení a je nezávislá na řízení ministerstev a jiných ústředních správních úřadů.

DIA spravuje několik aplikací, například eDoklady (elektronická správa dokladů), Identitu občana (slouží pro bezpečné přihlašování do různých portálů veřejné správy, pojišťoven a dalších služeb) nebo nově Registr zastupování REZA (umožňuje digitální alternativu k papírovým plným mocím vůči veřejné správě, kde je zaručena identifikace zmocňující osoby a umožňuje elektronickou správu poskytnutých plných mocí).

1.1.10 eDoklady

Aplikace eDoklady je spravována DIA a byla spuštěna 2024. Jde o elektronickou alternativu ke klasickým dokladům s tím, že pro začátek je zahrnut pouze občanský průkaz. Postupně se rozšiřují možnosti, kde lze aplikaci použít (policie, soudy, finanční úřady, úřady práce, banky, Česká pošta a další). Povinnost přijímat eDoklady vychází ze Zákona č.1/2024 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů a další související zákony [6].

1.1.11 Autentizace

Autentizace je proces a součást systému elektronické identifikace. Autentizační proces používá jemu předané identifikační prostředky, na jejichž základě ověří identitu osoby, která s nimi nakládá. Výsledkem autentizace by tedy měla být informace, zda osoba je ta, za kterou se vydává a s jakou mírou spolehlivosti (záruky) je touto osobou. Úroveň záruky (nízká, značná a vysoká) závisí na použitých identifikačních prostředcích a procesech užitých pro autentizaci. Jednotlivé úrovně záruky jsou popsány výše v popisu elektronické identifikace.

1.1.12 Poskytovatelé služeb vytvářejících důvěru

Poskytovatelé služeb vytvářejících důvěru se dělí na kvalifikované a nekvalifikované. Nekvalifikovaní poskytovatelé mohou poskytovat služby vytvářející důvěru (například poskytovat potvrzení o studiu nebo absolvování kurzu), ale buď nesplňují přísná kritéria pro zařazení mezi kvalifikované nebo o zařazení nepožádali. Aby byl subjekt zařazen mezi kvalifikované poskytovatele služeb vytvářejících důvěru, musí o to požádat a doložit posouzení shody s požadavky eIDAS.

V České republice spravuje seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru Digitální a informační agentura.

Tabulka 3: Aktuální seznam poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru

číslo	Kvalifikovaní poskytovatelé služeb vytvářejících důvěru	Kvalifikované služby	Zahájení poskytování
1.	První certifikační autorita, a. s. IČO 26439395, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů); Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí; Vydávání kvalifikovaných certifikátů pro elektronické pečetě; Vydávání kvalifikovaných elektronických časových razítek; Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek.	03/2002 04/2017 08/2017 08/2017 02/2018
2.	Česká pošta, s. p. IČO 47114983, Politických vězňů 909/4, PSČ 225 99 Praha 1	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů); Vydávání kvalifikovaných certifikátů pro elektronické pečetě; Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek; Vydávání kvalifikovaných elektronických časových razítek.	09/2005 08/2017 08/2017 08/2017
3.	eIdentity a. s. IČO 27112489, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů). Vydávání kvalifikovaných elektronických časových razítek Vydávání kvalifikovaných certifikátů pro elektronické pečetě	08/2005 01/2018 02/2018
4.	Software602 a. s. IČO 63078236, Hornokrčská 703/15,	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí;	06/2017 06/2017

číslo	Kvalifikovaní poskytovatelé služeb vytvářejících důvěru	Kvalifikované služby	Zahájení poskytování
	PSČ 140 00 Praha 4	Kvalifikovaná služba uchování kvalifikovaných elektronických podpisů a pečetí.	
5.	Správa základních registrů IČO 72054506, Na Vápence 915/14, PSČ 130 00 Praha 3 Správa základních registrů končí činnost kvalifikovaného poskytovatele služeb vytvářejících důvěru k 31. 12. 2023. Správa státních služeb vytvářejících důvěru přebírá k 1. 1. 2024 práva a povinnosti Správy základních registrů v pozici kvalifikovaného poskytovatele služeb vytvářejících důvěru, a to v návaznosti na zákon č. 471/2022 Sb.	Vydávání kvalifikovaných certifikátů pro elektronické podpisy; Vydávání kvalifikovaných certifikátů pro elektronické pečetě; Vydávání kvalifikovaných elektronických časových razítek Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí	05/2019 10/2022
6.	SEFIRA spol. s r.o., IČO 62907760, Antala Staška 2027/77, PSČ 140 00 Praha 4	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.	08/2019
7.	TECHNISERV IT, spol. s r. o. IČO 26298953, Traťová 574/1, PSČ 619 00 Horní Heršpice, Brno	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.	08/2022
8.	Komerční banka, a.s., IČO 45317054, Na Příkopě 33 čp. 969, PSČ 114 07 Praha 1	Vydávání kvalifikovaných certifikátů pro elektronické podpisy Vydávání kvalifikovaných certifikátů pro elektronické pečetě Vydávání kvalifikovaných elektronických časových razítek	06/2023
9.	Správa státních služeb vytvářejících důvěru, IČO 19122063, Na Vápence 915/14, PSČ 130 00 Praha 3 Správa státních služeb vytvářejících důvěru přebírá k 1.1.2024 práva a povinnosti Správy základních registrů v pozici kvalifikovaného poskytovatele služeb vytvářejících důvěru, a to v návaznosti na zákon č. 471/2022 Sb.	Vydávání kvalifikovaných certifikátů pro elektronické podpisy Vydávání kvalifikovaných certifikátů pro elektronické pečetě Vydávání kvalifikovaných elektronických časových razítek Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí	11/2023 11/2023 01/2024 01/2024
10	Seyfor, a. s., IČO 01572377, Drobného 555/49, Ponava, PSČ 602 00 Brno.	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí.	04/2025

Zdroj: https://www.dia.gov.cz/cs/legislativa/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/povinne-zverejnovane-informace/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru

1.1.13 Služby vytvářející důvěru

Služby vytvářející důvěru jsou služby, které eIDAS definuje a reguluje. Mají za úkol vytvářet důvěru pro vnitrostátní i přeshraniční elektronické transakce.

Pro zvýšení konkurenceschopnosti EU a v reakci na rychle se měnící online trh se EU

rozhodla zavést alespoň základní pravidla pro online služby tak, aby byly připraveny pro přeshraniční komunikaci v rámci všech států EU. Zejména se jedná o služby, které využívají úřady mezi sebou, ale také ve vztahu k občanům, kde je potřeba jednoznačné a bezpečné identifikace jednajících stran.

Proto mezi tyto regulované služby jsou zahrnuty:

- vytváření a ověřování platnosti elektronických podpisů nebo elektronických pečetí,
- vytváření a ověřování platnosti elektronických časových razítek,
- služby elektronického doporučeného doručování,
- vytváření a ověřování platnosti elektronických certifikátů související se službami vytvářejících důvěru,
- vytváření a ověřování shody a platnosti certifikátů pro autentizaci internetových stránek.

Aktuální seznam všech poskytovaných služeb lze najít na stránkách Digitální a informační agentury (viz. kapitola 1.1.12 Poskytovatelé služeb vytvářejících důvěru).

1.1.14 Elektronický podpis

Elektronický podpis je způsob autentizace, který zaručuje pravost a integritu elektronických dokumentů. Jsou to data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání. Rozeznáváme několik typů elektronických podpisů:

- prostý podpis - základní podpis s nejnižší úrovni zabezpečení, kdy ověřitelnost takového podpisu není velká a je snadno zneužitelný,
- zaručený podpis - podepisující osoba se ověřuje a je založen na certifikátu, který ale nemusí být uznáván v celé EU. Má nižší úroveň zabezpečení a ověřitelnosti než kvalifikovaný podpis,
- kvalifikovaný podpis - je vytvořen pomocí kvalifikovaného prostředku pro vytváření podpisů, založený na certifikátu ověřeném certifikační autoritou. Takový podpis je jednoznačně spojen s podepisující osobou a je rovnocenný vlastnoručnímu podpisu.

1.1.15 Časové razítko

Časové razítko je digitální záznam, který prokazuje, že elektronický dokument existoval v určitém čase. Kvalifikované časové razítko je důkazem, že elektronický dokument, který je jím označený, existoval v okamžiku uvedeném v daném časovém razítku a nebyl tento dokument později změněn.

1.1.16 eGovernment

eGovernment je ekvivalent veřejné správy a to prostřednictvím elektronických technologií. Podnikatelé i občané mají díky elektronizaci úřadů snadnější přístup k informacím a službám úřadů online, tedy odkudkoliv a kdekoliv mají přístup k internetu. Cíle eGovernmentu jsou:

- úspora času,
- zlepšení efektivity,
- zvýšení bezpečnosti,
- zvýšení transparentnosti,
- zlepšení uživatelské zkušenosti,
- zvýšení vzdělanosti v elektronické komunikaci a kyberbezpečnosti.

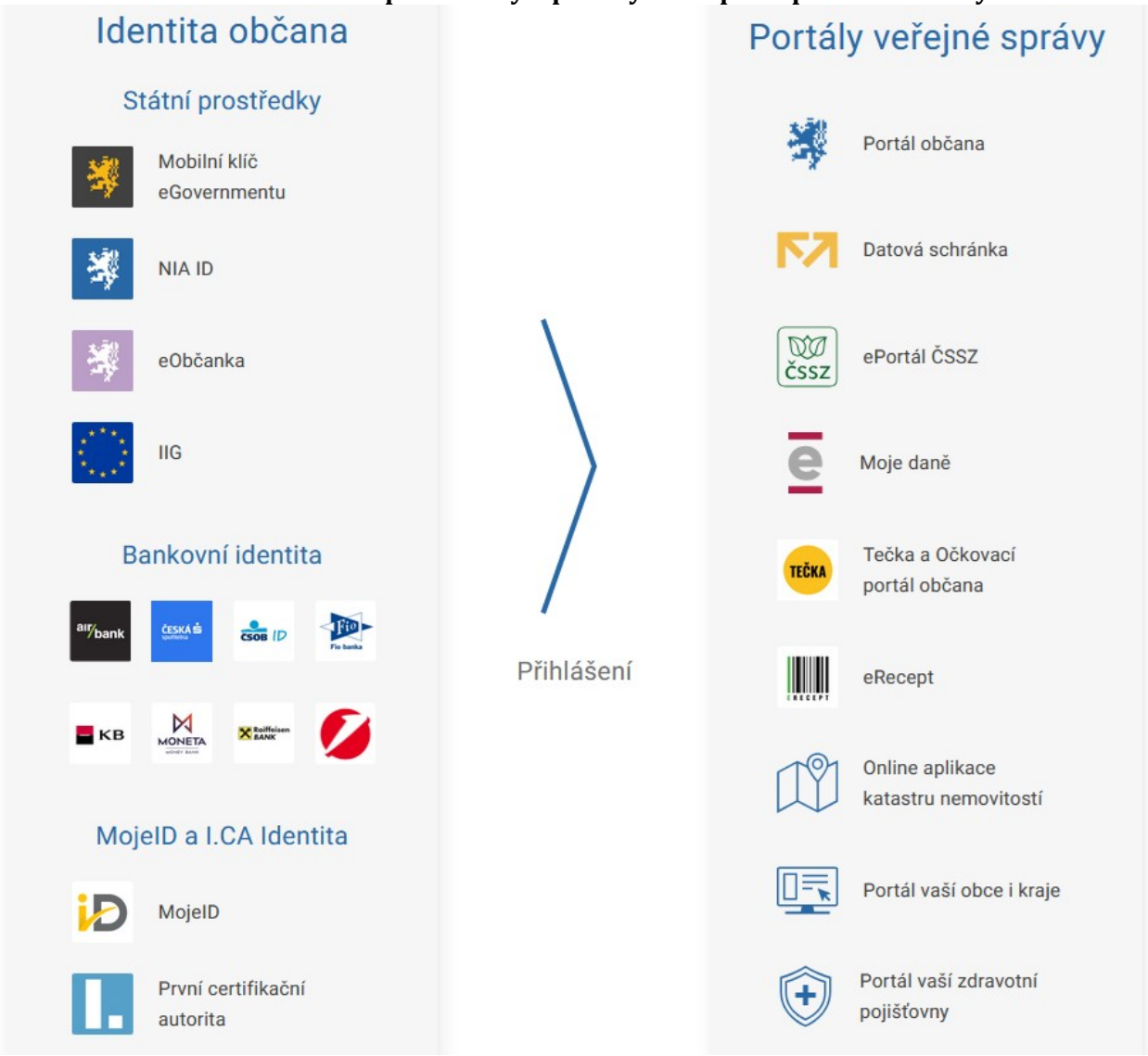
eGovernment přinesl praktické nástroje (nejen) pro komunikaci s úřady, které se v průběhu let osvědčily a staly se běžnou součástí osobního i podnikatelského života. Příkladem může být zavedení Datových schránek pro doručování nebo online podávání žádostí a podání pro úřady za pomocí interaktivních webových formulářů s nápovědou. Mít úřad dostupný kdykoliv, bez ohledu na úřední hodiny, byl velký milník pro komunikaci občanů a podnikatelů s úřady. Je ještě mnoho oblastí, kde digitalizace prozatím zaostává (zdravotnictví, soudy), ale daří se vytvářet nástroje, které by měly pomoci při digitalizaci procesů.

Příkladem nově vzniklého úřadu je například Správa státních služeb vytvářejících důvěru, která byla zřízena v roce 2023 za účelem poskytování služeb pro potřeby státu. Je to instituce spadající pod DIA a zastřešuje důvěryhodné služby pouze pro vybrané bezpečnostní složky státu, jako jsou Ministerstvo vnitra ČR, Policie České republiky, policejní školy, Bezpečnostní informační služba České republiky, Generální ředitelství cel a další. Napomáhá těmto úřadům s přístupem k digitálním službám, adaptací na nové podmínky a požadavky v elektronické komunikaci, jako je zavádění elektronického podepisování nebo vícefaktorová identifikace zaměstnanců.

Pro elektronickou komunikaci podniků, podnikatelů nebo občanů s úřady vzniká mnoho služeb a online formulářů přímo v režii jednotlivých úřadů, což vede k jejich nepřehlednosti. Vznikají proto i rozcestníky, kde jsou hlavní služby popsány a občan má možnost přistupovat k různým portálům veřejné správy z jednoho místa.

Takovým rozcestníkem je Identita občana spravovaná DIA, kde je možné se přihlásit pomocí některé z kvalifikovaných služeb vytvářejících důvěru, včetně dokladů vydaných v zahraničí (elektronická brána International ID Gateway, IIG):

Obrázek 1: Přihlašovací prostředky a portály dostupné z portálu Identity občana



Zdroj: Portál Identita občana, https://www.identita.gov.cz/

Portál Identita občana je dostupný z adresy: https://www.identita.gov.cz/
Webový rozcestník pro český eGovernment je dostupný z adresy: https://portal.gov.cz/

1.1.17 Datové schránky

Datové schránky jsou doručovacím systémem pro elektronickou komunikací (nejen) se státními institucemi, který umožňuje zdarma komunikovat s úřady (ale i jinými subjekty) jako ztotožněný uživatel. Zavedeny byly v roce 2009 a postupně se rozšiřoval počet služeb i počty uživatelů. Velký nárůst uživatelů přišel v roce 2023, kdy vznikla povinnost zřízení datové schránky pro všechny podnikající fyzické osoby. Nyní je povinnost mít zřízenou datovou schránku pro:

- orgány veřejné moci jako jsou úřady, zdravotnická zařízení, školy, samosprávy a další,
- všechny právnické osoby zapsané ve veřejném rejstříku,
- fyzické podnikající osoby zapsané v registru živnostenského podnikání nebo v jiné evidenci.

Dle informací DIA mělo v roce 2024 svou datovou schránku téměř 5 milionů uživatelů[7].

Získat datovou schránku je možné pomocí elektronické identifikace přes portál Identita občana (popsán v kapitole 1.1.16 eGovernment) nebo osobně na Czech POINT (fyzické kontaktní místo veřejné správy, které slouží pro komunikaci s různými úřady z jednoho místa).

Dokumenty doručené pomocí datových schránek mají tedy stejnou platnost, jako listinné dokumenty. Pomocí datové schránky je možné dělat podání a provádět úkony vůči orgánům veřejné moci. V případě přijetí zprávy je možné poslat notifikaci na zadanou emailovou adresu. Zprávy se ve schránce uchovávají 90 dní od doručení a po této lhůtě jsou vymazány. Proto je potřeba zprávy po přečtení uchovávat ve vlastním úložišti nebo využít některou ze služeb archivace.

Občan ani podnikatel nemá povinnost komunikovat s úřadem pomocí datových schránek, ale naopak úřady tuto povinnost mají. To je pro občany i podnikatele velký benefit a jistota, že se důležité zprávy z úřadu nikam nezatoulají a najdou je na jednom místě.

Odesílatel i příjemce mají k dispozici dodejku (potvrzení o doručení), která jednoznačně určuje stav doručení datové zprávy a je použitelná jako nezpochybnitelný důkaz u soudu. Proto je datová schránka vhodná i pro komunikaci v rámci pracovněprávních vztahů. Podporuje odesílání a přijímání elektronicky podepsaných dokumentů spolu s časovými razítky. Zpráva, která byla doručena do datové schránky je po 10 dnech považována za doručenou, i když si ji adresát nepřečte (tzv. fikce doručení). To je důležité jak pro úřady, tak pro další subjekty komunikující pomocí datových schránek.

1.1.18 Certifikáty pro autentizaci internetových stránek

Vydávání, ověřování shody a platnosti certifikátů pro autentizaci internetových stránek je služba vytvářející důvěru dle eIDAS. Certifikáty jsou vydávány kvalifikovanými poskytovateli služeb vytvářející důvěru a to jak fyzickým, tak právnickým osobám. Propojují tyto stránky s osobou, které byl certifikát vydán. Označují se jako QWAC (Qualified Website Authentication Certificate) certifikáty. Je sporné jejich širší využití, což dosvědčuje skutečnost, že tuto službu mají schválenou na tuzemském trhu pouze dva z deseti poskytovatelů kvalifikovaných služeb:

- Certifikát I.CA - certifikáty První certifikační autority jsou dle dostupných informací vydávány pouze právnickým osobám nebo organizačním složkám státu. Jde o certifikát využívající RSA kryptografický algoritmus pro zabezpečení komunikace.
- Certifikát PostSignum - certifikát od České pošty je dle dostupných informací "pouze" komerčním certifikátem a tedy nikoliv kvalifikovanou službou dle eIDAS.

V komerční sféře se používají tři typy SSL certifikátů:

- SSL DV (domain validation) - certifikát s ověřením vlastníka domény. Jde o základní certifikát, kdy je ověřeno, že vlastníkem domény je žadatel o certifikát.
- SSL OV (organization validation) - certifikát s ověřením společnosti, která provozuje doménu.

- SSL EV (extended validation) - certifikát vyšší úrovně, kdy se ověřuje nárok společnosti na doménu, platnost adresy nebo telefonního spojení. V některých prohlížečích se poté zobrazí adresní řádek zelenou barvou.

Kvalifikovaný QWAC certifikát dle eIDAS odpovídá "vylepšenému" komerčnímu SSL EV certifikátu, kde navíc probíhá ověření totožnosti žadatele. Podle výše uvedených zjištění takový certifikát na našem území vydává pouze První certifikační autorita,a.s..

1.2 Koncepce eIDAS (electronic Identification (eID) And Trust Services)

1.2.1 Vznik eIDAS

Přímé kořeny myšlenky eIDAS pocházejí z prvního pokusu o sjednocení evropské legislativy v oblasti elektronizace a to za pomocí směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy, která byla jednak zaměřena hlavně na elektronické podpisy a jednak šlo "pouze" o směrnici a nikoliv nařízení. Bylo tedy spíše doporučením. Její naplňování jednotlivými státy nepřineslo očekávané výsledky. Často zmiňovanou překážkou byla absence kritérií pro služby ověřování elektronického podpisu. Vnitrostátní i přeshraniční přijímání elektronických podpisů blokovala také nedostatečná technická interoperabilita. Vedla ke vzniku mnoha izolovaných ostrovů - aplikací elektronického podpisu, kdy lze osvědčení použít pouze pro jedinou aplikaci. Dalším úskalím byly úrovně záruk - vládla všeobecná nedůvěra ve spolehlivost identifikace podepisujících či jinak jednajících osob z jiných států.

Kladným přínosem směrnice 1999/93/ES bylo nesporně větší ukotvení elektronické formy podpisu do vnitrostátních legislativ. Přinesla větší právní jistotu a o obecnou přijatelnost elektronických podpisů.

1.2.2 Nařízení eIDAS

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

Tato nová směrnice tedy nahradila směrnici 1999/93/ES o zásadách Společenství pro elektronické podpisy. Na rozdíl od předchozí směrnice 1999/93/ES je eIDAS rovnou nařízením, tedy bylo účinné dnem vyhlášení. Nařízení eIDAS se dotýká všech občanů Evropské unie a to zejména v oblastech eGovernmentu (komunikace s úřady, elektronizace a digitalizace úřadů), služeb vytvářejících důvěru (elektronické podpisy a pečetě, časová razítka, elektronické doručování a uchovávání elektronických dokumentů) a digitální identity (identifikace jednotlivých osob, kdy jsou prostředky pro elektronickou identifikaci vydávány konkrétním osobám, které se poté těmito prostředky prokazují).

1.2.3 Cíle eIDAS

- **Nastavení společného rámce pro elektronickou výměnu informací** - nastavení podmínek

a standardů pro všechny státy EU, umožňující přeshraniční výměnu elektronických identifikačních údajů a aplikací vytvářející důvěru napříč všemi státy Evropské unie.

- **Zvýšení bezpečnosti a důvěryhodnosti** - posílení společné bezpečnostní politiky pro zvýšení důvěryhodnosti elektronických transakcí jak pro občany Evropské unie, tak pro podnikatelské subjekty.
- **Umožnit uznávání systémů elektronické identifikace jinými státy EU** - kvalifikovaný systém elektronické identifikace, který je ohlášen členským státem EU Komisi, projde schvalovacím procesem a je zařazen mezi ohlášené kvalifikované systémy elektronické identifikace a je uznáván ostatními členskými státy Evropské unie.
- **Zavedení právního základu pro platnost elektronických podpisů** - snaha o to, aby elektronický podpis měl stejnou právní platnost jako dosavadní papírová forma.
- **Snížení administrativní zátěže** - zjednodušení a zefektivnění elektronických transakcí spolu s podporou vzájemného uznávání má vést ke snížení administrativní zátěže zvláště u přeshraničních transakcí.
- **Přezkum a vyhodnocení** - v článku č. 49 nařízení eIDAS se Komise zavazuje k přezkoumání uplatňování nařízení a podá zprávu Evropskému parlamentu a Radě (EU). Vyhodnocení má být předloženo každé čtyři roky ve formě zprávy o pokroku v dosahování cílů.

1.2.4 Prováděcí předpisy eIDAS

Prováděcí rozhodnutí Komise upřesňují a doplňují nařízení eIDAS o konkrétní kroky, postupy nebo specifikace potřebné pro naplnění cílů eIDAS. Mezi nejdůležitější ve vztahu k eIDAS patří:

Prováděcí rozhodnutí Komise (EU) 2015/296 - kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu Text s významem pro EHP (Evropský hospodářský prostor).

Prováděcí rozhodnutí Komise (EU) 2015/806 - kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru. Poskytovatelé kvalifikovaných služeb vytvářejících důvěru dle eIDAS mohou dobrovolně používat značku důvěry EU, aby bylo uživatelům srozumitelné, že se jedná o kvalifikovanou službu dle eIDAS. Značku je možné používat pro označení služeb poté, co bude kvalifikovaný status zveřejněn v důvěryhodném seznamu členského státu dle čl. 22 eIDAS.

Obrázek 2: Značka důvěry EU v barevném provedení

Zdroj: EU, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG

Obrázek 3: Značka důvěry EU v černobílém provedení

Zdroj: EU, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3AOJ.L_.2015.128.01.0013.01.ENG

Prováděcí rozhodnutí Komise (EU) 2015/1501 - o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU). Nařízení stanovuje požadavky na vzájemné propojení oznámených systémů elektronické identifikace, které budou zajišťované takzvanými uzly, které budou součástí architektury interoperability elektronické identifikace. Tyto uzly budou zajišťovat bezpečnou a spolehlivou přeshraniční identifikaci dle eIDAS. V České republice provoz tohoto uzlu vysoutěžila podruhé společnost CZ.NIC z.s.p.o., Praha 3.

Prováděcí rozhodnutí Komise (EU) 2015/1502 - kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci. Nařízení stanovuje minimální technické specifikace a postupy pro tři úrovně záruky: nízká, značná a vysoká (viz. výše popis Elektronická identifikace v kapitole 1.1.2 Základní pojmy).

Prováděcí rozhodnutí Komise (EU) 2015/1505 - kterým se stanoví technické specifikace a formáty důvěryhodných seznamů. Dle tohoto nařízení má každý členský stát EU povinnost zřídit, zveřejnit a udržovat důvěryhodné seznamy, které obsahují informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru (viz. výše Poskytovatelé služeb vytvářejících důvěru v kapitole 1.1.2 Základní pojmy).

Prováděcí rozhodnutí Komise (EU) 2015/1506 - kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného

sektoru. Členské státy musí také ostatním státům umožnit ověřit obdržené elektronické podpisy a pečetě online a bezplatně.

Prováděcí rozhodnutí Komise (EU) 2015/1984 - kterým se stanoví okolnosti, formáty a postupy pro oznamování systémů elektronické identifikace. Členský stát, který oznamuje systém elektronické identifikace, má povinnost Komisi poskytnout všechny údaje o posuzovaném systému elektronické identifikace (včetně záruk) a o subjektech, které jsou zapojeny v systému elektronické identifikace.

1.3 Nařízení eIDAS 2

V Nařízení eIDAS v článku č. 49 se počítalo s revizí plnění a případnou novelizací eIDAS. Revize nařízení eIDAS poukázala mimo jiné na nízké přeshraniční uznávání elektronické identifikace, kdy jen menší část členských států Evropské unie oznámilo/notifikovalo systém elektronické identifikace. Novelizace eIDAS byla přijata v podobě Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu [8].

Tato novelizace eIDAS se obecně označuje jako eIDAS 2 a přinesla několik novinek. Jde zejména o novou službu vytvářející důvěru nazvanou "Vydávání elektronického potvrzení atributů a ověřování platnosti elektronického potvrzení atributů". Tímto se zřizuje "evropský rámec pro digitální identitu, který členské státy EU pověřuje, aby do konce roku 2026 svým občanům, rezidentům a podnikům poskytly peněženku digitální identity EU na základě stejných specifikací. Cílem tohoto rámce je občanům EU zajistit bezpečnou identifikaci online i offline, která umožňuje bezproblémový a důvěryhodný přístup k veřejným a soukromým přeshraničním digitálním službám" [9].

Dalšími novinkami je možnost vzdáleného podepisování a pečetění (příslušný certifikát je uložen na vzdáleném serveru), elektronická archivace (práce s elektronickými dokumenty) a elektronická kniha záznamů (ukládání záznamů posloupnosti elektronických úkonů podle času).

1.3.1 Evropská digitální identita

Vychází z původního nařízení eIDAS z roku 2014, kdy členské státy EU mohly Komisi oznamovat systémy elektronické identifikace, které po procesu schvalování byly povinně uznávány ve všech ostatních státech EU. Těchto oznámených systémů elektronické identifikace však bylo jednotlivými státy oznámeno velmi málo. Důvody mohly být různé - od nedostatku firem poskytujících tyto služby, přes nedostatek úředníků schopných připravit národní podmínky a výzvy a v neposlední řadě mohla být důvodem dobrovolnost, protože oznámení takových identifikačních systémů bylo dobrovolné. Proto v novelizaci eIDAS 2 dochází k doplnění služeb spojených s digitální identitou a to jak ve směru k členským státům, kdy jim ukládá povinnost zavést alespoň jednu službu poskytující důvěru nazvanou Peněženka digitální identity EU, která v sobě zahrnuje služby digitální

identity, tak i ve směru k občanům, kterým má tato služba přinést lepší kontrolu nad svými identifikačními údaji. Dle předpokladů by do konce roku 2026 měl mít každý občan EU možnost získat správu nad vlastní Peněženkou digitální identity EU, která by měla obsahovat potřebné identifikační údaje uznávané ve všech státech EU.

1.3.2 Vydávání elektronického potvrzení atributů a ověřování platnosti elektronického potvrzení atributů

Vydávání elektronického potvrzení atributů vychází z myšlenky zavedení evropské digitální identity a jde o novou službu vytvářející důvěru. Služba má umožnit autentizaci vybraných atributů osoby a tyto atributy budou mít stejnou platnost jako oficiální doklad z běžného života. Může jít například o ověření zletilosti, potvrzení vlastnictví řidičského oprávnění pro skupinu C, adresy, pohlaví, rodinného stavu nebo absolvování vysokoškolského studia. Atributů, které se takto budou uchovávat, ověřovat a prezentovat na základě vůle jeho vlastníka (občana) bude celá řada a bude záležet na trhu, kdo všechno si zažádá o kvalifikaci pro vydávání takových atributů. Některé atributové certifikáty budou s největší pravděpodobností vydávány povinně držiteli zdrojových informací nebo jimi pověření zástupci. Mohou to být školy, vzdělávací instituce nebo úřady. Jiné subjekty si budou moci zažádat o osvědčení k vydávání těchto elektronických atributů nebo spolupracovat s některým z kvalifikovaných poskytovatelů služeb vytvářejících důvěru, který bude atributy vydávat z jejich pověření.

Tato služba by měla být součástí Peněženky digitální identity EU a je předpoklad jejího širokého využití.

1.3.3 Peněženka digitální identity EU (EU Digital Identity Wallet, EUDIW)

Peněženka digitální identity EU, někdy taky nazývaná jako evropská digitální peněženka (dále jen Peněženka), je reakcí na nedostatečnou implementaci elektronické identifikace eIDAS jednotlivými státy v uplynulých letech. Původní myšlenka eIDAS spočívala v zavedení národních systémů identit, které jednotlivé státy předloží (ohlásí) Evropské radě a ty budou po schválení, stejně jako jiné služby vytvářející důvěru, uznávány ostatními státy EU. To se naplnilo jen z části, a proto přichází novelizace s "hotovým polotovarem", který by mělo být jednodušší implementovat a pomoci tak státům, kde digitalizace a elektronizace státní správy jde pomaleji.

Peněženka digitální identity EU má být snadno přenositelná (mobilní aplikace) a umožňovat ukládání a zobrazení osobních identifikačních údajů a potvrzení atributů jak online, tak offline.

Hlavní benefity:

- **snadnější přístup k digitálním službám** - služba Peněženky zefektivní a zjednoduší proces ověřování identity pro různé služby a nebude nutné si pamatovat přístupové údaje pro každou službu zvlášť,
- **snadnější kontrola a aktualizace údajů** - uživatel (občan) si zvolí, jaké údaje o sobě

poskytne a má plnou kontrolu nad svými údaji na jednom místě,

- **bezpečnost** - jednotlivé Peněženky budou spravovány kvalifikovanými poskytovateli služeb vytvářejících důvěru, kteří podléhají dozoru a přísným bezpečnostním podmínkám,
- **snadné použití** - aplikace Peněženky bude mít společné uživatelské rozhraní, které bude dostupné jak online, tak offline,
- **bezplatné elektronické podepisování** - všechny fyzické osoby mají mít možnost bezplatně a kvalifikovaně podepisovat pro nekomerční (neprofesionální) účely.

Zajímavým benefitem je možnost elektronicky podepisovat kvalifikovaným certifikátem pro nekomerční použití. Zatím není jasně vymezen rámec toho, co je považováno za nekomerční (či neprofesionální) použití a bude to nejspíše ještě upraveno. Za zmínku stojí, že nejspíše takový certifikát nebude (ze své podstaty) omezen svou platností.

Každý členský stát EU má za povinnost poskytnout alespoň jednu Peněženku digitální identity do 21. 11. 2026. Což není příliš dlouhá doba. Požadavkem na získání přístupu k Peněžence je úroveň záruky "vysoká". Tedy pro získání Peněženky je nutné se přihlašovat pomocí vysoké úrovně zabezpečení, s čímž mají některé státy potíže, protože nemají na trhu dostatek prostředků této nejvyšší úrovně. Jde o úroveň, kdy je zapotřebí hardwarový prostředek pro identifikaci, což například služba Bankovní identita nesplňuje (má úroveň záruky "značná") a nelze ji tedy použít pro získání nebo přístup k Peněžence.

V České republice se buduje v gesci Digitální a informační agentury aplikace eDoklady, která má potenciál se takovou Peněženkou stát. Prozatím lze do této aplikace uložit jen občanský průkaz, ale počítá se s dalším rozšířením na řidičský průkaz a další doklady a údaje.

1.3.4 Vzdálené podepisování

Vzdálené podepisování dle eIDAS umožňuje využít certifikát uložený na vzdáleném serveru a přistupovat k němu z libovolného zařízení po elektronické identifikaci. Dokument, který bude uživatel chtít podepsat, odešle vzdálené službě, ke které se přihlásí pomocí elektronické identity minimálně pomocí dvoufaktorové autentizace. Poté tato služba dokument podepíše a zabezpečeně pošle zpět uživateli. Uživatel tedy nemusí být u hardwarového zařízení, kterým podepisuje a které obsahuje podpisové certifikáty, fyzicky přítomen.

1.3.5 Elektronická archivace

Elektronickou archivací se rozumí důvěryhodné vytváření, uchovávání, zpřístupnění a skartace elektronických dokumentů. Po celou dobu musí být zachována jejich integrita, čitelnost a důkaz původu. Opatřuje se časovým razítkem, případně jinými prostředky prokazujícími, že dokument existoval v době vzniku ve stejné podobě a nebylo s ním manipulováno.

1.3.6 Elektronická kniha záznamů

Elektronickou knihou záznamů se rozumí důvěryhodná služba, která zajistí ověřenou posloupnost elektronických datových záznamů, zajistí integritu těchto záznamů a přesnost

chronologického pořadí těchto záznamů. Jde o službu poskytovanou kvalifikovanými poskytovateli služeb vytvářejících důvěru. V kombinaci s dalšími službami, ať už s Peněženkou digitální identity EU nebo Elektronickou archivací, může jít o hojně využívanou službu, kdy je zaručen původ podepsaného dokumentu i s přesným časem vzniku.

1.4 Důvěryhodné spojení - NIS 2 a nový kybernetický zákon

Služby pro vytváření zabezpečených dokumentů a bezpečných elektronických identifikací by nemohly fungovat bez zabezpečených počítačových a telekomunikačních sítí. Na tuto oblast sezaměřuje legislativa zabývající se kyberbezpečností. V rámci EU je realizována, spolu s eIDAS, směrnicí NIS (Network and Information System) a nově také NIS 2. Tyto směrnice určují, které oblasti jsou regulovány a jakým způsobem. Směrnice a navazující zákony mají za úkol posílit kybernetickou bezpečnost a chránit digitální prostor před hrozbami. Důraz je při tom kladen na prevenci, řízení rizik a hlášení incidentů.

1.4.1 NIS

Cílem směrnice bylo nastavit minimální úroveň zabezpečení v subjektech, které poskytují služby ve společensky významných oblastech, jakými jsou dodávky energií, zdravotní služby, bankovnictví nebo digitální infrastruktura.

1.4.2 NIS 2

Aktuálně byl prezidentem podepsán nový zákon o kybernetické bezpečnosti [10], který implementuje směrnici NIS 2 a vejde v platnost 1. 11. 2025. Subjekty, na které se bude vztahovat povinnost plnit tímto zákonem stanovené povinnosti, budou mít lhůtu 60 dnů na ohlášení regulované služby a roční lhůtu k zavedení povinností. Půjde opět o proces samoidentifikace, tedy podnik musí sám vyhodnotit, zda poskytuje některou z regulovaných služeb. Platí při tom, že stačí poskytovat jednu takovou službu a nemusí jít o hlavní podnikatelskou činnost.

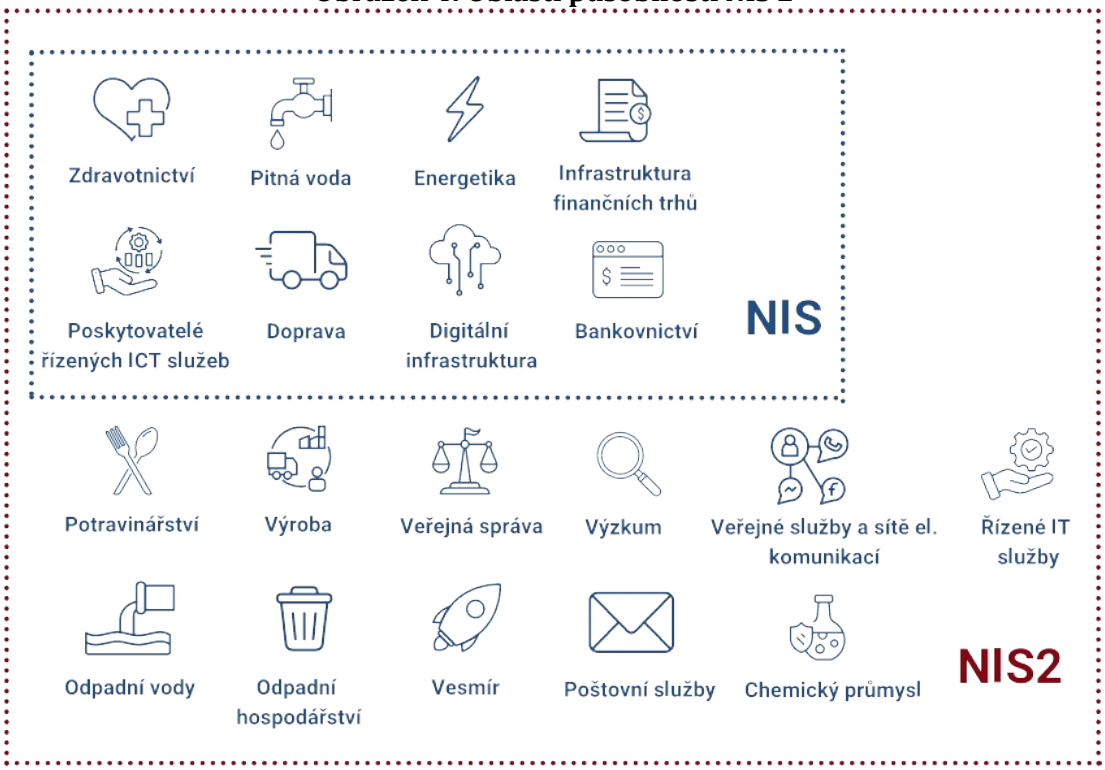
Pro určení, kterých podniků se nový zákon týká, jsou důležitá dvě kritéria:

- podnik zaměstnává alespoň 50 zaměstnanců nebo má roční obrat či bilanční sumu aktiv přesahující 10 mil. EUR,
- podnik poskytuje alespoň jednu z tzv. regulovaných služeb ve vyjmenovaném sektoru služeb.

Zda služba spadá mezi regulované služby je možné ověřit pomocí kalkulačky, která je dostupná na portálu NÚKIB:
https://portal.nukib.gov.cz/kalkulacka?mtm_campaign=Kalkulacka_aktualita.

V novém nařízení se oproti původní NIS rozšiřuje oblast působnosti o další sektory, jako například veřejná správa, poštovní služby, chemický průmysl nebo výzkum:

Obrázek 4: Oblasti působnosti NIS 2



Zdroj: Portál NÚKIB, https://portal.nukib.gov.cz/pruvodce-smernici-nis2

Jelikož jde o kritickou prioritu, za řízení kybernetické bezpečnosti bude nově plně zodpovědné vedení společnosti.

Co se u NIS 2 nezměnilo a zůstává stejné s původní NIS je rozdělení podniků do dvou kategorií:

- Režim nižších povinností - subjekty poskytující důležité služby pro chod společnosti, ale nejsou zařazeny do režimu vyšších povinností. Jejich výpadek nemá tak vážné dopady na společnost. Z povinností se na ně oproti režimu vyšších povinností nevztahuje například audit kybernetické bezpečnosti.
- Režim vyšších povinností - subjekty, které mají klíčový význam a jejich výpadek má vážné dopady na společnost. Podléhají širším povinnostem například v řízení rizik nebo vyhodnocování kybernetických bezpečnostních událostí.

Podnik se bude přihlašovat ke své povinnosti pomocí webového portálu Národního úřadu pro kybernetickou bezpečnost (NÚKIB). Odhaduje, že nově se povinnosti, ať už v nižším nebo vyšším režimu povinností, budou vztahovat na 6 000 až 10 000 firem a podniků. To je velký nárůst oproti původním několika set organizacím. Velkou neznámou v počtech bude hrát i vymezení pojmu "cloud computingu", který zatím není jasně vymezen. Nový zákon o kybernetické bezpečnosti říká, že se takovou službou rozumí "služba informační společnosti podle právního předpisu upravujícího služby informační společnosti, která umožňuje samoobslužnou správu a široký vzdálený přístup k rozšiřitelnému a pružnému seskupení sdílitelných výpočetních zdrojů, včetně těch, které jsou rozmístěny na více místech" [10]. Mohl by se tedy dotýkat mnohem většího počtu služeb využívající

sdílené cloudové zdroje.

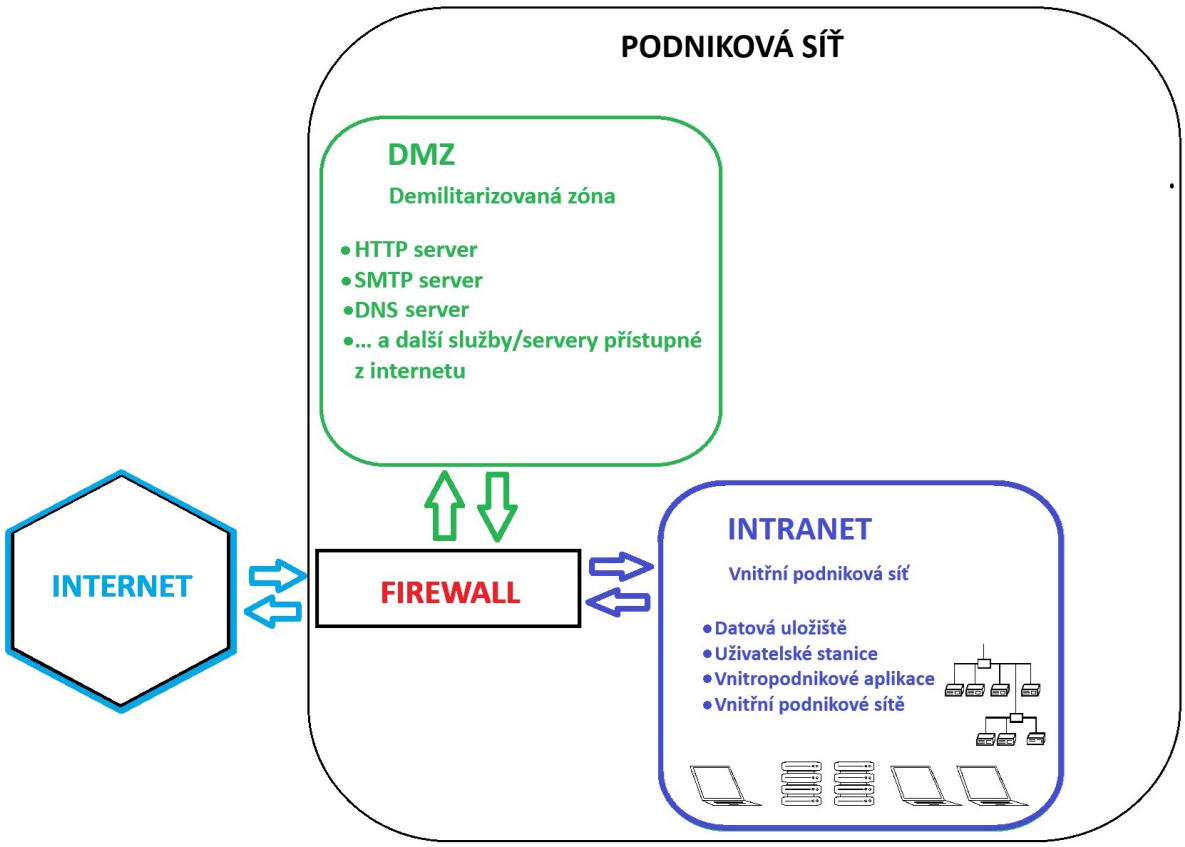
1.5 Podnikové systémy a eIDAS

Podnikové systémy již služby vytvářející důvěru dle eIDAS v různé míře využívají. Ať to je podepisování dokumentů nebo přístup ke službám eGovernmentu. Podle použití a přístupu k internetu lze podnikové sítě rozdělit na vnitřní (intranet) a vnější aplikace přístupné z internetu. Určitou část informačního systému si z bezpečnostních a jiných důvodů firmy udržují pouze v rámci vnitřní sítě (intranetu) a pouze určité služby a informace jsou dostupné z vnějšího prostředí. Řešení mohou být různá, například vyčleněním specifických služeb do tzv. demilitarizované zóny (DMZ).

DMZ je speciální část počítačové sítě, která je oddělená od zbytku interní počítačové sítě bezpečnostními prvky a zároveň je do této části umožněn přístup z internetu (opět přes bezpečnostní prvky). Typickými službami, které se takto zpřístupňují z internetového prostředí jsou HTTP neboli webové servery (www stránky), SMTP server (přenos emailů), DNS server (zajišťuje překlad názvů domén webových stránek) a další služby (eshop, AI nástroje, apod.), které chce firma poskytovat vnějšímu světu prostřednictvím internetu (a nejen internetu).

Bezpečnostní prvky pro ochranu DMZ a vnitřní sítě podniků mohou být jak hardwarové, tak softwarové. Jejich technologie se neustále vyvíjí a je nad rámec této práce. Pro zjednodušení pouze řekněme, že zabezpečují komunikaci jak ven, tak dovnitř chráněné sítě. Zjednodušené schéma podnikové sítě je na následujícím obrázku:

Obrázek 5: Podniková síť s DMZ



Zdroj: vlastní zpracování

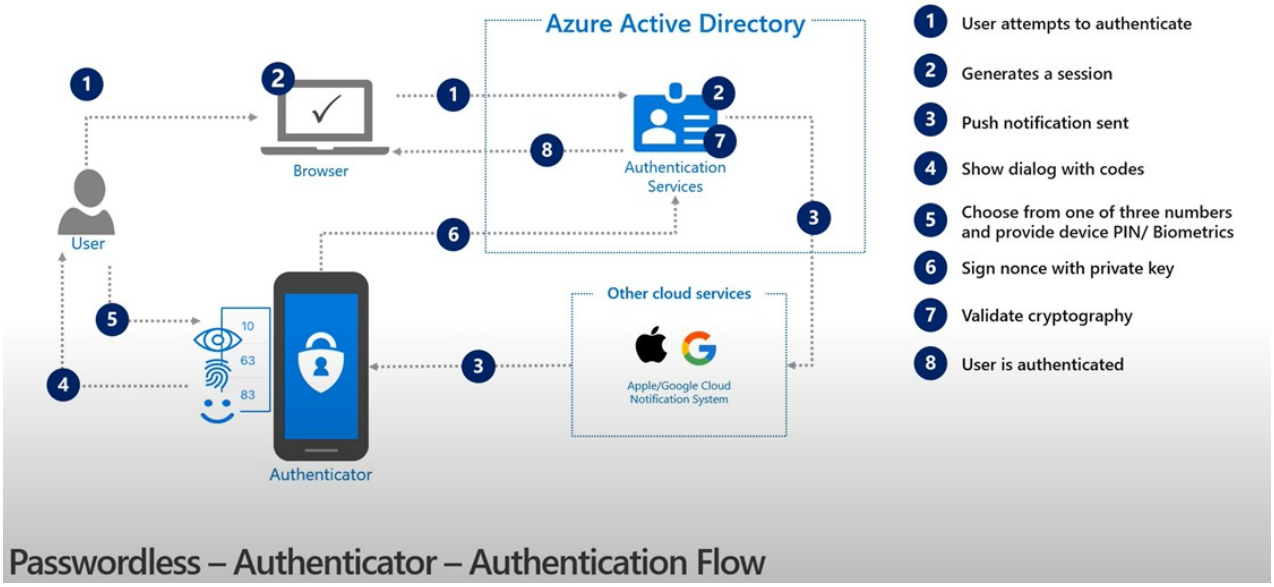
1.5.1 Podnikové systémy a vnitřní uživatelé

Podnikové systémy již mají svá řešení pro přihlašování uživatelů hotová. Nejčastěji jde o vlastní řešení s vlastní správou uživatelských účtů, které se v průběhu let vyvíjelo od uzavřeného intranetu po současná víceúrovňová řešení. Přihlašování uživatelů je obvykle rozdílné do vnitřní sítě podniku a do aplikací přístupných z internetu. Uživatelé vnitřní sítě jsou nejčastěji zaměstnanci podniku nebo externisté s obdobnými právy na služby a dokumenty jako zaměstnanci.

Zpravidla platí, že všichni tito lidé mají už v informačním systému podniku svou identitu uloženou a schválenou odpovědnými správci. Mají k dispozici přihlašovací údaje a často se také přihlašují přes notebooky či počítače s předinstalovanými programy nastavenými pro přihlašování.

Jako příklad takovéto správy uživatelů, fungujících na vícefaktorovém přihlašování, je například řešení Azure Active Directory od Microsoftu:

Obrázek 6: Technické principy Microsoft Authenticator



Zdroj: Microsoft: https://learn.microsoft.com/en-us/answers/questions/2242359/request-an-explanation-of-the-technical-principles

1. Uživatel se chce přihlásit do zařízení / služby.
2. Vygeneruje se session, tedy dočasné spojení mezi klientem a serverem, které je jedinečné pro každé přihlášení a po jeho ukončení (odhlášení, vypršení časového intervalu, apod.) je ukončeno a nemůže být obnoveno, ale musí se vytvořit nové spojení a tedy i proběhnout znovu přihlášení uživatele.
3. Odesílá se notifikace do Authenticatoru, tedy do externí aplikace, nejčastěji v mobilním telefonu.
4. Aplikace vyzve uživatele pro autorizaci požadavku (PIN, otisk prstu, sken očí apod.).
5. Externí aplikace provede ověření zadaných údajů.
6. Po ověření odešle externí aplikace notifikaci podepsanou privátním klíčem zpět autentizační službě.
7. Validační služby ověří kryptografický podpis.
8. Uživatel je ověřen a může využívat zařízení/službu.

Nutno podotknout, že než je možné využívat externí autentizátor (Authenticator), jak je například popsáno výše, musí mít uživatel vytvořen účet v autentizační službě (v tomto případě v Azure Active Directory) a mít již nainstalován autentizátor v mobilním zařízení (nejčastěji zařízení se systémem Android nebo Apple iOS systémem). K tomu je potřeba vygenerovat dva privátní klíče, které se poté používají pro komunikaci mezi službami. Jeden klíč je uložen v autentizační službě a druhý v autentizátoru.

Teprve poté, co má uživatel založen účet a nastavená všechna zařízení, se může přihlašovat a využívat zařízení nebo služby, které jsou mu přiděleny.

Pro taková vícefaktorová ověřování uživatele se používají kombinace informací z více zdrojů (minimálně ze dvou):

- něco, co uživatel má - typicky nějaké snadno přenositelné zařízení, jako je hardwarový token, mobilní telefon a autentizátorem, čipová karta, speciální hodinky nebo chytrý prsten
- něco, co uživatel zná - PIN, heslo, odpověď na otázku,
- něco, co je součástí uživatele - otisk prstu, rozeznání obličeje, DNA, sítnicový sken.

Při volbě způsobu přihlašování je potřeba pamatovat i na rizika s tím spojená. Například při biometrickém přihlašování pomocí otisku prstu by měla být možnost volby z více prstů. Pokud by zaměstnanec nešťastnou náhodou měl ruku v sádře právě s prstem potřebným pro autentizaci, tak se jednoduše nepřihlásí, pokud by neměl jinou možnost.

Jak je popsáno výše, v běžném informačním systému si podniky zachovávají vlastní systém přihlašování a správu nad ním. Je zde několik oblastí, kde je velký potenciál pro využití elektronické identifikace dle eIDAS a to z velmi dobrých důvodů:

- úspora času,
- úspora peněz,
- úspora lidských zdrojů,
- spolehlivost informací.

Služby vytvářející důvěru mohou nahradit některé procesy spojené s životním cyklem zaměstnance od jeho přijetí až po ukončení spolupráce.

Pro vnitřní potřebu informačního systému podniku začíná identifikace potencionálního zaměstnance (či jiného pracovníka/spolupracovníka) již při prvním kontaktu. Ještě než je přijat, prochází zaměstnanec dotazováním, například zda jeho vzdělání a získané zkušenosti odpovídají pozici, o kterou se uchází. Osobní oddělení vyhodnocuje životopisy a reference na základě údajů, které o sobě žadatel o práci uvedl. Ne vždy však ověřuje, zda uvedené informace jsou pravdivé.

Zde je ideální příležitost využít služeb vytvářejících důvěru dle eIDAS a za využití elektronické identity, kdy uchazeč zpřístupní vybrané údaje pro potřeby podniku, získat ověřené

informace o uchazeči o práci. Podnikový systém takové poskytnuté informace může automaticky načíst a vyhodnotit.

V průběhu pracovního vztahu jsou další možnosti využití elektronické identity a to jak ve vztahu zaměstnanec - zaměstnavatel, tak naopak zaměstnavatel - zaměstnanec.

Zaměstnanec si může udělat certifikovaný kurz, který může zviditelnit i pro zaměstnavatele a ten potom může lépe využít potenciál zaměstnance a nabídnout mu jinou pracovní pozici. Zároveň mohou být vzdělávání a certifikované kurzy nástrojem podniku pro odměňování zaměstnanců a tím přispívat k jejich větší produktivitě a spokojenosti.

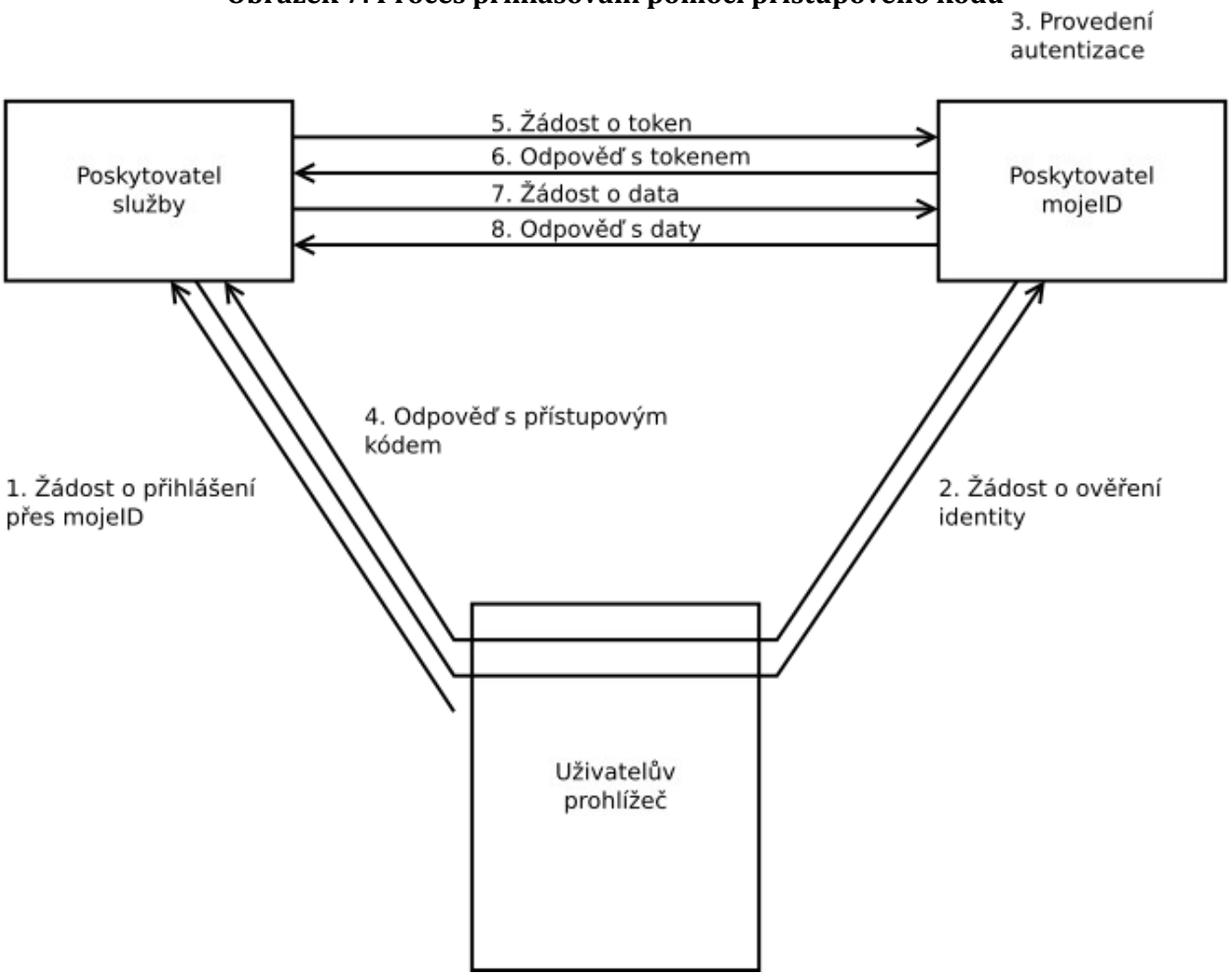
Ukončení pracovního vztahu může doprovázet referenční hodnocení spolupráce v podobě elektronicky podepsaného dokumentu, kterým zaměstnanec může prokazovat získané zkušenosti.

1.5.2 Podnikové systémy a vnější uživatelé

Uživatelé vnějších (nejen) webových služeb jsou označování jako klienti nebo zákazníci. Mají zpravidla omezený přístup k službám a dokumentům podniku. Jejich identifikace se zakládá často na dobrovolnosti - do eshopu zákazník zadá jméno, adresu, email a kontaktní telefon. Autentizace proběhne většinou pouze potvrzením přijatého emailu, případně kontrolní SMS. Pro tyto případy je využití identifikačních prostředků dle eIDAS mnohem bezpečnější, což dokazuje i neustále se rozšiřující počet služeb, které takové přihlášení umožňují. Za pomocí elektronické identity je už nyní možné se přihlásit do knihoven na hostingové služby, eshopy nebo datová úložiště.

Příkladem může být přihlašování pomocí elektronického identifikačního prostředku MojeID, spravovaného CZ.NIC, z.s.p.o. (viz. výše seznam elektronických identifikačních prostředků a kvalifikovaných správců):

Obrázek 7: Proces přihlašování pomocí přístupového kódu



Zdroj: https://www.mojeid.cz/dokumentace/singlehtml/

Před použitím protokolu OpenID Connect je nutné registrovat svého klienta na serverech MojeID.

1. **Žádost o přihlášení přes MojeID** – uživatel klikne na ikonu „Přihlásit přes MojeID“.
2. **Žádost o ověření identity** – poskytovatel služeb vytvoří žádost o ověření identity a tu nepřímo skrze přesměrování uživatelova prohlížeče odešle na koncový bod poskytovatele mojeID, kde se uživatel autentizuje.
3. **Provedení autentizace** – uživatel se na přihlašovací stránce MojeID přihlásí pomocí některé z přihlašovacích metod a tím je jeho identita ověřena. V současnosti je podporováno heslo, digitální certifikát, jednorázové heslo a bezpečnostní token.
4. **Odpověď s přístupovým kódem** – po přihlášení a potvrzení je uživatel přesměrován zpět na stránky poskytovatele služeb a prostřednictvím svého prohlížeče tak předá odpověď ze serverů MojeID s přístupovým kódem.
5. **Žádost o token** – poskytovatel služeb vytvoří žádost o token, ve kterém použije získaný přístupový kód, a odešle ji na koncový bod `poskytovatele mojeID pro získání tokenu`.
6. **Odpověď s tokenem** – poskytovatel služeb obdrží odpověď s přístupovým tokenem a ID tokenem.
7. **Žádost o data** – poskytovatel služeb vytvoří žádost o uživatelská data s využitím získaného přístupového tokenu a odešle ji na koncová bod `poskytovatele mojeID pro získání dat o uživateli.`
8. **Odpověď s daty** – poskytovatel služeb obdrží odpověď s daty uživatele.

Po získání ověřených údajů o zákazníkovi mu je umožněna služba nebo přístup ke zdrojům na základě přidělených práv.

1.5.3 Podnikové systémy a dokumenty

Správa dokumentů v podniku je řešena nejrůznějšími způsoby. Klasická papírová správa je už vesměs opuštěna a nahrazena efektivnější elektronickou správou, nazývanou DMS (Document management system). Hlavními úkoly takové správy dokumentů je:

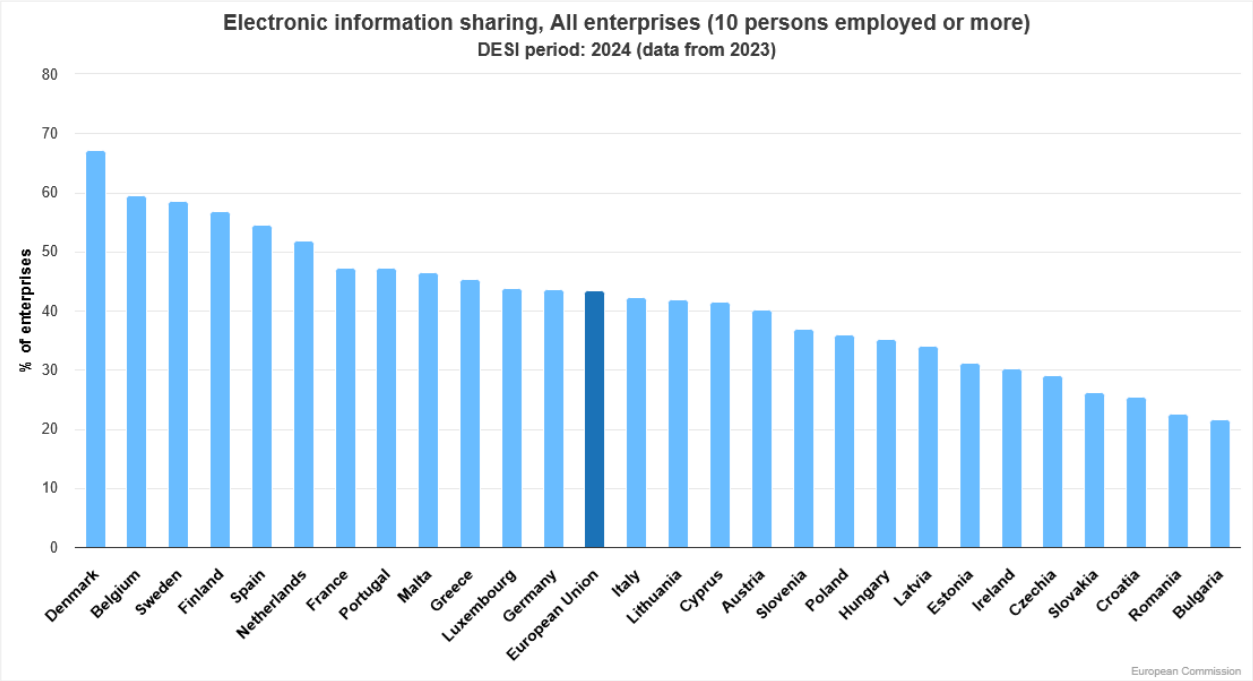
- vytváření dokumentů,
- ukládání dokumentů,
- zabezpečené přechovávání dokumentů,
- prezentace dokumentů podle přístupových práv,
- archivace dokumentů,
- skartace dokumentů.

Dokumentem je jakýkoliv písemný (papírový nebo elektronický), obrazový nebo zvukový záznam, který je používán v rámci podniku. A to jak pro vnitropodnikové účely (pracovní smlouvy, zápisy z porad, vnitřní nařízení apod.) nebo pro vnější uživatele (marketingové materiály, objednávky apod.).

Problematika uchovávání dokumentů a jejich lhůt pro skartaci je nad rámec této práce a je upravena mnoha právními předpisy (Zákon č. 499/2004 Sb., o archivnictví a spisové službě, Zákon č.235/2004, o dani z přidané hodnoty, Zákon č.563/1991 Sb., o účetnictví, a mnohé další). Liší se typem dokumentu, způsobem vzniku, jeho důvěrností nebo oblastí dalšího užití.

Vytváření dokumentů a jejich následná skartace je díky elektronizaci snadným úkolem. Větší problémy jsou s prezentací dokumentů, pokud ji nenásleduje i dostatečné rozlišení dle jednotlivých kategorií a podkategorií. Zejména větší společnosti, vydávající spoustu nařízení, prohlášení nebo informačních zpráv pro zaměstnance se stávají bludištěm stovek dokumentů a najít ten správný není snadné. To vede k zahlcení podnikových informačních systémů i uživatelů. Na druhou stranu důležité (praktické) dokumenty, jako zápisy z porad, bývají přístupné pouze vybranému okruhu zúčastněných. V tomto směru je ještě potřeba udělat mnoho práce, jak ve směru k přehlednosti prezentovaných dokumentů, tak k větší otevřenosti vůči zaměstnancům nebo zákazníkům. Nebude to snadný vývoj, protože jde i o změnu způsobu myšlení. Dokazuje to například následující graf, který ukazuje využití sdílených informací mezi jednotlivými oblastmi podniku (např. účetnictvím, marketingem, plánováním výroby):

Graf 1: Sdílení informací v rámci podniků (nad 10 zaměstnanců)



Zdroj: European Commission, https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_erp&breakdown=ent_all_xfin&unit=pc_ent&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE

Z grafu je patrné, že ve sdílení informací v podnicích nad 10 zaměstnanců výrazně zaostáváme za ostatními členskými státy EU.

1.5.4 Elektronický systém spisové služby (eSSL)

Spisovou službu jsem původně v této práci neměl v úmyslu popisovat, protože se často překrývá s dříve popsanou elekronickou správou dokumentů (DMS) nebo ji doplňuje o specifické služby.

Nicméně spisová služba se eIDAS úzce dotýká, protože na rozdíl od DMS podléhá mnoha zákonům a vyhláškám a je povinná pro tzv. "veřejnoprávní původce", což jsou mimo jiné organizační složky státu, státní příspěvkové organizace, vysoké školy, zdravotní pojišťovny, kraje, obce, právnické osoby zřízené zákonem a další.

Výkonem spisové služby se rozumí "zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti právních předchůdců. Zahrnuje řádný příjem, evidenci rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání a ukládání dokumentů a jejich vyřazování ve skartačním řízení, a to včetně kontroly těchto procesů" [11].

Veřejnoprávní původci mají povinnost od roku 2027 vykonávat spisovou služby atestovaným elektronickým systémem spisové služby.

Atestací eSSL se rozumí "posouzení souladu eSSL s požadavky zákona, vyhlášky a Národního standardu pro elektronické systémy spisové služby, který zveřejněný na stránkách Ministerstva

vnitra ČR. Soulad s jinými právními předpisy není v rámci atestace posuzován" [12].

Vzhledem k tomu, že se to týká jak velkých státních institucí, tak i nejmenších obcí, dá se očekávat, že na trhu bude k dispozici široká nabídka "spisovek", které budou jak variabilní pro použití, tak budou v sobě integrovat komunikaci se státní správou, datovými schránkami, elektronicky podepsanými dokumenty, přijímat eDoklady nebo akceptovat přicházející evropskou digitální peněženku.

Pro podniky tak bude snažší využít takové hotové řešení a adaptovat jej do svých interních systémů nebo na něm vystavět nové.

2 Praktická část - využívání služeb zvyšujících důvěru v podnikových systémech

Nařízení eIDAS si stanovilo nejen cíle a priority vůči občanům a státní správě, ale také ve směru k podnikatelské sféře a to ve třech základních oblastech:

- lepší uživatelská zkušenost - zvýšit důvěru zákazníků a tím i jejích spokojenost,
- zvýšení bezpečnosti a odpovědnosti - v úzké provázanosti se směrnicemi NIS a NIS 2,
- zvýšení efektivity - zvýšením automatizací procesů, zjednodušením prováděných úkonů a tím zvýšení výnosů ze služeb a produktů při zachování jejich kvality.

V této části se budu věnovat několika praktickým aplikacím, které jsou spojeny s nařízením eIDAS, a které jsem přímo využíval jako klient nebo se podílel na jejich vývoji.

2.1 Praktická aplikace - realizace zdravotních prohlídek zaměstnanců

Jde o projekt, kterého jsem se účastnil jako vývojář. Na počátku byl požadavek HR oddělení větší firmy na automatické upozorňování na blížící se povinné zdravotní prohlídky zaměstnanců s možností rezervovat konkrétní čas prohlídky ve zdravotnickém zařízení, komunikace s tímto zařízením a přijetím výsledné zdravotní zprávy v elektronické formě k dalšímu vnitropodnikovému zpracování. V tomto projektu byly využity podpisové zařízení Signotec Signature pad umožňující uložení certifikátů. S jejich využitím se ze zdravotního zařízení se do společnosti odesílaly elektronicky podepsané PDF dokumenty.

2.1.1 Zadání

Zadání z HR oddělení znělo na vytvoření aplikace pro plánování a evidenci zdravotních prohlídek pro zaměstnance tak, aby vyhovělo požadavkům legislativy, bezpečnosti dat (GDPR) a snížilo zatížení zaměstnanců HR oddělení.

Hlavní funkční požadavky:

- vytvořit aplikaci, která bude hlídat a upozorňovat na termíny zdravotních prohlídek zaměstnanců v závislosti na jejich pracovním zařazení, náplni práce a dalších atributů ovlivňujících rozsah a periodu zdravotní prohlídky,
- vytvořit uživatelské rozhraní pro personální oddělení s možností (pře-)rezervace zdravotních prohlídek pro všechny zaměstnance, upozorněními na blížící se termíny pro prohlídky vyplývající ze zákona nebo vyhlášek, možností prohlížet záznamy výsledků prohlídek nebo je mazat po uplynutí zákonné lhůty pro uchovávání,

- vytvořit uživatelské rozhraní pro nadřízené zaměstnanců v rámci intranetu s upozorněními na blížící se povinné prohlídky podřízených i jich samotných,
- vytvořit uživatelské rozhraní pro zaměstnance, kteří si mohou zdravotní prohlídku naplánovat v tzv. kioscích - počítačových terminálech v areálu společnosti, na kterých běžel firemní intranet,
- vytvořit uživatelské rozhraní pro personál zdravotnických zařízení, kde je možné vidět kalendář s naplánovanými prohlídkami, vyvolat si konkrétní předpřipravené formuláře pro konkrétní prohlídku s možností doplnění dalších záznamů,
- pro zdravotní zařízení umožnit v aplikaci změnu pracovní doby, plánování dočasného uzavření ordinace (dovolené, nemoc), možnost (pře-)rezervovat plánované prohlídky (navázané na notifikace pro personální oddělení společnosti, které změny schvaluje),
- pro zdravotní zařízení připravit podpisový HW + SW, aby mohly být do společnosti odesílány zdravotní zprávy podepsané jak lékařem, tak zaměstnancem,
- připravit adaptabilní formuláře prohlídek "na míru" tak, aby každý formulář odpovídal požadovanému rozsahu zdravotní prohlídky i s definovanými riziky pracovní pozice daného zaměstnance,
- pro zdravotní zařízení i personální oddělení umožnit tisk výsledků zdravotní prohlídky pro případ, že to bude zaměstnanec požadovat,
- zajistit přijímání elektronicky podepsaných dokumentů a hashů těchto dokumentů a obojí bezpečně ukládat,
- zajistit zpřístupnění zdravotních prohlídek odpovědným pracovníkům v souladu s GDPR,
- zajistit zobrazení výsledků zdravotních prohlídek ve stejné podobě, jako byla dosud a nebo jen s minimálními (nutnými) změnami.

2.1.2 Technické řešení

Vývojové prostředí: byl zvolen NETTE framework pro svou srozumitelnost, přehlednost a snadné začlenění nových programátorů do projektu.

Verzování projektu: vlastní GitLab pro verzování kódů a plánování sprintů.

Databáze: MS SQL databáze, pro svou robustnost a podporu transakcí.

Datové úložiště: vlastní datové úložiště (nejen) pro podepsané PDF dokumenty. Dostupné pouze interně v rámci společnosti.

Hardware pro podepisování: Signotec Signature pad připojený pomocí USB portu ke stolnímu počítači.

Certifikáty po podepisování: certifikáty vydané První certifikační autoritou, uložené v podpisovém hardware.

2.1.3 Implementace projektu

Vývoj probíhal agilním způsobem, jednotlivé funkcionality byly rozděleny do sprintů aprůběžně se testovaly. Každá dokončená funkcionalita byla představena zákazníkovi, který mohl hned reagovat a vznést požadavky na dodatečné úpravy. Komunikace se zákazníkem se ukázala jako klíčová pro akceptaci výsledné aplikace.

2.1.4 Spuštění aplikace a školení

Aplikace byla spouštěna po etapách. Nejprve byl na testovacích datech proškolen personál zdravotnických zařízení - jak sester, tak doktorů a doktorek. Školení probíhalo po každém dodání větší funkcionality a trvalo přibližně 14 měsíců. Vlastní vývoj trval asi 20 měsíců. Vývoj, testování a školení probíhalo současně.

Spuštění aplikace do ostrého provozu proběhlo až po dokončení všech akceptance testů.

2.1.5 Zhodnocení aplikace pro kontrolu zdravotních prohlídek

Šlo o úspěšnou aplikaci, přestože se zpočátku potýkala s technickými a personálními problémy. Zvláště u personálu zdravotnických zařízení byly nutné osobní konzultace a trpělivé vysvětlování nejen konkrétní aplikace, ale i běžné práce s osobním počítačem, včetně nástrah aktualizací systému Windows.

Největším dosaženým přínosem bylo odpadnutí papírových lékařských zpráv a snížení administrativní zátěže personálu na personálním oddělení.

V tomto projektu se podařilo úspěšně využít nástroje vytvořené na základě eIDAS směrnice pro praktické komerční použití.

2.2 Praktická aplikace - využívání elektronických podpisů

Pro účely testování jsem si zřídil podpisový certifikát vydaný společností První certifikační autorita, a.s. a pokusil se podepsat některé dokumenty.

2.2.1 Zadání

Vyzkoušet práci s podpisovým certifikátem a zjistit, jaká je náročnost instalace a zda jsou nutné technické IT znalosti pro použití podpisového certifikátu.

2.2.2 Technické řešení

HW: Osobní počítač s procesorem i5, 16 GB RAM, 512 GB HDD, připojený na internet.

SW: Operační systém Windows 7, Libre Office, Adobe Reader.

Certifikát: kvalifikovaný certifikát vydaný První certifikační autoritou, a.s. pro elektronické podepisován.

2.2.3 Implementace

Instalace proběhla dle návodu k certifikátu a to uložením do úložiště Windows a úpravou předvoleb v nastavení Adobe Reader přenačtením AATL seznamu (Adobe Approved Trust list), což je seznam důvěryhodných certifikátů vydaných certifikačními autoritami, které produkty Adobe považují za důvěryhodné.

Následně bylo ještě potřeba aktualizovat seznam kořenových certifikátů z databáze EUTL, což je důvěryhodný veřejný seznam Evropské unie aktivních i starších důvěryhodných poskytovatelů služeb, kteří mají akreditaci a poskytují digitální certifikáty, pečetě, časová razítka používaná pro vytvoření podpisů, které odpovídají dle eIDAS vlastnoručnímu podpisu. Jsou to podpisy, které jsou automaticky uznávány v přeshraničních transakcích.

2.2.4 Spuštění

Byl učiněn pokus podepsat PDF dokument, avšak s negativním výsledkem. Byly vyzkoušeny různé varianty, jak v programu Adobe Reader, tak Libre Office, ale bez kýženého výsledku.

U podepsaného dokumentu byla stále zobrazena chybová hláška: "The selected certificate has errors: Invalid policy constraint."

Poté byla kontaktována zákaznická podpora, která při prvním dotazu odpověděla návodem, který ovšem skončil stejným výsledkem.

Po druhém kontaktu bylo doporučeno smazat konkrétní soubor Adobe Reader a kořenové certifikáty přenačíst v opačném pořadí - tedy nejdříve aktualizovat z EUTL databáze a až poté z AATL. Toto řešení se již ukázalo jako správné a od té doby certifikát fungoval správně.

2.2.5 Zhodnocení používání podpisového certifikátu

Na základě vlastních zkušeností z instalace podpisového certifikátu mohu konstatovat, že jde o činnost, kde jsou potřeba alespoň základní znalosti o způsobu ukládání souborů v operačním systému počítače a je také potřeba znalost základních nastavení programů.

Zároveň tato zkušenost ukazuje, že je důležité investovat do vzdělání pracovníků technické podpory a kontrolovat a aktualizovat návody pro zákazníky.

Další zkušeností bylo zjištění, že tento elektronický prostředek (podpisový certifikát) není nejvhodnější pro běžné osobní použití v komunikaci s institucemi. Tento prostředek jsem využil pouze dvakrát a po jeho vypršení (1 rok) již nebyl obnoven (zaplaceno prodloužení).

Jeho původní předpokládané využití jsem později nahradil jiným identifikačním prostředkem a sice MojeID + Datovou schránkou.

Přes na první pohled nevhodnost elektronického podpisu pro běžného občana, který nemá potřebu často podepisovat elektronické dokumenty a nahraditelnost elektronického podpisu vůči státní správě datovými schránkami, má elektronický podpis své nezastupitelné místo a to především

v automatizovaných systémech, které využívají pro svou komunikaci podnikové systémy. Ty často mezi sebou navzájem komunikují pomocí zpráv, které jsou zabezpečené elektronickým podpisem.

Je dobré rovněž zmínit, že přicházející **Evropská peněženka digitální identity** má v sobě zahrnovat i bezplatný způsob podepisování pro neprofesionální účely kvalifikovaným podpisem. Když pomineme, že prozatím není vyjasněn pojem "neprofesionální účely", tak z uvedeného vyplývá, že občan bude mít k dispozici elektronický podpis, který bude prokazovat jeho vůli a nebude omezen platností, jako to je v současnosti u komerčně nabízených kvalifikovaných podpisů.

2.3 Praktická aplikace - Datové schránky

Pro účely podnikání, komunikaci s úřady a doručování písemností jsem si zřídil dvě datové schránky. Jednu jako soukromá osoba a druhou jako podnikatel.

2.3.1 Zadání

Usnadnit komunikaci s úřady, především s Finančním úřadem, a mít jistotu, že písemnosti od úřadů budou doručeny a přečteny aniž by bylo nutné cestovat do místa bydliště.

2.3.2 Technické řešení

HW: libovolný počítač / notebook

SW: Systém Windows s aktualizacemi a webovým prohlížečem

Přístup: přístupové údaje do datových schránek (jméno + heslo)

2.3.3 Implementace

Založení datové schránky proběhlo pomocí kontaktního místa Czech POINT na městském úřadu. Pro zřízení byl potřeba občanský průkaz a vyplnění žádosti. Po týdnu bylo možné vyzvednout přístupové údaje.

Žádná speciální implementace není potřeba.

2.3.4 Spuštění

Pro přihlášení do Datové schránky stačí aktualizovaný webový prohlížeč (např. Google Chrome, Mozilla Firefox nebo Microsoft Edge), přihlašovací jméno a heslo.

Další možností přihlášení namísto jména a hesla je pomocí elektronické identifikace.

2.3.5 Zhodnocení používání Datové schránky

Zprovoznění Datových schránek byl velký posun a zjednodušení komunikace se státní správou a úřady. Zvláště v době, kdy jsem se častěji stěhoval a neměl stálou adresu bylo obtížné cestovat do trvalého bydliště a zde vyzvedávat písemnosti určené do vlastních rukou. Možnost pomocí Datových schránek online vyplňovat formuláře a podání pro úřady v kombinaci se vzrůstající nespolehlivost služeb České pošty byly hlavními důvody přechodu na komunikaci s úřady pomocí

Datových schránek.

Tato služba se osvědčila a je pravidelně využívána.

3 Zhodnocení přínosů a rizik nařízení eIDAS v podnikových systémech

Možná si málo uvědomujeme, že jsme během dvou generací přešli ze společnosti "analogové", která se spoléhala na osvědčený a léty prověřený osobní kontakt s orazítkovanými papíry na společnost "digitální", kde část svého profesního i osobního života žijeme ve virtuálním světě digitálních technologií. Tyto dva světy se čím dál tím více prolínají, omezují a doplňují.

3.1 eIDAS 2 z pohledu přínosů pro podniková řešení

Některé přínosy byly představeny v teoretické části i v praktických ukázkách užití služeb, které pomohla na trh uvést implementace nařízení eIDAS. Většina, ne-li všechny služby vytvářející důvěru dle eIDAS / eIDAS 2, jsou aplikovatelné nejen vůči státní správě, ale i v rámci fungování podniku. Podniky profitují z toho, že nemusí vymýšlet vlastní řešení. Mohou využívat standardy a služby, které se implementují ve státní správě, jsou bezpečné a přijímané jak v rámci České republiky, tak v přeshraniční komunikaci.

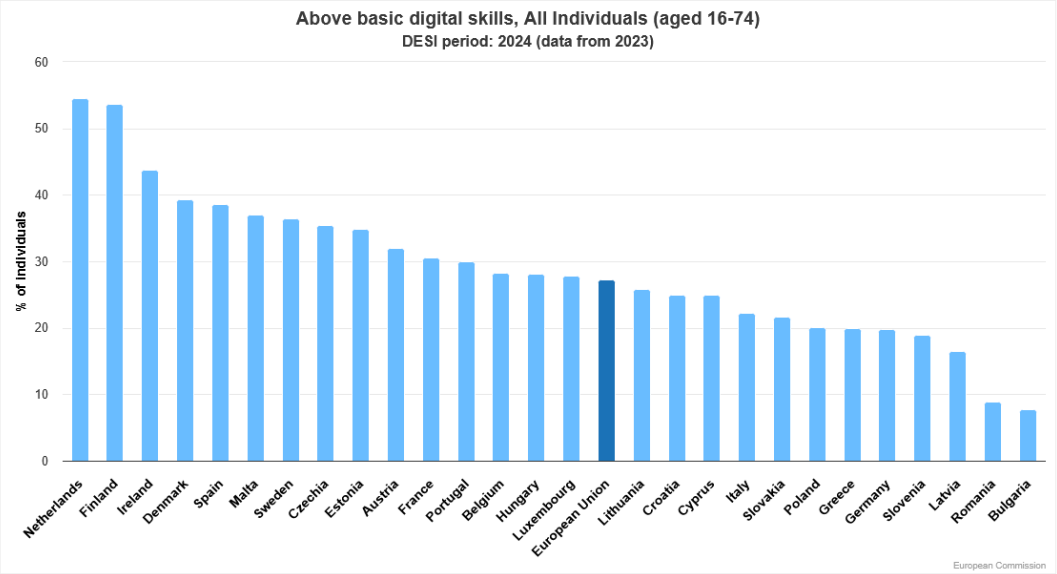
Hlavní přínosy:

- snížení administrativní zátěže zaměstnanců, hlavně v personálním oddělení,
- získání nástroje pro vzdělávání pracovníků a zvýšení jejich spokojenosti,
- zvýšení digitální gramotnosti zaměstnanců,
- snadnější nastavování podnikových cílů, jejich dosahování a kontrolu dosažené úrovně,
- zjednodušení komunikace s úřady, obchodními partnery i koncovými zákazníky,
- zvýšení efektivity a úspor lidských a jiných zdrojů,
- zvýšení důvěryhodnosti služeb.

Jedním z velkých přínosů eIDAS a navazujících služeb vytvářejících důvěru je zvyšování digitální gramotnosti, což je už nyní důležitý aspekt jak profesního, tak soukromého života zaměstnanců.

V rámci EU na tom není Česká republika špatně, o čemž svědčí i počet obyvatel, kteří mají v porovnání s ostatními zeměmi EU nadprůměrné digitální znalosti ve větším zastoupení, než je průměr zemí EU:

Graf 2: Nadprůměrné digitální dovednosti (obyvatelé 16-74 let)



Zdroj: European Commission, https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dsk_ab&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE

Jak je vidět na grafu č.2, je na trhu práce pro české firmy (a úřady) dostatek pracovníků s nadprůměrnými digitálními znalostmi.

3.2 eIDAS 2 z pohledu rizik v podnikových řešeních

Rizika pro podnikové systémy bych rozdělil do tří oblastí:

- Hardwarová rizika.
- Softwarová rizika.
- Lidská rizika.

3.2.1 Hardwarová rizika

Mezi tato rizika patří chyby v IT infrastruktuře vnitřní sítě podniku a jejího napojení na vnější svět - internet. Je potřeba dodržovat zásady, jako je provoz vnitropodnikových aplikací na fyzicky oddělených serverech od aplikací určených pro vnější uživatele nebo používání hardwarových komponent spolehlivých dodavatelů (zranitelnost firmware těchto zařízení). Fyzická zranitelnost zařízení by měla být chráněna proti neoprávněnému přístupu. Vyřazená zařízení je nutné bezpečně zlikvidovat, protože mohou obsahovat citlivá data.

3.2.2 Softwarová rizika

Softwarová rizika se postupně s dalším rozšiřováním digitálních technologií rovněž rozšiřují. Mezi nejčastější rizika patří

- **Zastaralý a neaktualizovaný software** - neaktualizovaný software a firmware zařízení je náchylný na chyby a více zranitelný. Jde o velké bezpečnostní riziko.
- **Platnost podpisových certifikátů** (obvykle 1 rok) - služba, která se spoléhá na platný certifikát bude nedostupná, jakmile vyprší stávající podpisový certifikát. To je nebezpečné zejména u automatizovaných systémů, kde je výměna datových zpráv ve stovkách nebo tisících zpráv za den. Přesto, že se většina služeb automatizuje, vydávání a instalace podpisového certifikátu je zatím doménou IT oddělení a tedy závisí na lidech, kteří certifikáty spravují a instalují.
- **Chybějící monitoring sítě** - monitoring sítě je nepřetržité sledování a vyhodnocování stavu a zatížení sítě. Je důležitý pro prevenci. Jeho absence může znamenat kolaps z důvodů přetížení zdrojů nebo nezaznamenání potenciálně nebezpečných procesů.
- **Nedostatečné zálohování dat** - data jsou základem fungování veškerých technologií. Jejich pravidelné zálohování a občasné testy obnovy dat z těchto záloh by měly být samozřejmostí. Simulace výpadku serveru, kde běží databáze nebo aplikace může ukázat na mezery v zálohování a obnově dat.
- **Nedostatečná dokumentace aplikací** - spoléhání se na klíčové pracovníky je velkým rizikem v případě, kdy z podniku tito lidé odejdou nebo jsou nenadále indisponováni. Nositelem informací jak systém má fungovat a jak skutečně funguje by měla být dokumentace a nikoliv lidé.

3.2.3 Lidská rizika

Oblíbené úsloví nejen korporátních společností: "Naše společnost, to jsou naši lidé" je zcela na místě. I přes maximální hardwarové a softwarové zabezpečení, pokud lidé nejsou dostatečně vzděláváni, školeni a motivováni pro kvalitní práci, tak zavedení elektronických služeb bude zdlouhavé, nákladné nebo zcela nemožné. Jak je již zmíněno výše, v kapitole 3.2.2 Softwarová rizika, digitalizace s sebou přináší i lidskou účast na procesech nezbytných pro fungování digitálních technologií.

Přechod od analogové společnosti k digitální, kde dříve jsme se spoléhali na osobní kontakt a některé věci byly "očividné", tedy máme v sobě zažité určité stereotypy, které nejsou aplikovatelné v digitálním světě. Díky vzdáleným přístupům nebo videokonferencemi se ztrácejí informace, které využíváme při osobním kontaktu a bývají ukazatelem spolehlivosti protistrany.

Nedostatečná znalost zaměstnanců, obchodních partnerů či zákazníků může vést k riziku, že při elektronické komunikaci nebudeme schopni zjistit skutečnou identitu, omezení nebo

i schopnosti druhé komunikující strany.

- **Odosobněný přístup** - při přílišném využívání vzdálené elektronické komunikace hrozí riziko, že se lidé, se kterými spolupracujeme/komunikujeme stanou pouhými čísly nebo symboly. Nejsou to ti lidé, kteří mají svá specifika založená na reálném základě, ale stanou se jakousi idealizovanou představou, kterou si vytvoříme na základě obdržených informací a vlastní zkušenosti, která však může být značně vzdálená od reality. Může tak snadno dojít k vzájemnému nepochopení a konfliktům, protože v elektronické komunikaci stále ještě chybí řeč těla, mimiky a gest.
- **Bílí koně** - termín bílý kůň se používá pro osoby, které vědomě nebo nevědomě pomáhají zločincům legalizovat výnosy z trestné činnosti. Tak, jako se bílí koně vyskytují u investic nebo bankovních účtů a jejich počty čím dále tím více rostou, tak se jistě vyskytnou i při získávání elektronických identit osob neznalých technologií nebo důvěřivých osob. Pokud by se do podniku přišel o práci databázového specialisty ucházet slepý člověk, pracovníka osobního oddělení napadne, že to není běžné a přinejmenším by důkladněji prověřil, zda disponuje schopnostmi a technikou, aby tuto práci zvládl. V elektronickém prostředí nám však podobné aspekty mohou uniknout z důvodu absence osobního kontaktu a za tímto člověkem se může skrývat potencionální útočník, který pouze zneužil něčí elektronickou identitu pro získání přístupů k firemním údajům.
- **Farmy bílých koní** - troufám si tvrdit, že brzy vzniknou i Farmy bílých koní - podobně, jako existují tzv. "trollí farmy". Tedy vzniknou organizované skupiny, které budou vytvářet a různými způsoby využívat / zneužívat větší množství získaných elektronických identit. Boj s takovými skupinami nebude jednoduchý, zvláště pokud se nepodaří do služeb kyberbezpečnosti získat kvalifikované odborníky.
- **Neúplné nebo nepravdivé informace** - zavádění digitální identity a s tím spojené elektronické potvrzování atributů nemusí mít dostatečnou vypovídací hodnotu. Například potvrzení, že osoba je starší 18 let ještě nemusí znamenat, že jde o osobu svéprávnou. Není jisté, jak se budou stavět služby digitální identity ke změnám, které uživatel (občan) nebude chtít sám o sobě změnit, když vezmeme v úvahu, že atributy elektronické identity mají být dostupná i offline a jejich správcem je právě uživatel. Dalším problematickým atributem se může ukázat pohlaví, kdy jsou snahy o nové kategorie. Navíc někteří jedinci si nejsou jisti, kam spadají a subjektivní pocity jsou v tomto směru nadřazeny fyziologickým (objektivním) znakům.
- **Nevyužití potenciálu zaměstnanců** - podniky a vůbec společnost je historicky spjatá s osobním přístupem, který zcela nevymizí, ale jistě se změní.
- **Odchod klíčových zaměstnanců** - souvisí se softwarovými riziky, kdy zaměstnanci jsou

nositeli důležitých informací. Je proto potřeba mít všechny důležité procesy v podniku popsány a zdokumentovány.

Z důvodů zvyšujícího se podílu externích zaměstnanců a práce z domova jsem přesvědčený, že by si podniky i úřady měly ponechat možnost "předvolat" zaměstnance (občana) k osobnímu jednání, ať již formou porady, meetingu nebo nějakého úkonu vyžadujícího osobní účast a to bez možnosti zastupování.

V oblasti vzdělávání zaměstnanců jsem se zatím nesetkal ani s jediným skutečně funkčním motivujícím systémem vzdělávání podpořeným mzdově či jinými jinými benefity. A to ani v menších ani ve velkých společnostech. Společnosti a podniky nabízejí širokou škálu školení a kurzů, ale chybí jim širší koncepce spojená s podnikovými plány, vizemi a hodnocením.

4 Závěr

Závěrem této práce je zjištění, že podniky sice čeká mnoho práce a změn, ale jsou buď na změny související se zaváděním eIDAS/eIDAS 2 již připraveny, nebo by ty změny neměly být omezující pro chod podniku.

Důvodem pro tato tvrzení je jednak velké množství praktických služeb vytvářejících důvěru, které jsou již nyní dostupné jak pro občany, tak pro podnikatele a jednak s tím související zvyšování digitální gramotnosti obyvatel, kde je Česká republika mezi předními státy EU.

Podniky na jednu stranu povinně zavádějí certifikované procesy, na druhou stranu z těchto povinných nařízení samy profitují, protože se mohou spolehnout na to, že stejné procesy a standardy zavádějí i jejich obchodní partneři, dodavatelé, zákazníci nebo úřady. Otevírají se tak nové možnosti bezpečné komunikace, které mají univerzální použití jak pro komunikaci s vnějším světem, tak pro vnitropodnikovou komunikaci. A nejde jen o komunikaci, ale také o celou správu informací a dokumentů důležitých pro chod společnosti.

Kritickými oblastmi, do kterých budou muset podniky více investovat jsou:

- zabezpečení
- lidské zdroje a jejich neustálé vzdělávání
- sledování legislativy a vyhovění jejím požadavkům
- větší sdílení interních informací

Závěrečná kapitola 3.2.3 Lidská rizika se mi během psaní rozrostla a jen tak potvrzuje fakt, že nejdůležitější pro úspěšný vstup podniků do digitální éry bude správný výběr kvalifikovaných lidí, investice do jejich neustálého vzdělávání a podpora jejich motivace pro vzdělávání.

Seznam použitých zdrojů

[1] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910

[2] Maslow, A.H.: Motivation and Personality. Harper & Row. New York 1954

[3] Pojetí e-identity z pohledu eGovernmentu. Dostupné z: https://archi.gov.cz/znalostni_baze:bezpecnost_identity

[4] Zákon č.250/2017 Sb. o elektronické identifikaci. Dostupný z: https://www.zakonyprolidi.cz/cs/2017-250

[5] Zákon č. 471/2022 Sb.,kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. Dostupné z: https://www.zakonyprolidi.cz/cs/2022-471

[6] Zákon č.1/2024 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. Dostupný z: https://www.zakonyprolidi.cz/cs/2024-1

[7] Počet datových scrhánek, DIA, Dostupné z: https://www.dia.gov.cz/cs/aktuality/1-7-2024-datove-schranky-slavi-15-let-pouziva-je-temer-5-milionu-uzivatelu

[8] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2024/1183, ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L_202401183

[9] Peněženka digitální identity EU. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=LEGISSUM:4812147

[10] Zákon ze dne 2025, o kybernetické bezpečnosti. Dostupné z: https://www.zakonyprolidi.cz/media2/file/2505/File75338.pdf

[11] Mendelova univerzita v Brně, Výkon spisové služby. Dostupné z: https://spisovasluzba.mendelu.cz/slovnik-pojmu

[12] Česká agentura pro standardizaci, Co je atestace elektronického systému spisové služby. Dostupné z: https://agenturacas.gov.cz/atestace/otazky-a-odpovedi/

Seznam obrázků

Seznam tabulek

Seznam grafů