VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

DIGITÁLNÍ IDENTITA

DIGITAL IDENTITY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Roman Dvořák

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Václav Zeman, Ph.D.

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Roman Dvořák ***ID:*** 208528

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Digitální identita

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je zmapovat současný stav využívání digitální identity osob ve státním i soukromém sektoru. Uveďte definice a vysvětlení pojmů systémů určených pro spolehlivou a bezpečnou identifikaci a popište technické prostředky, které tyto systémy zajišťují. Pozornost věnujte také bezpečnostním hrozbám, které s využitím digitální identity souvisí, proveďte jejich klasifikaci a uveďte možná opatření pro jejich eliminaci. Na základě rozboru navrhněte a realizujte webovou aplikaci, určenou pro výukové účely, který bude názorně demonstrovat fungování digitální identity.

DOPORUČENÁ LITERATURA:

[1] DOSTÁLEK, Libor. - VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Vyd. 2. Brno : Computer Press, 2010. 544 s. ISBN 978-80-251-2619-6.

[2] Zákon č. 297/2016 Sb. Zákonu o službách vytvářejících důvěru pro elektronické transakce. Sbírka zákonů České republiky. 2016, částka 115, s. 4466-4504. ISSN 1211-1244.

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 31.5.2022

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

Abstrakt

Tato bakalářská práce pojednává o tématu digitální identity osob, jejím cílem je popsat doprovodné technologie, které zajišťují používání této technologie a popis jejího stavu v různých sektorech.

Nejdříve je pozornost věnována základním pojmům popisujícím toto téma, následuje popis technických prostředků, které se využívají v této problematice. V další kapitole je kladen důraz na objasnění pojmů spojených s digitální identitou, vysvětlení struktury státního eGovernmentu, na který navazuje samotný popis e-identity. V této kapitole jsou rozvedeny identifikační prostředky, které jsou poskytovány státem jak ve smyslu e-identity, tak i ty, které ve smyslu e-identity využít nelze. Dále jsou společně s nimi uvedeny prostředky poskytované soukromoprávními kvalifikovanými poskytovateli. Jedna kapitola je také věnována Evropské digitální identitě, jejímu současnému stavu a uvedení příkladů států, které již využívaly digitální identitu před příchodem té z Evropské komise. Následující kapitola se věnuje bezpečnostním hrozbám, jejich výčtu a klasifikaci dle různých kritérií. Jsou v ní zmíněny typy kybernetických útoků, rizika spojená s využíváním digitální identity a také eliminace těchto útoků a hrozeb, jak z pohledu uživatelů, tak z pohledu poskytovatelů digitální identity.

V poslední části je popsána praktická část této práce, kterou je výuková webová aplikace, jež shrnuje výstupy bakalářské práce.

Klíčová slova

Autentizace, autorizace, BankID, bezpečnostní hrozba, digitální identita, eID, e-identita, eObčanka, Evropská digitální identita, identifikace, Identita občana, kybernetický útok.

Abstract

This bachelor‘s thesis deals with the personal digital identity area. Its goal is to describe accompanying technologies which ensure the course of this field. In addition, another goal is to describe the state of things in related sectors.

At first, attention is focused to basic concepts and terms describing this topic. The following section describes technologies which are used in area of digital and bank identity. In the next chapter, the emphasis is on explaining terms linked with digital identity and the structure of public eGovernment, followed by the description of e-identity. In this chapter, the identification means, provided by the government or commercial sector, are more explained. The same applies to the identification means provided by the government, but which are not considered as e-identity. Another chapter is dedicated to European Digital Identity and its current state, followed by mentioning states which have used digital identity before it was made mandatory by the regulation from European Commission. The following chapter explores security threats, their enumeration and classification according to different criteria. It mentions types of cyberattacks, threats associated with using digital identity and elimination of the threats. The point of view is taken from user’s experience, but from providers as well.

The last chapter describes the practical part which is an educational web application that summarizes the output of this bachelor’s thesis.

Keywords

Authentication, authorization, BankID, security threat, digital identity, eID, e-identity, eObčanka, European digital identity, identification, Identita občana, cyberattack.

Bibliografická citace

DVOŘÁK, Roman. *Digitální identita* [online]. Brno, 2022 [cit. 2022-05-31]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/141322. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Václav Zeman.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	Roman Dvořák
VUT ID studenta:	208528
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	Digitální identita

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne: 31. května 2022 ……..

podpis autora

Poděkování

Chci poděkovat vedoucímu mé bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D. za jeho trpělivost, odborné vedení, ochotu a rady, které mi poskytnul k mé bakalářské práci.

V Brně dne 31. května 2022 .....

podpis autora

Obsah

SEZNAM OBRÁZKŮ **11**

SEZNAM TABULEK **12**

ÚVOD **13**

1 ZÁKLADNÍ POJMY **14**

2 DIGITÁLNÍ IDENTITA OSOB **15**

2.1 IDENTITA 15
2.2 DIGITÁLNÍ IDENTITA 15
2.3 DIGITÁLNÍ STOPA 15
2.3.1 Aktivní digitální stopa *16*
2.3.2 Pasivní digitální stopa *16*
2.4 DIGITÁLNÍ IDENTITA VE STÁTNÍ SPRÁVĚ 16
2.4.1 Národní identitní autorita *16*
2.4.2 Národní bod pro identifikaci a autentizaci *17*
2.4.3 Národní uzel eIDAS *17*
2.4.4 Správa základních registrů *17*
2.4.5 Kvalifikovaný systém a správce *17*
2.4.6 Portál občana *18*
2.4.7 Přínosy eID *19*
2.4.8 Úrovně záruky *19*

3 E-IDENTITA (IDENTITA OBČANA) **20**

3.1 IDENTIFIKAČNÍ PROSTŘEDKY NABÍZENÉ STÁTEM 20
3.1.1 Elektronický občanský průkaz s čipem *20*
3.1.2 Mobilní klíč eGovernmentu *22*
3.1.3 NIA ID *23*
3.1.4 International ID Gateway (IIG) *23*
3.2 IDENTIFIKAČNÍ PROSTŘEDKY, JEŽ NEJSOU E-IDENTITOU VE SMYSLU ZÁKONA 24
3.2.1 Datová schránka *24*
3.2.2 Kvalifikovaný certifikát *24*
3.2.3 Elektronický podpis *24*
3.2.4 Daňová informační schránka (DIS+) *25*
3.3 IDENTIFIKAČNÍ PROSTŘEDKY NABÍZENÉ SOUKROMOPRÁVNÍMI KVALIFIKOVANÝMI POSKYTOVATELI 25
3.3.1 BankID *25*
3.3.2 Čipová karta Starcos *26*
3.3.3 MojeID *26*
3.4 VYUŽITÍ V ČÍSLECH 26

3.5 BANKOVNÍ IDENTITA 28
3.5.1 Struktura BankID *28*
3.5.2 Pro uživatele *28*
3.5.3 Pro firmy *29*
3.5.4 Vývoj projektu *30*
4 EVROPSKÁ DIGITÁLNÍ IDENTITA 31
4.1 VYUŽITÍ EVROPSKÉ DIGITÁLNÍ IDENTITY 31
4.2 EVROPSKÉ STÁTY POUŽÍVAJÍCÍ DIGITÁLNÍ IDENTITU 32
4.2.1 Estonsko *32*
4.2.2 Dánsko *33*
4.2.3 Německo *33*
4.2.4 Švédsko *34*
4.2.5 Belgie *34*
5 BEZPEČNOSTNÍ HROZBY 35
5.1 KLASIFIKACE KYBERNETICKÝCH HROZEB 35
5.2 ADVANCED PERSISTENT THREAT 36
5.3 THREAT HUNTING 36
5.4 RIZIKA TECHNOLOGIE DIGITÁLNÍ IDENTITY 37
5.4.1 Únik citlivých osobních údajů *37*
5.4.2 Krádež identity *37*
5.4.3 Kyberšikana *38*
5.4.4 Centralizace osobních údajů *38*
5.5 ÚTOKY NA POSKYTOVATELE SLUŽBY 39
5.5.1 Ransomware *39*
5.5.2 Zero-day exploit *39*
5.5.3 Denial of Service (DoS) *40*
5.5.4 Příklad zranitelnosti estonských eID karet *40*
5.6 ÚTOKY NA UŽIVATELE SLUŽBY 41
5.6.1 Sociální inženýrství *41*
5.6.2 Počítačový virus *42*
5.6.3 Počítačový červ *42*
5.6.4 Spyware *42*
5.6.5 Keylogger *42*
5.6.6 Man-in-the-Middle *43*
5.7 ELIMINACE HROZEB Z POHLEDU UŽIVATELE SLUŽBY 43
5.8 ELIMINACE HROZEB Z POHLEDU POSKYTOVATELE SLUŽBY 44
6 TECHNICKÉ PROSTŘEDKY 45
6.1 VÍCEFÁZOVÉ OVĚŘENÍ 45

6.1.1 Typy autentizace *45*
6.2 X.509 46
6.3 AUTENTIZAČNÍ/AUTORIZAČNÍ PROTOKOLY 47
6.3.1 OpenID Connect *47*
6.3.2 OAuth 2.0 ..... *47*
6.3.3 Security Assertion Markup Language (SAML) *48*
6.3.4 Porovnání protokolů *48*
6.4 BANKID 48
6.4.1 Bezpečnost *50*
6.4.2 Kryptografické algoritmy *50*
6.4.3 Možné technické vektory útoku na BankID *50*
6.5 PROSTŘEDKY PRO BEZPEČNOU AUTENTIZACI 51
6.5.1 Softwarový klíč *51*
6.5.2 Heslo *51*
6.5.3 Certifikát *51*
6.5.4 Jednorázové heslo *52*
6.5.5 Hardwarový token *52*
7 WEBOVÁ APLIKACE 53
ZÁVĚR 54
LITERATURA 56
SEZNAM SYMBOLŮ A ZKRATEK 62

SEZNAM OBRÁZKŮ

Obrázek 2.1: Schéma přihlášení do Portálu občana 18
Obrázek 3.1: Schéma využití kódů eObčanky [15] 22
Obrázek 3.2: Identifikační proces při využití různých státních id. prostředků [8] 23
Obrázek 3.3: Rozdělení Bankovní identity [25] 28
Obrázek 5.1: Oblasti ovlivněné zranitelnou knihovnou RSALib [50] 40
Obrázek 6.1: Schéma komunikace při ověřování koncového zákazníka 49

SEZNAM TABULEK

Tabulka 3.1: Souhrn identifikačních prostředků pro eID ve smyslu zákona.....27
Tabulka 3.2: Souhrn bank provozujících BankID.....30

Úvod

Za celou dobu lidského pokolení si lidstvo snaží ulehčit svoji práci. Lze zmínit vynález kola nebo mnohem pozdější vynález parního stroje. Stejně jako u těchto vynálezů je snahou jednotné digitální identity ulehčit lidem námahu, kterou musí vynakládat. S rozmachem informačních a komunikačních technologií vyvstaly nové potíže, které však mají svou analogii v dřívějších „off-line dobách“. A to, že se vždy objeví zlí lidé, kteří chtějí něco zničit nebo ukrást. Proto se po začátcích éry počítačové, kdy se na bezpečnost těchto systémů nebralo tolik zřetel, objevila potřeba je zabezpečit před právě těmi zlými lidmi, kterých pochopitelně rostlo s neustálým rozšiřováním povědomí a znalostí o těchto systémech.

Z toho logicky vyplývá, že jednou možností, jak zabezpečit nějaké IT zařízení, bylo zavedení uživatelských účtů, kde je potřeba znát své uživatelské jméno a tajné heslo, které zná jen dotyčná osoba. Ale s postupujícím časem, kdy se velká část lidských životů v různé míře propojila s ICT systémy, mnohonásobně vzrostlo množství přihlašování do nejrůznějších služeb, kdy uživatel musí znát své autentizační údaje nebo musí být ověřována jeho identita, to vše v rámci zachovávání bezpečnosti. Naneštěstí jsou bezpečnost a uživatelská přívětivost nepřímo úměrné. To znamená, že čím je úroveň zabezpečení vyšší, tím méně je příjemné pro uživatele běžné používání služby.

Proto je účelem jednotné identifikační metody, která využívá digitální identity, usnadnit pro člověka jeho každodenní fungování v běžném životě. Z pohledu státu je velkým benefitem zjednodušení byrokratických procedur, které musí být vykonány a také ušetření nemalého množství vynaložených nákladů. V důsledku je digitální identita hmatatelným zlepšením pro život občana i pro chod státních institucí, které je již na dosah.

Tudíž si myslím, že si tohle téma zasluhuje pozornost kvůli své aktuálnosti a přínosu. Nejprve chci uvést základní pojmy, které se vztahují k digitální identitě a jejímu dnešnímu využití, aby mohl čtenář lépe pochopit kontext digitální či bankovní identity. V návaznosti na to bude uvedena digitální identita, její popis, její architektura ve státní správě, identifikační prostředky s ní spojené, na to v návaznosti bude zmíněna e-identita a prostředky pro identifikaci využívané i v komerčním sektoru. Dále chci zmínit nadcházející evropskou digitální identitu a uvést příklady evropských států, které již mají implementovány národní digitální identity a srovnat je s českým přístupem. V neposlední řadě je mým cílem vyjmenovat hrozby a rizika spojená s digitální identitou. Následovat bude popis technických prostředků, které stojí v pozadí fungování digitální a bankovní identity. Posledním cílem mé bakalářské práce je vypracovat webovou aplikaci, jejímž účelem je seznámit uživatele stručnou, jasnou a výstižnou formou s touto problematikou, uvést souhrnné informace na jednom místě, zmínit výhody a nevýhody používání bankovní identity, aby si každá osoba mohla udělat svůj vlastní obrázek.

1 ZÁKLADNÍ POJMY

Identifikace – proces pro určování identity jedince, kupříkladu hledání dané identity v databázi, zpravidla předchází procesu autentizace.
Autentizace – proces, při kterém je ověřována jedincem prohlašovaná totožnost vůči jeho skutečné identitě, po níž většinou následuje proces autorizace.
Autorizace – proces kontroly, při kterém jsou již autentizované osobě kontrolována její oprávnění a následně jsou udělena povolení pro vykonání dané operace. Pojmy autentizace a autorizace jsou často navzájem zaměňované.
Důvěrnost – cílem důvěrnosti je utajení dané informace před nežádoucími osobami nebo počítačovými systémy.
Integrita – cílem integrity je zajištění originality, nepozměnění a důvěryhodnosti dané informace.
Přístupnost – cílem přístupnosti je zajištění konzistence dostupnosti informací a udržování neustálého přístupu k nim.
Nepopiratelnost – cílem nepopiratelnosti je jednoznačné určení původu daných dat.
Metadata – data, která poskytují informace o jiných datech.
Hash (otisk) – jednocestná, výpočetně nenáročná funkce, která z libovolně dlouhého textu vytvoří otisk o pevně definované délce, který se využívá pro zaručení integrity dat.
Digitální podpis – nástroj pro zajištění pravosti digitálních dokumentů (integrity a nepopiratelnosti), je založen na principu asymetrické kryptografie, kdy odesílatel spočte otisk zprávy, ten podepíše svým soukromým klíčem, přiloží svůj certifikát a odešle; příjemce z přijaté zprávy spočítá otisk, ověří digitální podpis veřejným klíčem odesílatele a porovná hashe z dat a ověřeného digitálního podpisu, zdali se rovnají; jestli ano, tak je zpráva legitimní a naopak.
Digitální certifikát – dokument sloužící k ověření autenticity dat či držitele; v prostředí asymetrické kryptografie to je vydavatelem (certifikační autoritou) digitálně podepsaný veřejný klíč držitele, který obsahuje veřejně viditelný souhrn informací o držiteli, jež ho jednoznačně identifikují, a informace o vydavateli certifikátu [1].
„Soft“ certifikát – soubor, ve kterém je certifikát, je uložen na počítači uživatele v souborovém systému či v registrech [2].
„Hard“ certifikát – na rozdíl od „soft“ certifikátu je soubor uložen externě na USB tokenu či PKI kartě, je považován za bezpečnější variantu [2].
Certifikační autorita – nezávislá třetí strana, která podepisuje svým soukromým klíčem žadatelům jejich certifikáty a zaručuje pravost dat v jejich certifikátech; mezi certifikačními autoritami (CA) panuje hierarchický systém v podobě stromového grafu, kde vyšší autorita podepisuje certifikáty nižším CA, přičemž nejvyšší CA se nazývá kořenová certifikační autorita, která má kořenový (tzv. „self-signed“) certifikát a obecně se jí důvěřuje, že je její certifikát legitimní [1].

2 DIGITÁLNÍ IDENTITA OSOB

2.1 Identita

Bylo by vhodné nejprve definovat pojem identita, nehledě na jeho výskyt v digitálním prostředí. Identita člověka je utvářena jako souhrn znaků, vlastností či sociálních vztahů, jejichž kombinací je člověk jednoznačně identifikován. Z psychologického hlediska lze posuzovat identitu jedince buď jako proces sebepoznávání a konstrukce spolu s hledáním a zvnitřňováním osobní ideologie, nebo jako obsah, což je uvědomování vlastností, kterými se jedinec odlišuje a které má společné s ostatními [3].

2.2 Digitální identita

Digitální identita (dále jen dig. id.) je definována doporučující normou ITU-T X. 1252 jako digitální reprezentace informací známých o zdroji, specifickém jedinci, skupině či organizaci [4]. V této práci se bude nadále pracovat výhradně s dig. id. osob. Podstatou dig. id. je zastupování lidské skutečné identity, která má unikátně reprezentovat svého majitele. Pokud si uživatel internetu není vědom tématu digitální stopy (viz kapitola 2.3), tak se zpravidla jeho dig. id. moc neliší od jeho identity v off-line životě. Největším rozdílem je absence fyzické identity, která může být do jisté míry nahrazena biometrickými údaji člověka (otisky prstů, sken oční duhovky apod.). Jednotlivými typy informací, ze kterých se dig. id. skládá, mohou být například kontaktní údaje (jméno, telefonní číslo, e-mailová adresa, adresa bydliště apod.), profilová fotka, seznam přátel na sociálních sítích, zveřejněné zájmy (koníčky, preference, myšlenky apod.) či jiné osobní údaje (číslo bankovního účtu, rodné číslo, zdravotní údaje nebo již výše zmíněné biometrické údaje).

2.3 Digitální stopa

Digitální stopa se definuje jako uživatelem zanechaná informace při pohybu po internetu či telefonních sítí. Dělíme je primárně na aktivní a pasivní. Uživatel při pobývání na virtuálních sítí vytváří soubor informací, které zůstávají nadále uchované na serverech nejrůznějších služeb či na serverech ISP, které podle zákona o elektronických komunikacích (Zákon č. 127/2005 Sb., § 97, odst. 3) [5]:

„Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací.“

2.3.1 Aktivní digitální stopa

Uživatelem je zanechávána dobrovolně a vědomě. Jedná se například o zasílání zpráv pomocí e-mailů, chatovacích aplikací apod. Dále je zahrnuta tvorba profilu na sociálních sítích, zveřejňování příspěvků na nich nebo vyplňování osobních údajů (např. dodacích údajů při nákupu přes internetový obchod).

2.3.2 Pasivní digitální stopa

Uživatelem je zanechávána během jeho internetové relace bez přímého svolení či konání jedince. Těmito informacemi jsou například metadata, IP adresa, nastavení prohlížeče, operační systém, cookies, historie vyhledávání, informace o pohybu mobilního telefonu, které zaznamenaly BTS stanice apod.

2.4 Digitální identita ve státní správě

Státní správa již několik let využívá některé možnosti identifikace a autentizace pomocí digitální identity, jež je v tomto sektoru státem označovaná jako elektronická identita či eID. To je státem garantovaná a podporovaná forma digitální identity. Důvěryhodnost eID je základní předpoklad pro její používání v této sektoru. V celé této kapitole jsou čerpány informace z tohoto zdroje [6]. Ohledně provázání důvěryhodnosti digitální identity a atributů konkrétních osob se rozlišují dva typy:

- **Elektronické identity s prokázanou totožností osoby jejího držitele (eID podporovaná státem)**
  Tento typ slouží k unikátní a nepopiratelné identifikaci konkrétních osob v digitální sféře. Tento typ identity bude v práci nadále popisován.
- **Elektronické identity bez prokázání totožnosti jejího držitele**
  Do této kategorie spadá většina digitálních identit, které si jedinec vytváří sám na internetu a je na něm, jaké vlastnosti či atributy ho popisují. Tento typ identity nezaručuje pravost jedince, za kterého se ve své digitální identitě vydává.

2.4.1 Národní identitní autorita

Národní identitní autorita, zkráceně NIA, vytváří federativní systém, který poskytuje orgánům veřejné správy státem garantované služby identifikace a autorizace. Předává portálu Národního bodu dotazované informace z informačních systémů základních registrů, které spravuje Správa základních registrů. NIA je do značné míry identický pojem s Národním bodem pro identifikaci a autentizaci, jenž je podrobněji popsán níže [7].

2.4.2 Národní bod pro identifikaci a autentizaci

Zkráceně jako Národní bod, je portálem Národní identitní autority (NIA) a zároveň středem tohoto federativního systému. Tento portál vystupuje pro veřejnost pod názvem Identita občana, dříve jako e-identita. Má sloužit jako prostředek pro bezpečné a zaručené ověření identity uživatele online služeb, jejichž poskytovatelem je veřejná správa. Jeho cílem je zaručit poskytovatelům informace o uživateli, jenž se přihlašuje k jimi poskytovaným službám. Zpracovává a federuje údaje o subjektu ze základních registrů a předává údaje dle principu single sign-on (SSO) přihlašování. Národní bod je definovaný zákonem č. 250/2017 Sb., o elektronické identifikaci (dále jen „zákon č. 250/2017 Sb.“) [8],[9].

2.4.3 Národní uzel eIDAS

Národní uzel eIDAS je mezinárodní bránou s funkcí zpracování vzdálených, respektive přeshraničních, prokázání totožnosti občanů ostatních států EU, kde je zapracováno nařízení eIDAS. Je samostatnou součástí NIA [7]. V rámci identifikace na portálu Národního bodu je poskytována tato možnost přihlášení pod názvem IIG – International ID Gateway.

2.4.4 Správa základních registrů

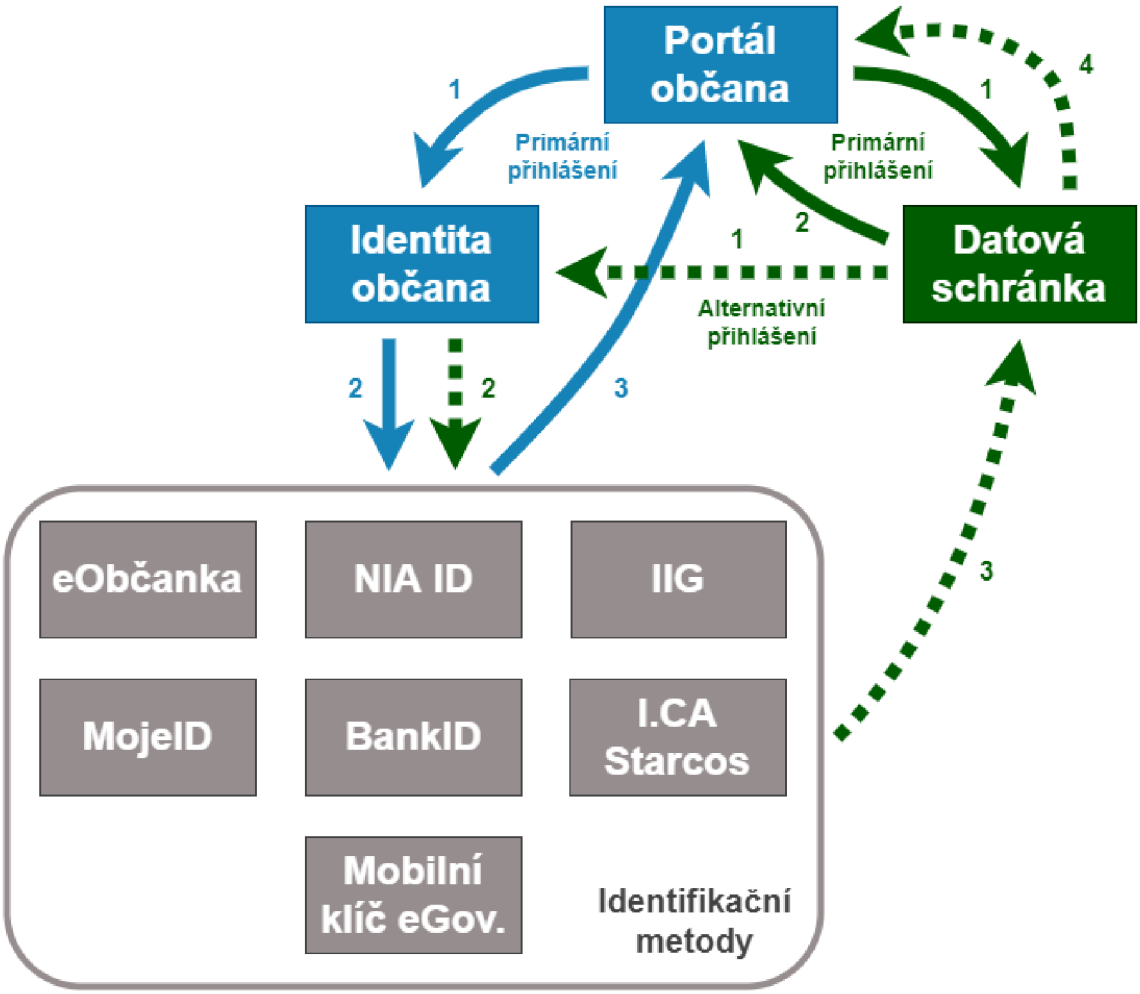
Správa základních registrů je úřad podřízený ministerstvu vnitra, který je dle zákona č. 250/2017 Sb. správcem Národního bodu pro identifikaci a autentizaci [9]. Jeho kompetencemi jsou provoz základních registrů jako registru obyvatel, osob, práv a povinností, realizuje vazby mezi jednotlivými registry a informačními systémy a zpřístupňuje referenční údaje v rámci své agendy a v rozsahu svého oprávnění [10]. Jinými slovy je to systém, který běží na pozadí a z nichž oprávněné subjekty získávají informace pro jejich autorizované úkony.

2.4.5 Kvalifikovaný systém a správce

Tyto dva pojmy jsou již definovány ve zmíněném zákoně č. 250/2017 Sb. [9]. Kvalifikovaný systém je systémem pro elektronickou identifikaci, jenž je spravován kvalifikovaným správcem, umožňuje vytvoření národního bodu. Důležitým požadavkem tohoto systému je, že musí poskytovat značnou minimální úroveň záruky. Kvalifikovaným správcem může být jen státní orgán, anebo osoba, které byla udělena akreditace pro správu kvalifikovaného systému.

2.4.6 Portál občana

Jeden ze systémů vytvořených za účelem digitalizace státní správy. V tomto konkrétním si může občan vstupující na tento portál zobrazit jím personalizovanou sadu služeb eGovernmentu a řešit řadu úkonů z pohodlí domova, bez nutnosti návštěvy daných úřadů. Pro přihlášení musí občan prokázat svoji totožnost, a to přes Identitu občana, potažmo přes Datovou schránku. Buď jsou služby přímo dostupné v portálu, anebo jsou zprostředkované, resp. přenesené přes odkaz a uživatel je přesměrován na jiné portály, ovšem již bez nutnosti opětovného přihlašování díky principu SSO. Po přihlášení je možné si zobrazit informace o vlastní osobě a s ní spojenými údaji, například z registru řidičů, registru obyvatel, katastru nemovitostí, registru silničních vozidel, zdravotnické dokumentace vedené u některých připojených poskytovatelů zdravotních služeb a další [11].



Obrázek 2.1: Schéma přihlášení do Portálu občana

2.4.7 Přínosy eID

Přínosů, které přináší elektronická identita podporovaná státem, je hned několik. Jelikož digitalizace státní správy bude v budoucnosti pokračovat, tak lze očekávat další růst její přínosnosti.

Jednou z výhod je bezesporu zvýšení úrovně zabezpečení, které je způsobeno například díky využití vícefázové autentizace či nepopiratelnému přiřazení identifikačních prostředků konkrétní osobě.

Dalším přínosem je centralizace služeb poskytovaných státem (z jiného pohledu nevýhodou, viz kapitola 5.4.4). Díky tomuto není potřeba si pamatovat tolik přihlašovacích jmen, hesel, mít několik dodatečných autentizačních prvků, které byly před příchodem centralizace, resp. federace služeb, nutné vědět či vlastnit. S nižším počtem znalostních údajů je jednodušší si zapamatovat komplexnější hesla, což má také za následek zvýšení bezpečnosti.

Jedním z přínosů je taktéž urychlení komunikace mezi občanem a státní správou, které taktéž snižuje byrokracii ohledně návštěvy úřadů, čekání u přepážky, tisknutí fyzických dokumentů, atd. Portály státní správy jsou kromě plánovaných technických údržeb otevřené neustále, zatímco úřady jsou pro občany otevřeny jen v úřední hodinách.

Státní eID má oproti komerčním identitám jednu nespornou výhodu, a to, že stát nemůže monetizovat tyto databáze a prodávat z ní data za účelem zisku. Řada společností poskytující komerční identity prodává (oficiálně anonymizovaná, ale to nelze tvrdit s jistotou) vyhodnocená data o chování spotřebitelů atd., jiným firmám, které pak z těchto informací profitují [6].

2.4.8 Úrovně záruky

Tři úrovně záruk stanovené nařízením eIDAS poskytují kategorizaci důvěryhodnosti identifikace a autentizace. Jak lze předpokládat, čím vyšší úroveň, tím vyšší důvěra je těchto záruk. Níže jsou zmíněny tyto úrovně:

- **Nízká úroveň** – ověření totožnosti není zaručené, jméno a heslo je zvoleno uživatelem a jeho identita je pouze jím deklarována.
- **Značná úroveň** – ověření totožnosti je zaručené, pro přihlášení je využíváno jména, hesla a dalšího faktoru.
- **Vysoká úroveň** – ověření totožnosti je zaručené, k přihlašování je používán navíc i fyzický identitní prostředek, který byl vydán osobě s ověřenou totožností a pro jeho použití jsou potřeba přihlašovací údaje na bezpečném zařízení (kupříkladu to může být čip elektronického občanského průkazu či FIDO token služby MojeID).

3 E-IDENTITA (IDENTITA OBČANA)

Hned na začátku této kapitoly se sluší zmínit, že během zpracovávání mé bakalářské práce byl dne 28. listopadu 2021 Správou základních registrů jako správcem změněn název portálu Národního bodu pro identifikaci a autentizaci z e-identita na Identitu občana. Jelikož jsou v této práci používány zdroje i staršího data než výše zmíněného a objevují se v ní oba tyto názvy, tak je berte prosím za ekvivalentní. V celé této kapitole jsou čerpány informace z tohoto zdroje [8].

Základ pro Identitu občana byl položen již v 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 (aneb nařízení „eIDAS“) [12]. V české legislativě s tímto nařízením souvisí zákon č. 297/2016 Sb., Zákon o službách vytvářejících důvěru pro elektronické transakce (dále jen „zákon č. 297/2016 Sb.“) [13]. Na poli elektronické identifikace bylo toto nařízení zapracováno do národní legislativy v zákoně č. 250/2017 Sb. [9] (přes Národní bod pro identifikaci a autorizaci).

Identita občana je státem vytvořená přihlašovací služba eGovernmentu, jejímž účelem je unikátní a nepopiratelná identifikace nakládající osoby, jenž se shoduje s osobou, jejíž údaje jsou zaznamenány na jejím účtu Identity občana. Tento účet je během procesu přihlašování ověřován důvěryhodnou autoritou vůči Národnímu bodu.

Na webové stránce info.identitaobcana.cz/sep/ je možné si zobrazit výčet všech poskytovatelů služeb, kteří využívají pro službu identifikace portál Identita občana [14].

3.1 Identifikační prostředky nabízené státem

Prostředky pro elektronickou identifikaci, které jsou poskytovány státní správou a jsou e-identitou ve smyslu zákona, jsou rozvedeny v níže uvedených podkapitolách.

3.1.1 Elektronický občanský průkaz s čipem

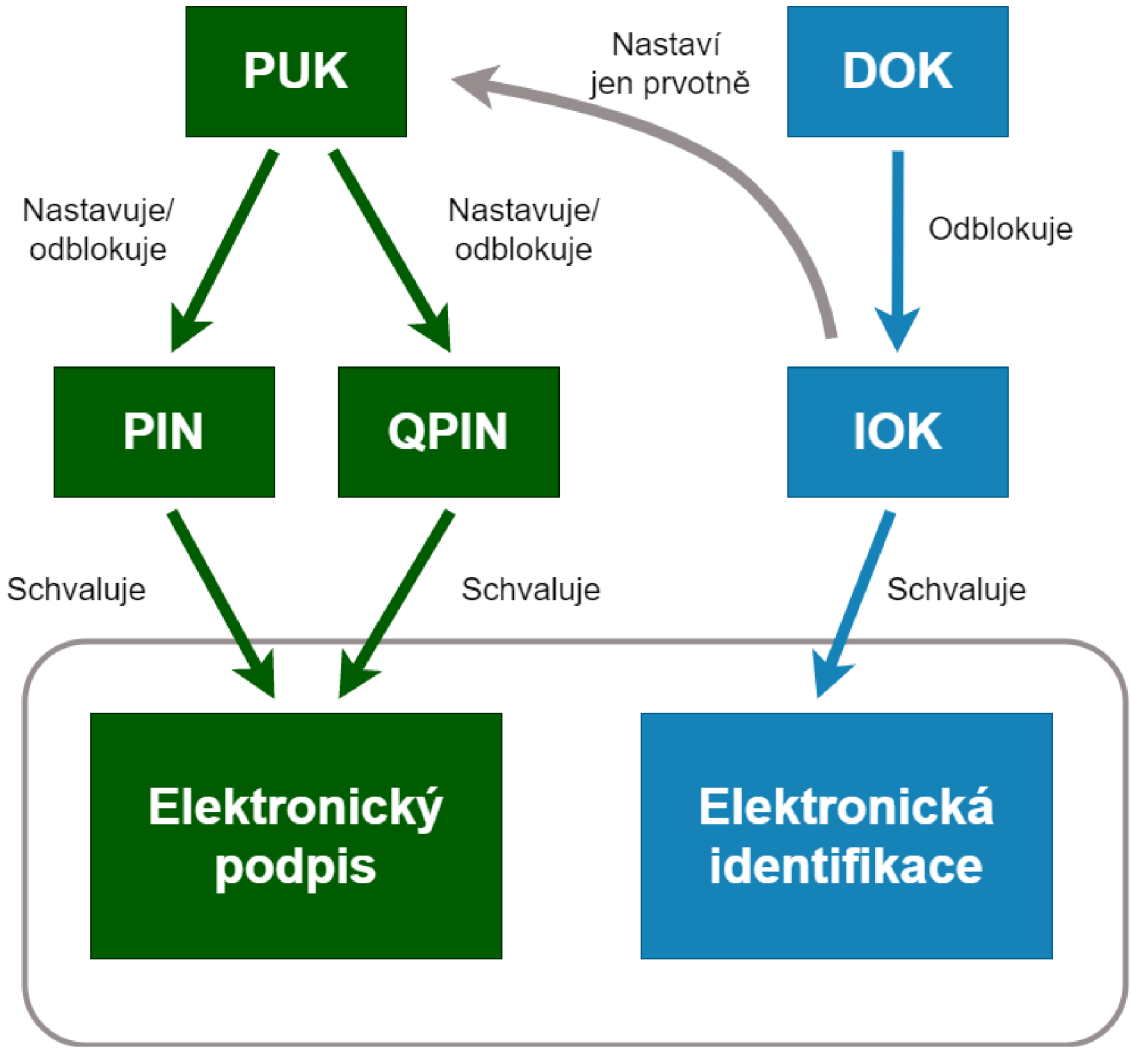
Jiným názvem eObčanka, poskytuje vysokou úroveň záruky, používá se pro přihlášení k online službám státu na úrovni vysoká a nižší. Občanské průkazy vydané po datu 1. července 2018 obsahují elektronický čip, který je nutné aktivovat pro tento způsob identifikace. Možností, jak využít eObčanku je řada, například pro přihlášení na Portál občana, Finanční správu, portál Ministerstva práce a sociálních věcí, přihlásit se jím pro eRecept či nahlédnout do živnostenského rejstříku. Výhodou eObčanky je také, že se dá využít i pro přihlášení k online službám jiných států Evropské unie.

Při vydávání občanského průkazu je nutné si tuto funkci aktivovat, aby mohla být takto využívána. Během procesu aktivace si občan zadá ochranné přístupové kódy. Kódy IOK, PIN a QPIN slouží pro schvalování operací. Kódy DOK a PUK slouží k odblokování nebo nastavení jiných kódů. Níže jsou podrobněji rozvedeny funkce jednotlivých kódů:

- **Identifikační osobní kód (IOK)** – využíván pro schválení elektronické identifikace a prvnímu nastavení PUK, používá se při každé identifikační operaci.
- **Deblokační osobní kód (DOK)** – využíván pro odblokování IOK, ale je málokdy používán.
- **Bezpečnostní osobní kód (BOK)** – využíván při osobním prokazování totožnosti, protože s ním lze zajistit vyšší úroveň prokazování, také se využívá jen málokdy.
- **Personal Identification Number (PIN)** – využíván pro schvalování operací s certifikáty a kryptografickými klíči (vytvoření klíčů, autentizace, zápis certifikátu do čipu aj.), je používán za každé situace, která obsahuje přihlášení certifikátem nebo při jejich správě.
- **PIN Unblocking Key (PUK)** – využíván pro nastavení nebo odblokování kódů PIN a QPIN, též je málokdy používán.
- **PIN pro kvalifikované elektronické podpisy (QPIN)** – využíván pro schvalování kvalifikovaného elektronického podpisu, používán vždy při vytváření kvalifikovaného elektronického podpisu [15].

Aby mohl občan z domu využívat svoji aktivovanou eObčanku, musí vlastnit čtečku čipových karet, ať už externí, připojenou do svého PC kabelem pomocí sběrnice USB či bezdrátově přes Bluetooth, anebo interní, jelikož některé notebooky a klávesnice mají v sobě tyto čtečky již integrovány. Samozřejmě je nutné mít nainstalované příslušné ovladače pro danou čtečku.

Posledním požadavkem je instalace softwaru eObčanka, který slouží k její obsluze. Celý software se skládá ze tří komponent, a to aplikace pro identifikaci, ovladačů certifikátové karty a aplikace Správce karty [16].



Obrázek 3.1: Schéma využití kódů eObčanky [15]

3.1.2 Mobilní klíč eGovernmentu

Poskytuje značnou úroveň záruky, používá se pro přihlášení k online službám státu na úrovni značná a nižší. Původně byl designován pro přihlašování k systému Datových schránek, avšak poté se jeho využití rozšířilo pro přihlašování do Národního bodu. Je nutné mít nainstalovanou aplikaci mobilního klíče na smartphonu.

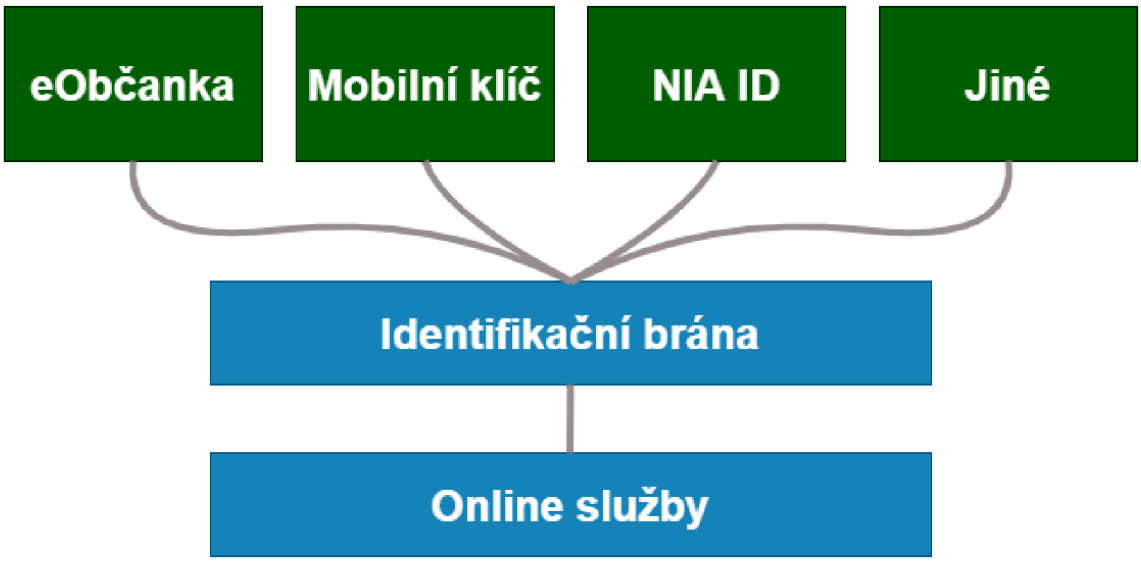
Má několik výhod, třeba z pohledu uživatelské přívětivosti, umožňuje několik metod přihlášení (např. pomocí hesla, obrázkových hesel, biometriky, rozpoznání obličeje) a nevyžaduje dodatečné zadávání jiných ověřovacích kódů. Další výhodou je upozornění uživatele na přihlášení kterýmkoli prostředkem při přihlášení do Národního bodu. Pro připojení do národního bodu se využívá naskenování QR kódu, který je vygenerován webovou aplikací na doméně eidentita.cz, kam je uživatel přesměrován z aplikace mobilního klíče [8].

3.1.3 NIA ID

Poskytuje značnou úroveň záruky, používá se taktéž k přihlášení k online službám státu. Původní název pro tuto metodu přihlášení byl „jméno, heslo a SMS“. Z tohoto vyplývá, že uživatel musí znát své přihlašovací údaje (jméno a heslo) a být vlastníkem unikátního telefonního čísla, aby mu mohl přijít autentizační jednorázový kód v SMS zprávě. Výhodou z uživatelského hlediska je právě tento jednoduchý způsob přihlašování, který využívá dvoufaktorovou autentizaci [7],[8].

3.1.4 International ID Gateway (IIG)

Poskytuje nízkou až vysokou úroveň záruky, to záleží na zvoleném identifikačním prostředku. Tento identifikační prostředek spadá pod národní uzel eIDAS, díky kterému se mohou občané různých zemí Evropské unie přihlásit k eGovernmentu dané země. Jak se dá předpokládat, tato možnost je zobrazena při přihlašování k národním uzlům eIDAS v každé zemi EU, nejen při přihlašování k českému eGovernmentu. Na této stránce lze najít seznam zemí a jejich příslušných eID systémů [7],[17].



Obrázek 3.2: Identifikační proces při využití různých státních id. prostředků [8]

3.2 Identifikační prostředky, jež nejsou e-identitou ve smyslu zákona

3.2.1 Datová schránka

Datová schránka je elektronické úložiště, jež bylo vymezené zákonem č. 300/2008 Sb., Zákon o elektronických úkonech a autorizované konverzi dokumentů [18]. Primárním účelem tohoto úložiště je zaručená komunikace a doručování elektronických dokumentů od orgánů veřejné moci fyzickým či právnickým osobám, nebo mezi doručováním dokumentů mezi fyzickými a právnickými osobami. Další její funkcí je možnost ji využít pro přihlášení na různé webové stránky státní správy či samospráv. Ačkoli ji lze využívat v určité míře pro přihlášení do webových aplikací jako přes e-identitu, ale ani tak není identifikačním prostředkem ve smyslu zákona č. 250/2017 Sb. K datové schránce je možné se přihlásit mnoha způsoby, prvním je přesměrováním na portál Identity občana, další možností je pomocí jména a hesla, třetí variantou je pomocí Mobilního klíče eGovernmentu a pak také pomocí SMS (jméno, heslo, SMS kód), certifikátu nebo bezpečnostního kódu (jméno, heslo, kód). K datové schránce se lze dostat také přes portál občana [6].

3.2.2 Kvalifikovaný certifikát

Neboli kvalifikovaný elektronický podpis byl vymezen v České republice také zákonem č. 227/2000 Sb., Zákon o elektronickém podpisu, avšak dnes již je tento zákon zrušen zákonem č. 297/2016 Sb., § 20 [13]. Tento typ certifikátu může vydávat jen kvalifikovaný poskytovatel certifikačních služeb, jehož definice je vymezena ve stejném zákoně zmíněném v předchozí větě.

Je to standardní digitální certifikát, avšak jeho použití je směřováno zejména pro komunikaci s českými státními institucemi, např. při bezpečném ověřování elektronického podpisu, e-mailovou elektronickou komunikaci se státní správou (soudy, zdravotní pojišťovny, Finanční úřad apod.) nebo při zajištění neodmítnutelnosti odpovědnosti.

V České republice jsou akreditovaní tři poskytovatelé kvalifikovaných certifikátů. Jediným státním poskytovatelem je Česká pošta, s. p. Druhým, avšak komerčním subjektem vydávající tyto certifikáty je První certifikační autorita, a. s. a třetím je subjekt eIdentity, a. s.

3.2.3 Elektronický podpis

Elektronický podpis je z technického hlediska defacto to stejné jako digitální podpis, ovšem elektronický podpis je správné označení z právního hlediska. Legislativně byl ošetřen stejným způsobem a ve stejných zákonech, jako to bylo zmíněno výše v kapitole o kvalifikovaném certifikátu.

Z právního hlediska se v České republice dělí na zaručený elektronický podpis a kvalifikovaný elektronický podpis (identický termín jako kvalifikovaný certifikát zmíněný výše). Elektronický podpis prostý není v českém právu definován (je tím myšlen kupříkladu naskenovaný vlastnoruční podpis). Z technického hlediska je elektronický podpis v podstatě jakýkoli soubor dat, která jsou připojena ke zprávě a jejichž funkcí je ověřit identitu osoby, jež se podepsala pod danou datovou zprávu.

3.2.4 Daňová informační schránka (DIS+)

Tato schránka je definována podle zákona č. 280/2009 Sb., Zákon daňový řád [19]. Poskytuje službu, kdy se přes vzdálený přístup lze dozvědět určité informace o daňovém subjektu, které jsou na daňovém účtu poplatníka. Informacemi, které se zde nacházejí, mohou být například daňový kalendář, stav daňového účtu, přehled zpráv a dokumentů vyměňovaných mezi poplatníkem a správcem daně apod.

Jsou tři způsoby, jakým se lze přihlásit do DIS+, a to buď pomocí datové schránky, nebo pomocí identity občana, anebo pomocí přístupových údajů, které byly přiděleny Finanční správou ČR [20].

3.3 Identifikační prostředky nabízené soukromoprávními kvalifikovanými poskytovateli

Níže jsou zmíněny prostředky, které nejsou poskytovány státní správou, nýbrž soukromoprávními kvalifikovanými poskytovateli. Podmínky a postupy nastavené pro tyto poskytovatele jsou definovány v již několikrát zmiňovaném zákoně č. 297/2016 Sb. [13].

3.3.1 BankID

Poskytuje značnou úroveň záruky, používá se k přihlášení k online službám státu a ke službám soukromých společností. Výhoda tohoto řešení spočívá v jednotné identifikaci jak vůči státní správě, tak vůči soukromým společnostem. Mnoho vlastníků bankovních kont již má aktivovanou bankovní identitu anebo ji mám možnost aktivovat a rovnou používat, protože jejich identita byla již ověřena při zakládání bankovního konta. Podrobnější informace z popisující BankID z technického hlediska jsou v kapitole 6.4, zatímco popis z obecného hlediska se nachází v kapitole 3.5.

3.3.2 Čipová karta Starcos

Poskytuje vysokou úroveň záruky, je zprostředkována soukromou společností První certifikační autorita, a. s. Nevýhodou této karty je, že je zpoplatněná, ale to je vyváženo kvalitním řešením, jež má profesionální využití (např. pro přístup do portálu elektronického mýta či přístupů zaměstnanců do jiných informačních systémů). Na čipové kartě je nahrán identifikační certifikát, při jejím je generována dvojice kódů PIN a PUK. PIN slouží k ochraně citlivých operací. Kód PUK je využit při zablokování karty, když je zadán kód PIN vícekrát chybně. Pro správu karty je využívána aplikace I. CA SecureStore [21].

3.3.3 MojeID

Dle uživatelem poskytnutých identifikátorů nabízí úrovně záruk od nízké až po vysokou, používá se pro přihlášení k online službám státu nebo samospráv, pro přihlašování do soukromoprávní sféry (např. e-shopy, knihovny, zpravodajské weby apod.) i pro správu domény u některých doménových registrátorů. Provozovatelem této služby je sdružení CZ.NIC.

Je zde využívána vícefázová autentizace, proto je potřeba kromě hesla mít i další faktor. Jako bezpečnostní klíče se doporučují zařízení standardu FIDO2 alespoň úrovně L1, tj. lze využít fyzický hardwarový klíč (např. YubiKey od firmy Yubico, Idem Key od firmy GoTrust), mobilní aplikaci MojeID klíč či využít systémového klíče (otisk prstu, zadání PIN kódu atd.) [22].

3.4 Využití v číslech

Vzhledem k informacím aktualizovaným ke dni 1. února 2022, z celkového počtu necelých 9 milionů vydaných ID prostředků bylo celých 8 milionů jen bankovních identit. Kolem 800 tisíc ID prostředků bylo vydaných státem, přičemž nadpoloviční většinu si v této podmnožině zaujala eObčanka. Identifikační prostředky, které jsou poskytovány přes soukromoprávní kvalifikované poskytovatele, dosahují sotva 100 tisíc vydaných prostředků. Ovšem tyto prostředky jsou aktivně využívány, už jen z důvodu, že když si je někdo musel ne tak jednoduše vyřídit a založit, tak je bude využívat. Celkový podíl profilů, jenž se přihlásili alespoň jedním prostředkem, byl lehce nad 5 milionů [7].

Tabulka 3.1: Souhrn identifikačních prostředků pro eID ve smyslu zákona

Identifikační prostředek	Úroveň záruky	Poskytovatel	Autentizační prvky	Dostupnost pro cizince	Využitelnost
eObčanka	vysoká	stát	občanský průkaz s elektronickým čipem, IOK kód	ne	jen eGovernment
Mobilní klíč eGovernmentu	značná	stát	mobilní klíč	ano, ale s trvalým pobytem v ČR	jen eGovernment
NIA ID	značná	stát	jméno, heslo, SMS kód	ano	jen eGovernment
International ID Gateway (IID)	nízká až vysoká	stát/EU	záleží na národnosti občana	ano	záleží na státu EU
BankID	značná	Bankovní identita, a.s.	mobilní klíč	ano (s elektronicky čitelným dokladem)	částečně eGovernment i komerční e-služby
Čipová karta Starcos	vysoká	První certifikační autorita, a.s.	elektronická čipová karta	ano	eGovernment i komerční e-služby
MojeID	nízká až vysoká	CZ.NIC, z.s.p.o.	HW klíč, mobilní klíč, systémový klíč	ano	eGovernment i komerční e-služby

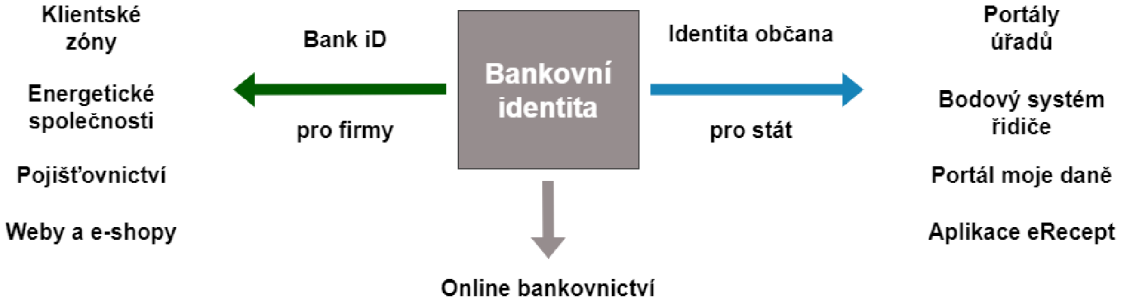
3.5 Bankovní identita

Bankovní identita (neboli BankID) je elektronická identifikační metoda, jejímž cílem je identifikovat jejího uživatele vůči subjektu, který potřebuje ověřit jeho identitu. Je zamýšlena pro spolupráci jak s komerčním sektorem, který poskytuje e-služby, tak pro využití elektronických služeb státu, které lze také nazývat jako eGovernment.

3.5.1 Struktura BankID

V České republice je společnost Bankovní identita a. s. původním projektem České bankovní asociace (ČBA), což je dobrovolné sdružení bank a stavebních spořitelen působících na českém trhu. ČBA sdružuje 37 bank, které reprezentují 99 % českého bankovního sektoru [23].

Pro objasnění struktury: Termín „bankovní identita“ je používán spíše v obecném významu pro identifikační metodu. Za to termín „BankID“ je používán více pro konkrétní službu poskytovanou uskupením bank (firma Bankovní identita a. s.). Ta bude službu BankID poskytovat prostřednictvím firmy Bankovní identity soukromým firmám. Ve vztahu ke státu je vhodnější používat pro službu termín bankovní identita [24].



Obrázek 3.3: Rozdělení Bankovní identity [25]

3.5.2 Pro uživatele

Z pohledu uživatelů jako fyzických osob nabízí bankovní identita funkce jako přihlašování do internetových obchodů, klientských zón nebo jiných aplikací, v případě uděleného souhlasu mohou být za uživatele bankovní identitou vyplňovány formuláře, dále nabízí prokázání osobních údajů při potřebě jejich ověření a je možné s ní elektronicky podepisovat dokumenty. Pro uživatele jsou tyto funkce bezplatné.

Ověření identity je založené na propojení API webové stránky firmy/portálu státní správy a banky. Pro přihlášení uživatel klikne na ikonu přihlášení přes BankID, zvolí svou banku, pak je přesměrován na přihlašovací stránku internetového bankovnictví své banky. Jako druhý faktor je využíván mobilní klíč aplikace banky nebo jednorázový autentizační SMS kód odeslaný na telefonní číslo uživatele. Po úspěšném ověření totožnosti je uživatel přihlášen. Výhodou BankID je, že neposkytuje informace o uživateli třetí straně. Jinými slovy, služba (firma či úřad), kam se uživatel přihlašuje, nevidí jeho soukromé údaje a nemá k nim přístup [26].

3.5.3 Pro firmy

Z pohledu firem tento produkt podle tvůrců BankID může nabídnout výhody jako zjednodušení procesů, má ušetřit papírování, snížení finančních nákladů díky větší míře automatizace, zajistit, že více zákazníků dokončí registraci nebo objednávku na webových stránkách firem. Dalšími proklamovanými výhodami jsou rychlost aktivace a integrace tohoto systému, společně s vysokou bezpečností.

Společností BankID jsou poskytovány služby CONNECT, SIGN a IDENTIFY, které jsou rozděleny do balíčků, jež si firmy pořizují. Tyto služby jsou podrobněji zmíněné níže:

- **CONNECT** – již zahrnuta v základním balíčku, funkcí této služby je zabezpečené přihlášení ke službám firem či do klientských zón.
- **SIGN** – služba zajišťující zaručený elektronický podpis PDF dokumentů.
- **IDENTIFY** – poskytuje sadu informací pro ověření klienta.

Podle zakoupené varianty balíčku se liší sada informací, které mohou být využity pro chod služby firmy. V každé variantě balíčku je obsažena funkce CONNECT. Obsah údajů v balíčcích je uveden níže:

- **CONNECT** – ID uživatele, jméno a příjmení, telefon, e-mail, datum narození.
- **IDENTIFY** – vše z CONNECT a navíc adresy, bankovní účet, titul, pohlaví, rodné číslo.
- **IDENTIFY PLUS** – vše z CONNECT, IDENTIFY a navíc místo narození, stav, doklad, právní status.
- **IDENTIFY AML** – vše z CONNECT, IDENTIFY, IDENTIFY PLUS a navíc sada informací ke vzdálené identifikaci klienta dle zákona č 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu [27].

3.5.4 Vývoj projektu

V dnešní době je bankovní identita velmi aktuálním a dynamicky se proměňujícím tématem. Projekt byl zahájen v únoru 2019, pokračoval legislativními změnami, projednáváním Poslaneckou sněmovnou, poté v únoru 2020 vyhlášením zákona č. 49/2020 Sb., o bankách [28]. Až se nakonec během roku 2021 postupně implementovala bankami působícími v České republice, což v dnešní době způsobuje častá upozornění a nabídky pro její aktivaci od komerčních bank, u nichž mají zákazníci otevřená svá konta, takže jsou majitelé bankovních účtů relativně často konfrontováni s tímto tématem. Na začátku roku 2022 byl web bankovni-identita.cz zrušen a nyní je při zadání této adresy do vyhledávání jedinec přesměrován na web bankid.cz, takže informace čerpané z webu bankovni-identita.cz jsou dnes dostupné jen přes Wayback Machine, což je webová aplikace, která funguje jako archiv internetových webových stránek [24].

K datu 15. května 2022 banky Air Bank, Česká spořitelna, Československá obchodní banka (ČSOB), Komerční banka a MONETA Money Bank poskytovaly pro své zákazníky plnou funkcionalitu bankovní identity. Tím je myšlena identifikace jak vůči státní správě, tak vůči soukromoprávním firmám. Banky Raiffeisenbank a Fio banka poskytují k výše zmíněnému datu zatím jenom využití do portálů státní správy. Banky mBank a UniCredit Bank plánují zprovoznit bankovní identitu pro své zákazníky do konce roku 2022.

Plná funkcionalita	Funkční zatím jen vůči státní správě	Zatím nezprovozněné
Air Bank	Raiffeisenbank	mBank
Česká spořitelna	Fio banka	UniCredit Bank
ČSOB		
Komerční banka		
MONETA Money Bank		

Tabulka 3.2: Souhrn bank provozujících BankID

4 EVROPSKÁ DIGITÁLNÍ IDENTITA

Evropská digitální identita (dále EDI) je projektem Evropské komise, jejímž cílem je umožnit občanům EU jednodušší prokazování své totožnosti vůči soukromým společnostem i vůči státní orgánům v členských zemích EU. Pro EDI byly položeny základy již v nařízení eIDAS [12]:

„Jedním z cílů tohoto nařízení je odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají k autentizaci, alespoň pro účely veřejných služeb. Toto nařízení nemá za cíl zasahovat do systémů správy elektronické identity a souvisejících infrastruktur zřízených v členských státech. Jeho cílem je zajistit, aby u přístupu k přeshraničním on-line službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace.“

Dne 3. června 2021 byl Evropskou komisí dále upřesněn rámec EDI. Státy EU byly vyzvány, aby do září roku 2022 vytvořily společnou sadu nástrojů a ihned začaly přípravné práce. Sada nástrojů by měla zahrnovat technickou architekturu, normy apod. Dokumenty prokazující totožnost budou uloženy v evropských peněženkách digitální identity, které budou mít podobu mobilní aplikace. EDI nebude nahrazovat stávající digitální identity, bude jen nadstavbou, která propojí ty již dříve vzniklé [29],[30],[31].

4.1 Využití Evropské digitální identity

U EDI je zamýšleno značné praktické využití (např. k prokázání věku, při ubytování v hotelu, při pronájmu vozidla, k prokazování totožnosti, při podávání daňového přiznání, k uložení lékařského předpisu, otevření bankovního účtu, žádosti o bankovní úvěr, podepsání dokumentů elektronickým podpisem nebo u veřejných služeb). Peněženka bude umožňovat propojení vnitrostátní digitální identity s jinými doklady, které bude možné do ní uložit (např. bankovní účet, řidičský průkaz, kvalifikovaný elektronický podpis, potvrzení o kvalifikaci, recepty na léky aj.). Při prokazování bude velkou výhodou, že nebude třeba ukazovat více údajů, než bude nutné (např. při nákupu tabákových výrobků se zobrazí jen žádoucí osobní údaj (věk) bez dalších nežádoucích údajů, které kontrolující nemusí znát (jako rodné číslo, bydliště apod.)) [29],[30],[31].

4.2 Evropské státy používající digitální identitu

Jak je zmíněno výše, v následujících letech bude v EU celoplošně zavedena Evropská digitální identita. Následkem nařízení eIDAS se v roce 2018 stalo pro státy EU povinným uznávání elektronické identifikace všech občanů EU. Nicméně, některé státy EU samy začaly v oblasti e-identity konat mnohem dříve, než vznikla tato iniciativa ze strany Evropské unie. Průkopníkem v této oblasti se stalo Estonsko. V následujících odstavcích budou zmíněny příklady evropských států, kde byly zavedeny digitální identity pro komunikaci se státní správou ještě před působením nařízení eIDAS a následně EDI.

4.2.1 Estonsko

Je považováno za průkopníka v oblasti digitalizace státní správy. Již v roce 2002 zde byla zavedena digitální identita zvaná „e-ID“. Dnes má 99 % Estonců státem vydanou digitální identitu. V Estonsku se mohou lidé se svou e-ID autentizovat do svého internetového bankovnictví, digitálně podepisovat dokumenty, volit pomocí „i-Voting“ systému, založit firmu apod. Důsledkem zavedení e-ID byla dvouprocentní úspora ročního HDP [32].

Uživatelé mají možnost využívat e-ID pomocí třech řešení pro elektronickou identifikaci, z čehož druhé a třetí jsou využívané mobilními telefony. Všechna zmíněná řešení mají ekvivalentní funkce ohledně identifikace, viz níže.

První možností je držení tzv. „ID-card“, což není nic jiného než průkaz totožnosti, jehož vlastnictví je povinné pro všechny občany Estonska. ID-card obsahuje s ní dva svázané certifikáty. S ní se vydávají PIN a PUK kódy, které slouží k ověření identity a podepisování. I v případě ztráty e-ID není možné využívat elektronické služby bez znalosti PIN kódů. Jen na tento dokument je možné cestovat po Schengenském prostoru, na dva níže zmíněné ne. Tento dokument je platný po dobu pěti let.

Druhé je „Mobile-ID“, které je založeno na principu digitální identifikace skrze speciální SIM kartu, která je vydávaná lokálními operátory. Dorazí společně s PIN a PUK kódy. PIN1 se používá pro ověření totožnosti či přihlášení do systému, PIN2 pro digitální podpis nebo potvrzování transakcí a PUK se využívá pro odemčení zamčených PIN kódů. Všechny automaticky vygenerované kódy je možné a velmi doporučené změnit. Mobile-ID je přenosné a použitelné podle toho, kde se SIM karta nachází. Platnost tohoto certifikátu je také pět let.

Třetím řešením je využití „Smart-ID“, což je aplikace, která není vázána na SIM kartu, ale jen na chytré zařízení, na které je nainstalována. Na každém zařízení musí být vytvořen personalizovaný účet pomocí ID-card nebo Mobile-ID. Platnost tohoto certifikátu jsou tři roky [33].

4.2.2 Dánsko

V Dánsku je využíváno tzv. „NemID“, které se používá pro přihlašování do internetového bankovnictví, pro přihlašování ke službám poskytovaných státem nebo pro řadu firem, které taktéž využívají tento projekt. Přihlašování v NemID se skládá z uživatelova identifikátoru, hesla a druhého faktoru (např. fyzické papírové karty s kódy, aplikace na mobilním telefonu nebo pomocí hardwarového tokenu).

Na kartě s kódy je vytištěno mnoho jednorázových hesel, jejichž sada je unikátní pro každého uživatele. Je podmínkou, aby kódy z této karty nebyly za žádných okolností digitalizované, ani vyfotografované, ani přepsané do elektronického zařízení. V případě, že budou brzy všechny kódy využity, banka odešle novou kartu s kódy.

Alternativou místo karty s kódy je tzv. „NemID code app“, což je aplikace pracující na bázi dvoufázového ověření. V případě, kdy je potřeba použít aplikaci, uživateli se zobrazí notifikace na jeho chytrém zařízení. Samotný přístup do aplikace je zabezpečen buď pomocí čtyřmístného kódu, rozpoznáním otisku prstu nebo obličeje.

Třetí alternativou je hardwarový token, což je malé zařízení s displejem a tlačítkem, které zastává funkci elektronické karty s kódy. Po zmáčknutí tlačítka je vygenerován jednorázový kód. Tento token je vydáván poskytovatelem služby a jeho obsah je taktéž unikátní pro každého uživatele [34].

4.2.3 Německo

V Německu je poskytovatelem tzv. „ePerso“, resp. „eID“, stát. Tyto průkazy totožnosti, ve kterých jsou na čipech uloženy unikátní údaje o majiteli a soukromých klíčích, slouží pro autentizaci. Začaly se vydávat v roce 2010, avšak původní záměr se nepotkal s očekáváním. Dlouhou dobu nechtěla valná část veřejnosti využívat jejich elektronické identity. Proto se německá vláda v roce 2017 rozhodla, že ve výchozím nastavení bude funkce ověření eID na nových průkazech totožnosti aktivovaná a připravená k použití. Samozřejmě zůstala možnost pro ty, jenž si nepřejí, aby byla tato funkce na jejich průkazech aktivovaná, ji deaktivovat. eID se dá v Německu primárně využít pro on-line identifikaci při komunikaci s úřady, ochota komerční sféry se připojit k tomuto státnímu projektu není moc velká. Lze se domnívat, že je to kvůli zabezpečení a problémům, které již v minulosti postihly tento projekt [35].

Od září roku 2021 je spuštěna možnost mít svoji eID uloženou v mobilním telefonu na SIM kartě, přičemž pro autentizaci se využívá šestimístného PIN kódu. Ovšem je nutné, aby byla v mobilním telefonu nainstalována aplikace „AusweisApp2“. Tím je eliminována potřeba fyzické čtečky karet, která je při použití eID na průkazu totožnosti zapotřebí [36].

Německý systém pracuje na principu vzájemné autentizace, kdy se autentizuje držitel eID vůči terminálu, ale i terminál vůči držiteli eID. Mezi terminálem a eID je pomocí technologie NFC navázán kanál s šifrovanou end-to-end komunikací. Po úspěšné autentizaci jsou ověřována autorizační práva terminálu [37].

4.2.4 Švédsko

Ve Švédsku je největším elektronickým identifikačním systémem „BankID“, který je využíván 94 % uživatelů chytrých telefonů. Počátky BankID se datují už do roku 2003, od té doby služba získala 8 milionů aktivních uživatelů a je akceptována 600 webovými službami [38]. Jen lidé se švédským rodným číslem mohou získat BankID. Lze ho využít v platební aplikaci Swish, k přístupu ke svým lékařským záznamům přes službu Vårdguiden 1177, k přihlášení do internetového bankovnictví nebo pro přihlášení do služeb e-governmentu.

Uživatelé si mohou zvolit jeden ze tří typů rozhraní, které slouží k přístupu ke svému BankID. První je pomocí „Bank-id on file“, kdy je na lokálním disku uložen tajný šifrovací klíč i „soft“ certifikát. Nutností je ovšem mít na počítači nainstalovaný speciální program. Druhým způsobem je pomocí „Bank-id on card“, kdy je tajný šifrovací klíč uložen v čipu karty s integrovaným obvodem, ten funguje jako „hard“ certifikát. K tomuto způsobu je nutné mít speciální čtečku karet. Třetí možností je přistoupit pomocí „Mobile bank-id“, které funguje na smartphonech po stažení aplikace [39].

4.2.5 Belgie

V Belgii jsou všechny karty vydané od roku 2004 elektronické s čipem, pomocí nichž lze využívat eID. Čip obsahuje stejné informace, které jsou viditelné na kartě, spolu s adresou majitele karty a jeho identitou, která obsahuje certifikát a soukromý klíč na podepisování dokumentů. Pro využívání těchto služeb musí mít držitelé karet doma vlastní eID kartu, čtečku karet a nainstalovaný software, který funguje jako prostředník mezi čtečkou a počítačem [40].

5 BEZPEČNOSTNÍ HROZBY

Digitální identita je širokým a atraktivním cílem, na který se dají provádět útoky. Je mnoho možností, jak může být útočníky zneužita tato nastupující technologie. Útočníci mají nejrůznější motivace, proč provádí svůj útok. Od prostého škození, získání dobrého pocitu z podařeného útoku, přes získání peněz, poškození dobrého jména, získání know-how či konkurenční výhody, strategických plánů a informací, až po vedení hybridní války státními aktéry.

5.1 Klasifikace kybernetických hrozeb

Kybernetické hrozby mohou být klasifikovány dle několika kritérií:

- **Cíle útoku** – útočník se může zaměřit na zprostředkovatele digitální, respektive bankovní identity a zkusit využít zranitelnosti v zabezpečení systému; nebo se zaměřit na uživatele, respektive majitele digitální identity a snažit se přes něj dostat různými způsoby k jeho citlivým údajům.
- **Vektoru útoku –** jinými slovy to jsou způsoby, jakou cestou proniknout do cílového systému (např. emailem, pomocí přenosného média (převážně USB flash disků), přímo/bezdrátově, útokem na dodavatelský řetězec nebo využitím sociálních sítí) [41].
- **Vyspělosti útočníka –** po světě existuje celé spektrum útočníků, jejichž znalosti a finanční možnosti se extrémně liší. Níže jsou vyjmenované některé typy útočníků:
  - ***Script kiddies***

    Jsou nejméně sofistikovanými útočníky. Využívají automatizované metody využívání zranitelností (tzv. „exploitace“) pomocí programů či automatizovaných skriptů jako je např. Metasploit, nejsou opatřeni finančními prostředky, ani velkými znalostmi. Dělají to pro zábavu, pro získávání znalostí apod., ale i tak mohou mít jejich útoky značné následky, protože automatizované programy/skripty jsou mocnými nástroji. Ovšem jejich šance na provedení útoku na banky či úřady jsou malé, větší pravděpodobnost mají pro útoky na jednotlivce pomocí phishingu apod.

  - ***Hacktivisté***

    Jsou sofistikovanější skupinou, jejich cílem je bojovat za své ideje a dehonestovat určité společnosti či státní instituce, se kterými nesouhlasí pomocí tzv. defacementu. Zpravidla jsou limitováni finančními prostředky, které jsou nutné pro podnikání složitějších útoků.

- ***Státní aktéři***
  Tato skupina je nejvíce sofistikovanými útočníky, jsou to zpravidla státem financované skupiny hackerů. Cílem takových skupin je plnit úkoly zadané vládou daného státu, jenž spočívají v poškození jejich nepřátel (ostatních států, organizací či jednotlivců). Jsou považováni za největší hrozbu, jelikož mají největší finanční prostředky a jsou složeni z velmi schopných bezpečnostních expertů. Tyto skupiny mají největší pravděpodobnost úspěchu pro provedení útoku na systémy bank, státních úřadů či uživatele digitální identity.

5.2 Advanced persistent threat

Neboli APT je označován cílený dlouhotrvající útok prováděný zejména státními aktéry, při kterém se útočník snaží nenápadně vyhledat a zneužít jakoukoli zranitelnost, díky které by se mohl dostat do systému. Po infikování systému je do něj umístěn tzv. RAT (Remote Access Trojan), což je malware, který pro útočníka vytváří tunely a zadní vrátka (tzv. „backdoory“), díky nimž je umožněn vzdálený přístup a nepozorovaný pohyb po napadeném systému. Pak jsou nenápadně prováděny akce uvnitř systému, včetně průzkumu nebo odesílání žádoucích dat v malých objemech. Velmi důležité je zůstat nezpozorován, případná kompromitace či finalizace útoku může být provedena až roky po průniku do systému [42]. Na webu MITRE ATT&CK lze nahlédnout na seznam jednotlivých APT skupin [43].

5.3 Threat hunting

APT jsou obtížně zachytitelné, největší šanci na zachycení mají oběti v době průniku, poté je již jen velice obtížné v rámci běžného monitoringu sítě. V této situaci přichází vhod tzv. threat hunting. Tato obranná technika je metodou proaktivního vyhledávání hrozeb ve vlastní síti. Při využívání threat hunting se předpokládá, že je síť již kompromitována a vyhledávají se určité znaky kompromitace, které splňují hypotézu, která se definuje na začátku prohledávání. Valná část výsledků je negativní (např. se zvolí nevhodná hypotéza nebo síť není napadena). Tato metoda je mnohem nákladnější než jiné typy obrany, proto se využívá jen u velkých nadnárodních korporací, které si to mohou finančně dovolit. Jde o relativně nový typ obrany, jehož plný potenciál ještě není naplněn.

5.4 Rizika technologie digitální identity

5.4.1 Únik citlivých osobních údajů

V případě digitálních identit, které jsou lidmi vytvořeny na různých sociálních sítích typu Facebook, Twitter apod., občas dochází po útocích hackerů k únikům dat uživatelů, která jsou zpravidla přeprodávána na internetu či darknetu. Například, poslední velký únik uživatelských dat z Facebooku se stal letos, kdy byla ukradena osobní data (jména, telefonní čísla, Facebook ID, data narození, lokace uživatelů aj.) 533 milionů uživatelů [44]. Následně byla zveřejněna na hackerském fóru, kde byla dostupná komukoli.

Digitální identity na sociálních sítích naštěstí neobsahují tak citlivé údaje, které by při ztrátě, ve většině případů, ohrozily oběť velkou měrou. To ovšem neplatí pro únik dat z identity poskytované státem. Ta obsahuje nejcitlivější údaje včetně zdravotních údajů, biometrických prvků, dat spojených s komunikací s úřady, bankami atd.

Evropská unie si již několik let zpět uvědomila důležitost ochrany fyzických osob při zpracování osobních údajů a práva jedince se svými údaji nakládat podle vlastního uvážení, proto bylo vydáno Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), známé pod zkratkou GDPR [45]. To zadává správcům a zpracovatelům osobních údajů povinnosti zavést různá opatření za účelem souladu s nařízením GDPR. Jako výstražný prvek byly zavedeny astronomické sankce za porušení tohoto nařízení.

5.4.2 Krádež identity

Největším rizikem spojeným s digitální identitou je její zcizení, potažmo její části. Krádež je útočníkem vykonávána zpravidla podvodem za účelem dosažení finančního či jiného prospěchu nebo z důvodu poškození dobrého jména. Z internetu je viditelná pouze dig. id. uživatele, proto se při odcizení může zloděj vydávat za svou oběť, aniž by si toho ostatní uživatelé nebo poskytovatelé všimli. Zejména v případě sociálních sítí, kdy útočník nemůže získat přihlašovací údaje k účtu, se může vydat cestou vyhledávání a stahování veřejně dostupných informací a následně založení duplicitního účtu, pomocí kterého se vydává za oběť.

Za podmínky, že je zcizena dig. id. poskytovaná státem nebo bankovní identita, tak je to mnohem větším rizikem než při krádeži dig. id. například ze sociálních sítí. Útočník má nesrovnatelně větší pravomoci a možnosti, jak zneužít tohoto činu. V případě zcizení všech faktorů má útočník plný přístup ke všem údajům a funkcím identity. Jakmile se oběť dozví o zneužití její identity, je nutné bezprostředně kontaktovat poskytovatele své digitální identity.

5.4.3 Kyberšikana

Tímto termínem se označuje skupina forem šikany, které jsou prováděny prostřednictvím informačních a komunikačních technologií, zejména skrze internet a mobilní sítě, při kterých jsou využívány elektronická zařízení jako mobilní telefony, tablety, počítače atd. Aktéry kyberšikany jsou oběť–útočník–publikum. Mezi projevy kyberšikany se řadí vydírání, zastrašování, obtěžování, ponižování, provokování, krádeže identity, sexting, kybergrooming apod.

S normální šikanou sdílí stejný cíl, ale v některých vlastnostech se liší. Například ve velmi časté anonymitě útočníka, který se skrývá za falešnými účty na sociálních sítích, používá jednorázová uživatelská jména a e-mailové adresy apod. Také profil útočníka nebývá stejný jako v klasické šikaně, útočník nemusí být starší, silnější atd., tyto rozdíly se na internetu mažou a záleží na umu a znalostech útočníka. Dalším odlišným prvkem je obtížnost předpokladu pro místo a čas útoku. Publikum pomáhá útoku, jelikož se získaná osobní data, zprávy, videa apod. po publikaci příspěvku sdílejí a amplifikují dopad kyberšikany [46].

Kyberšikana se projevuje především psychologickými účinky, které ovšem mohou s rostoucí závažností útoků přejít i do fyzické roviny. V dnešní době jsou s ní stejně jako s klasickou šikanou nejvíce konfrontovány děti a mladiství, ale s různými formami kyberšikany se potýkají i dospělé osoby (např. sexting, kyberstalking, vyhrožování atd.). V případě, že se jedinec potýká s dopady kyberšikany nebo ví o osobě, která se s ní potýká, pak je doporučováno kontaktovat Policii ČR.

5.4.4 Centralizace osobních údajů

S nasazením elektronické identity se shromažďuje více dat, která jsou jednoznačně přiřazena k majiteli identity, protože je propojeno více služeb pro jeden typ přihlášení. To jde kontradiktorně s doporučeními pro zmenšování své digitální stopy. Proto lidé, jenž lpí na svém soukromí na internetu, které je v tomto prostředí poněkud chimérou, mohou mít problém s přijetím elektronické identity. Mohou mít pocit, že o nich jejich banka, stát či korporace vědí příliš mnoho informací. Také může panovat obava z dopadu útoků, které mohou způsobit masivní úniky velmi citlivých dat. S přetrvávajícím tempem přesunu fyzických služeb na internet lze ovšem předpokládat, že bude digitální stopa uživatele internetu nadále růst.

Zajímavou diplomovou prací zabývající se analýzou sběru informací o uživateli společností Google s názvem Digitální identita v době služeb Google se zaobíral Jakub Skoček [47]. Pro běžného uživatele může být tato práce zajímavým a překvapivým vhledem do toho, jak a co již v roce 2015 monitorovaly služby poskytované společností Google.

5.5 Útoky na poskytovatele služby

Jak lze usoudit z dosavadní minulosti, v budoucnu se budou nadále objevovat útoky na společnosti či státy, jež poskytují určité formy elektronické identity. V roce 2021 je dle AV-Test Institute registrováno každý měsíc přes 17 milionů nových instancí malware [48]. Dá se předpokládat, že tento počet bude do budoucna růst ještě rychleji. Proto musí firmy kontinuálně vynakládat peníze a úsilí, aby těmto hrozbám stíhaly čelit.

Následně budou uvedeny příklady útoků, se kterými se mohou poskytovatelé potýkat. Útoky jako sociální inženýrství, viry, červi, trojské koně apod., se mohou vyskytnout i u poskytovatele služby, ale aby se neopakovaly dvakrát, tak jsou zmíněny jen v podkapitole útoků na uživatele služby.

V případě bankovní identity, poskytovatelé bank mají své technologie, na kterých běží bankovní služby, zabezpečeny největším možným způsobem. Proto se dá očekávat, že útok na jimi poskytovanou bankovní identitu bude méně pravděpodobný a technicky náročný, protože disponují nemalým množstvím peněz, za které si mohou dovolit nejnovější technologie a zaměstnat řadu technických, bezpečnostních či síťových expertů, jejichž úkolem udržovat bezpečný stav těchto systémů. Technicky mnohem méně náročným je útok na uživatele, respektive majitele digitální identity.

5.5.1 Ransomware

Je škodlivý kód, který po infikování zařízení zašifruje jeho obsah. Nebývá konkrétně cílen, je vypuštěn do internetu jeho cílem je infikovat jakékoli zařízení, ke kterému se dostane. Využívá se k vydírání oběti za účelem získání finančního obnosu. Po zašifrování se objeví na obrazovce žádost o zaplacení, velmi často v kryptoměnách, po které má být oběti odeslán klíč k dešifrování dat. Obecným doporučením je neplatit požadovanou částku. V případě napadení ransomwarem lze na stránce nomoreransom.org najít dešifrovací programy pro desítky druhů ransomware [49].

5.5.2 Zero-day exploit

Neboli útok nultého dne, je typ hrozby využívající zranitelnosti, která byla objevena black-hat hackery, ale ještě nebyla objevena vývojáři, takže na ni nemohla být vydána záplata opravující zranitelnost napadeného hardware nebo software. I po vydání záplaty bývá exploit aktuální po dlouhou dobu, jelikož část uživatelů napadeného HW/SW si není vědoma této hrozby a neaktualizují svoje zařízení.

5.5.3 Denial of Service (DoS)

Denial of Service, v českém překladu odepření služby, je typem útoku, který má za cíl zapříčinit nedostupnost služby poskytované uživatelům. Využívá toho zahlcením serveru či zneužitím chyby, po které je server nefunkční. Variantou DoS je útok zvaný „Distributed Denial of Service (DDoS)“, který využívá obrovské množství počítačů, jež posílají dotazy na jednotlivé cíle. Tato varianta útoku je mnohem efektivnější, může pro ni být použita síť na dálku ovládaných napadených počítačů, která je nazývána termínem botnet.

5.5.4 Příklad zranitelnosti estonských eID karet

V roce 2017 byla českým výzkumníkem Petrem Švendou a jeho týmem z Masarykovy univerzity objevena zranitelnost pojmenovaná ROCA (Return of Coppersmith’s Attack) v čipech německého výrobce Infineon Technologies. Konkrétně chyba algoritmu v knihovně Infineon RSALib, kvůli které se generovaly nedostatečně náhodné RSA klíče, takže bylo teoreticky možné vypočítat soukromý klíč ze znalosti veřejného klíče.

Obrázek 5.1: Oblasti ovlivněné zranitelnou knihovnou RSALib [50]

To bylo způsobeno vzorcem pro generování prvočísel

$$p = \mathrm{k} * \mathrm{M} + \left(65537^{\mathrm{a} \bmod \mathrm{M}}\right), \tag{5.1}$$

kde p je generované prvočíslo, k a a jsou neznámá celá čísla při lámání a M je násobkem prvních n vygenerovaných prvočísel [50],[51].

Tento vzorec byl bez znalosti zdrojového kódu odvozen českými vědci, kteří našli zranitelnost právě v malých hodnotách čísel k a a. Knihovna RSALib používala výchozí set předdefinovaných prvočísel, ze kterých vždy vybírala určitý počet (hodnota záležela na velikosti RSA klíčů) namísto náhodně generovaných prvočísel, což bylo znatelné oslabení. To dohromady významně snižuje entropii náhodně vygenerovaného prvočísla. Pro 512bitové klíče se počet dostupných prvočísel snížil z 2^{256} na 2^{99} [51].

Tento objev způsobil, že všech 800 tisíc estonských eID karet vydaných po roce 2014 bylo ohroženo potenciální krádeží citlivých osobních údajů. Bylo zjištěno, že se problematické čipy nacházely v nemalém počtu elektronických technologií i geografických oblastí (Obrázek 5.1), třeba i ve slovenských a španělských občanských průkazech. V Estonsku vyměnili způsob generování a používání bezpečnostních klíčů. Na Slovensku používají stejné klíče, jen s větší délkou, což prakticky znemožňuje v dnešní době provést útok na čipy jejich občanských průkazů [51],[52],[53]. Obrázek 5.1 byl přeložen z anglického jazyka do českého s výslovným souhlasem autora.

5.6 Útoky na uživatele služby

Potenciálních útoků, které útočníci využívají pro dosažení svých cílů, je nespočet. V této části budou zmíněny jen ty, se kterými se mohou jedinci vlastnící digitální identitu v případě útoku pravděpodobně setkat.

5.6.1 Sociální inženýrství

Je souborem technik, které útočník používá za účelem manipulace s lidmi, aby zjistil jím kýžené informace nebo nenápadně donutil oběť k požadovanému úkonu. K provedení jsou např. využívány lživé informace, emoce či nátlak na oběť. Níže jsou uvedeny příklady metod, které mohou být využívány při útoku [54]:

- **Phishing** – podvodná technika, při které útočník láká oběť, aby vyzradila své citlivé údaje (uživatelská jména, hesla, čísla kreditní karty, PIN apod.) pomocí nevyžádaných zpráv nebo e-mailů. Útočníci vytváří falešné e-maily, zprávy, internetové platební portály, webové stránky atd., které mají přesvědčit oběť, že jsou legitimní [55]. Variantou phishingu je tzv. „spear phishing“, který je přesně zacílen na danou osobu a pro ni je specifikován, aby působil co nejvěrněji.
- **Vishing** – telefonická varianta phishingu, opět má za cíl podvést oběť a neoprávněně získat její peníze nebo osobní údaje.

- **Pretexting** – metoda, při které útočník vytváří smyšlený příběh za účelem vymámení určité informace či vykonání akce obětí. V jeho smyšleném příběhu se snoubí určitá lež s částí pravdivé informace, kterou získal útočník nějakým způsobem už dříve.
- **Watering hole** – technika, při které útočník buď náhodou, nebo po získání klíčové informace zjistí, jaké webové stránky, např. zaměstnanci firmy, často navštěvují. Do zdrojového kódu špatně zabezpečené stránky je útočníkem vložen škodlivý kód, který přesměruje oběti na jím vytvořenou stránku. Tato stránka často vypadá identicky, ale po kliknutí na nějaký prvek je spuštěn malware a počítač oběti kompromitován.
- **Baiting** – metoda, jenž využívá zvědavosti oběti, která nalezne na veřejném prostranství „zapomenuté“ CD či flash disk. Oběť ovšem neví, že se na přenosném úložišti nachází malware. Oběť ho připojí ke svému elektronickému zařízení, následně vidí soubor, který je velmi často pojmenován takovou formou, aby název škodlivého souboru vyvolal v oběti zvědavost a donutil ji ho otevřít.

5.6.2 Počítačový virus

Počítačový virus je program navržený tak, aby se byl schopen šířit a spustit na infikovaném zařízení i bez uživatelova vědomí. Je analogií biologického viru, protože má stejné vlastnosti své existence. Aby se mohl šířit, tak využívá jiné soubory jako své hostitele, ve kterých se replikuje a dále přenáší. Jeho cílem je se množit a vykonávat škodlivé akce na počítači oběti.

5.6.3 Počítačový červ

Červi jsou typem virů, které se ovšem dokážou šířit samovolně po síti a posílat své repliky na jiné hostitelské stanice. Po infikování počítače se zmocní prostředků dedikovaných pro síťovou komunikaci a dále se šíří. Krom schopnosti šíření mají i další schopnost, a to nést tzv. payload (škodlivý kód, který má za cíl vykonat danou akci), který má za cíl jím daným způsobem poškodit uživatelův počítač.

5.6.4 Spyware

Druh špionážního software, jenž běží na pozadí počítače a sbírá informace o oběti, které jsou následně odesílány do vzdálené stanice útočníka. Bývá často součástí různých volně šiřitelných programů společně s adware. Pomocí těchto programů mohou být sbírány a odesílány osobní údaje pro personalizaci reklam, ale i hesel atd.

5.6.5 Keylogger

Je útočníky zneužívaný hardware nebo software, který zaznamenává stlačení kláves na klávesnici. Je používán za účelem snímání hesel nebo čísel platebních karet oběti a využití těchto údajů k jejich následnému zneužití.

5.6.6 Man-in-the-Middle

Je množinou útoků, které mají společnou vlastnost, a tou je, že se útočník nachází uprostřed komunikačního kanálu mezi uživateli A a B, resp. přesměrovává provoz a zachytává jejich komunikaci. Pro příklad lze uvést útoky jako ARP/IP/DNS Spoofing, Session Hijacking, SSL Stripping atd.

5.7 Eliminace hrozeb z pohledu uživatele služby

Je na místě tu uvést parafrázi známé rčení z oblasti kyberbezpečnosti, a to, že největší zranitelnost celého systému se nachází mezi židlí a počítačem. Tohle rčení platilo, platí a zřejmě bude dále do budoucna platit. Proto by se mělo trvat na konzistentní edukaci společnosti za účelem vyššího povědomí o hrozbách, kterým je uživatel internetu vystaven, a způsobu obrany proti nim. To by v důsledku vedlo obecně zvýšení bezpečnosti uživatelů a jejich zařízení, v kontextu této práce ke snížení počtu zneužití osobních údajů, podvodů, krádeží identit, peněz apod. Možností, jak by měl uživatel eliminovat hrozby, je hned několik.

První možností je snížit množství informací, které obsahuje jeho digitální stopa. Toho se dá docílit převážně pomocí informovanosti a prevence (např. používat více profilů, více přihlašovacích jmen a e-mailových adres, anonymní režim prohlížeče, jednou za čas vyhledat informace o své vlastní osobě pomocí tzv. „people search engine“, využívat VPN sítě či prohlížeče typu Tor, používat vyhledávače, které neukládají cookies a neprodávají data třetím stranám (např. Duckduckgo)).

Dále je možné přímo snížit úroveň rizika útoku. To opět zahrnuje informovanost a edukaci před typy útoku jako je sociální inženýrství, phishing, potažmo spear phishing, vishing, URL Redirection, útoky typu MitM apod. Pro přihlášení je nutné používat dostatečně dlouhá hesla s využitím malých a velkých písmen, čísel a speciálních znaků.

Třetí, poněkud triviální možností, je být prostě obezřetný a pozorný. V kontextu digitální identity, kupříkladu, mít heslo či PIN v hlavě a zálohu na bezpečném místě, nemít tyto údaje napsané někde, kde se k nim může dostat neoprávněná osoba, neztratit svůj mobilní telefon, používat kritické myšlení, být ve zdravé míře opatrný vůči podezřelým lidem, věcem, situacím atd.

5.8 Eliminace hrozeb z pohledu poskytovatele služby

Již v návrhu systému a architektury musí poskytovatel klást silný důraz na zajištění bezpečnosti, který ovšem musí být udržován i v rámci kontinuálního poskytování služby zákazníkům.

Z technického hlediska je zapotřebí smysluplně segmentovat síť, plánovat využití bezpečnostních prvků jako jsou DMZ (demilitarizované zóny), VLAN, firewallů, zajistit redundanci sítě pro zajištění dostupnosti služby. Tyto prvky musí být zajištěny i proti fyzickému přístupu, proti živelním pohromám, výpadkům elektrického proudu atd. Všechny síťové prvky je nutné správně a bezpečně nakonfigurovat, tomu se říká tzv. hardening. Samozřejmě je nutné pověřit přístupem jen povolané osoby. Dále je zapotřebí využívat verze protokolů umožňující šifrování, mít aktualizovaný firmware i software na všech zařízeních, dělat pravidelné skeny sítě pro rozpoznání zranitelností. Pro udržování bezpečného chodu služby a vyhledávání možných rizik je třeba využívat monitoringu sítě, např. pomocí systémů SIEM (Security Information and Event Management) pro analýzu logů či ve větších firmách využít výše zmíněný threat hunting atd.

Z procesního hlediska je vhodné mít sestavené plány pro analýzu rizik, krizové plány, také nastavit řízení přístupu osob, nastavit efektivní politiku hesel, rozdělit role pro udržování chodu systému, školit své zaměstnance, udržovat v průběhu poskytování služby tzv. „compliance“ (soulad s nastavenými pravidly ve firmě) apod.

6 TECHNICKÉ PROSTŘEDKY

6.1 Vícefázové ověření

Vícefázové ověření (vícefaktorové, angl. multi-factor authentication (MFA)) je způsobem, který zajišťuje přihlášení jedince do aplikace či na webovou stránku, při kterém jedinec poskytuje dva nebo více důkazů, resp. faktorů, které potvrzují jeho identitu.

Prvním faktorem je znalost (jedinec něco ví), druhým je vlastnictví (jedinec něco má) a třetím je charakteristika (jedinec je unikátně spjatý s nějakou vlastností).

Atributy jsou dalšími prvky, jenž doplňují posuzování identity při autentizaci či autorizaci jedince. Je několik kategorií atributů, které mohou být využity. Prvním atributem je poloha (jedinec někde je), druhým je schopnost akce (jedinec může něco udělat), ukázka (jedinec může něco ukázat) a známost (jedinec někoho zná).

MFA zvyšuje úroveň zabezpečení během autentizace, protože je pro útočníka mnohem složitější, když je nucen ukrást identifikační údaje ze dvou či více nezávislých autentizačních kanálů [56].

6.1.1 Typy autentizace

Dělení podle faktorů:

- **Znalost** – uživatelské jméno, heslo, PIN, doplňující otázky, rozpoznání zvolených obrázků apod.
- **Vlastnictví** – fyzický autentizační token (může být v podobě přístupové karty/čipu, USB token), průkaz totožnosti s čipem, platební karta, mobilní telefon, kartička s jednorázovými kódy, aplikace generující jednorázové kódy.
- **Charakteristika** – biologická biometrická vlastnost (otisk prstu, sken oční duhovky, rozpoznání obličeje, geometrie ruky, mapa žil v dlani, DNA aj.) či behaviorální biometrická vlastnost (hlas, dynamika psaní na klávesnici, dynamika podpisu, EEG, EKG atd.).

Dělení podle atributů:

- **Poloha** – IP adresa, GPS pozice, MAC adresa apod.
- **Schopnost akce** – schopnost zvládnout nějakou akci, jako vyřešení hádanky, tajné potřesení rukou, kliknutí na specifická místa na obrazovce, schopnost poznat, co je na obrázcích (využívá se v CAPTCHA).
- **Důkaz** – schopnost něco dokázat, co splňuje určité podmínky, které identifikují jedince či jeho připojení (např. zdali má jedinec nainstalované poslední aktualizace, zdali je schopen šifrovaného připojení atd.).
- **Známost** – jedinec je autentizován na základě toho, že je znám osobě, která provádí autentizaci (vrátný, bezpečnostní služba aj.).

Použití biometrických údajů je, kromě otisku prstu a rozpoznání obličeje, značně limitované v běžném prostředí, ve kterém je uživatel připojen k internetu. S ostatními formami použití biometrických údajů se není časté běžně setkat. Tyto systémy jsou využívány pro autentizaci při vstupech do míst, resp. k datům, kde je potřeba velmi vysoké úrovně zabezpečení.

Nejběžnějším způsobem, kterým se dnes využívá dvoufázová autentizace, je znalostí uživatelského jména a hesla, doplněná vlastnictvím mobilního telefonu, na který přijde SMS s jednorázovým kódem nebo použitím charakteristického rysu jedince, zejména otisku prstu.

6.2 X.509

Standard vytvořený za cílem definovat formát systémů veřejného klíče známé jako PKI, který se využívá pro elektronické podepisování, a specifikaci formy digitálních certifikátů. V dnešní době se využívá verze standardu X.509 v3, která je definovaná v dokumentu RFC 3280 [57].

Pro generování páru veřejného a soukromého klíče bývají využívány kupříkladu kryptografické algoritmy RSA, DSA, ECDSA či ElGamal. Přípony, jež se využívají pro certifikáty vytvořené dle tohoto standardu jsou např. .der, .p12 (.pfx), .p7b (p7c), .pem, z nichž každý má své náležitosti, třeba zdali obsahují certifikát samotný nebo certifikát společně se soukromým klíčem, typem kódování (Base64, ASCII či binární) apod.

Obecná struktura certifikátu vytvořeného dle standardu X.509 je následující:

- **Version**: verze certifikátu (X.509 v3).
- **Serial Number**: unikátní sériové číslo certifikátu.
- **Signature Algorithm**: identifikace typu algoritmu, který byl využit pro podepsání tohoto certifikátu.
- **Issuer**: informace o vydavateli (CA, jež vydala a podepsala certifikát).
- **Validity**: doba, po jakou je certifikát platný a validní.
- **Not Before**: neplatný před datem.
- **Not After**: neplatný po datu.
- **Subject**: pole identifikující vlastníka certifikátu (stát, organizace atd.).
- **Subject** Public Key Info: informace o veřejném klíči vlastníka.
- **Public Key Algorithm**: použitý algoritmus pro vytvoření veřejného klíče.
- **Public Key**: (data).
- **Subject/Issuer** Unique Identifier: unikátní identifikátor vlastníka/vydavatele certifikátu.
- **X.509 v3 extensions**: rozšíření, jež jsou volitelná (Subject Alternative Name, Certificate Policies atd.).
- **Signature Algorithm**: typ algoritmu, který již byl formulovaný výše pro generování veřejného klíče.
- **Certificate**: (samotný elektronický podpis).

6.3 Autentizační/autorizační protokoly

Protokoly zmíněné v této kapitole se velmi často využívají ve federativních systémech, kde poskytovatel identity (IdP) už disponuje identitou koncového uživatele. V případě, kdy se chce koncový uživatel přihlásit ke službě poskytovatele služby (SeP), může uživatel využít jíž vytvořeného účtu u poskytovatele identity. Poskytovatel identity ověřuje identitu koncového zákazníka uvnitř a zpátky posílá jen konkrétní údaje a potvrzení či zamítnutí.

6.3.1 OpenID Connect

Dále jen „OpenID“, je decentralizovaný open-source standard poskytující službu autentizace. Běží nad protokolem OAuth 2.0 (dále jen „OAuth“), jemuž poskytuje vrstvu autentizace, kterou samotný OAuth nemá. Formátem tokenů jsou digitálně podepsané JSON Web Tokeny (JWT), které zajišťují, že identifikační tokeny a přístupové tokeny nebyly pozměněny během výměny s ostatními účastníky komunikace.

Ve schématu OpenID figurují tři zúčastněné strany, a to poskytovatel služby (SeP), koncový uživatel a poskytovatel identity (IdP). Během procesu přihlášení se koncový uživatel chce přihlásit vůči SeP, ten ho přesměruje, aby se autentizoval u IdP a autorizoval přístup k údajům pro SeP. Poté IdP pošle autorizační kód pro SeP, který ho využije pro získání přístupového a identifikačního tokenu od IdP. Jakmile má SeP tokeny, může provádět úkony jménem koncového uživatele [58].

6.3.2 OAuth 2.0

Je open-source standardem a autorizačním protokolem. Jeho funkcí je posílání dotazů a odpovědí o přístup ke zdrojům webových API vzdálených služeb z webové stránky či aplikace běžící lokálně jménem uživatele. Pro dotazování jsou využívány přístupové tokeny, které mají z bezpečnostních důvodů expirační dobu. Častým formátem těchto tokenů je taktéž JSON Web Token [59].

Pro zjednodušení: Uživatelem (koncovým zákazníkem) využívaná aplikace (SeP, tj. poskytovatel služby) vyžaduje přihlášení. Nabízí ovšem přihlášení přes API nejmenované banky, kde už má uživatel vytvořenou identitu (IdP, tj. poskytovatel identity).

Po kliknutí na přihlášení pomocí banky IdP v aplikaci SeP nejdříve uživatel může potvrdit, zda povoluje autorizaci aplikaci SeP, aby o něm mohla získat dané údaje od banky IdP. Pak aplikace SeP požádá o autorizaci autorizační server banky IdP. Autorizační server IdP poté udělí tzv. „grant“ společně s autorizačním kódem, který bude využit v dalším kroku. Aplikace SeP pošle bance IdP autorizační kód z předešlého kroku, která mu na oplátku pošle přístupový token, který je potřeba pro přístup na server obsahující zdroje (v tomto případě potřebné osobní údaje o uživateli).

S tímto tokenem aplikace SeP žádá informace ze serveru, a zpět jsou již odeslány dotazované údaje [60].

Banka IdP neposkytuje žádné utajované informace jako heslo apod. aplikaci SeP, ověřování probíhá uvnitř banky IdP. Aplikace SeP totiž důvěřuje procesu ověřování API bankou IdP.

6.3.3 Security Assertion Markup Language (SAML)

Je open-source standardem, jehož cílem je poskytovat mechanismus pro výměnu autentizačních a autorizačních dat mezi stranami SeP a IdP. SAML využívá pro komunikaci protokol HTTP a SOAP, jehož formátem je XML.

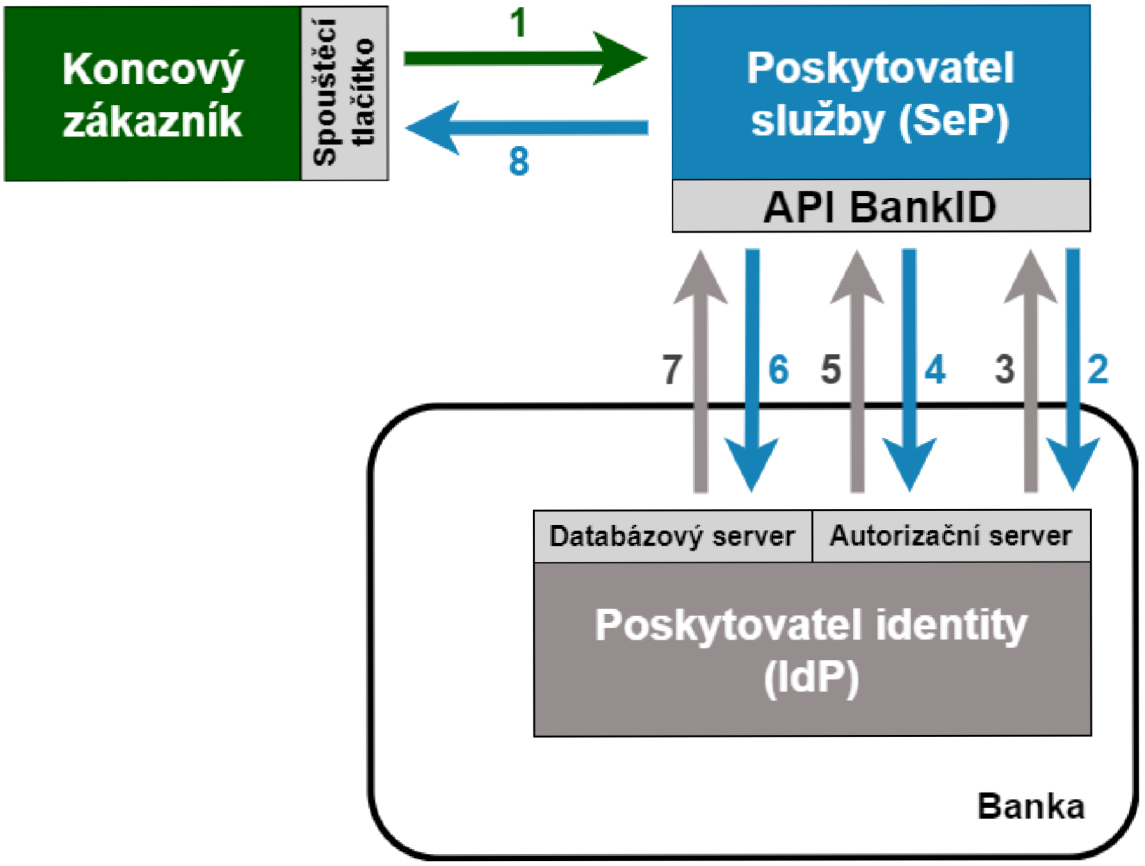
Koncový uživatel přistupuje obvykle pomocí webového prohlížeče ke zdrojům SeP. SeP pošle žádost o autentizaci k IdP přes webový prohlížeč. IdP může požádat koncového uživatele o poskytnutí jména a hesla. Po ověření identity uživatele IdP pošle k SeP tzv. „prosazení“ (angl. assertion) autentizace, společně s přihlašovacími údaji uživatele. Následně na základě zprávy od IdP SeP povolí nebo odmítne uživateli udělit přístup ke zdrojům SeP [58],[61].

6.3.4 Porovnání protokolů

OpenID je autentizační protokol, zatímco OAuth je protokol zajišťující autorizaci. Protokoly OpenID a OAuth jsou velmi blízce provázané a zpravidla využívané společně. OpenID je vrstva identity nad OAuth, jenž zlepšuje zabezpečení a nabízí funkce jako správu a zjišťování relací. SAML je nezávislý na OAuth, na rozdíl od OpenID. OpenID i SAML poskytují prostředky pro federovanou autentizaci. SAML využívá pro autentizační zprávy formát XML SAML, zatímco OpenID užívá JWT formát. SAML je využíván častěji interně ve velkých firmách, kdy pro přihlášení k mnoha firemním službám a zařízením stačí jen jedno heslo [58],[62].

6.4 BankID

BankID je prostředníkem mezi poskytovatelem služby (třetí stranou) a bankou koncového uživatele. Koncový uživatel se ověřuje vůči poskytovateli služby pomocí přihlášení do své banky. Poté poskytovatel služby získá ověřené a koncovým uživatelem schválené osobní údaje od jeho banky [27].



Obrázek 6.1: Schéma komunikace při ověřování koncového zákazníka

V následujících odrážkách je v osmi krocích stručně vypsaný postup komunikace mezi těmito protistranami:

- **Krok 1** – žádost o autentizaci,
- **Krok 2** – žádost o autorizaci,
- **Krok 3** – autorizační „grant“ + autorizační kód,
- **Krok 4** – autorizační kód,
- **Krok 5** – přístupový token,
- **Krok 6** – žádost o dané údaje + přístupový token,
- **Krok 7** – poskytnuté údaje,
- **Krok 8** – dokončení autentizace.

V této aplikaci jsou využívána dvě rozhraní REST API, z čehož jedno využívají banky a jedno využívají poskytovatelé služeb. Jejich základem jsou standardy OpenID Connect a OAuth 2.0, popsané v kapitolách výše.

6.4.1 Bezpečnost

Služby CONNECT a IDENTIFY jsou velmi citlivé služby z bezpečnostního hlediska. Je nutné zajistit tzv. CIA triádu plus nepopiratelnost. Zabezpečení BankID je podrobeno stejným podmínkám jako pro zabezpečení bank, což značí velmi vysokou úroveň.

- **Důvěrnost** – jsou přenášeny a zprostředkovávány osobní údaje přes API.
- **Integrita** – při přenosu mezi zákazníkovým API a bankou musí zůstat osobní data nezměněna.
- **Dostupnost** – v případě využití kritickou infrastrukturou musí být zachována dostupnost tohoto systému.
- **Nepopiratelnost** – v případě nesprávných a neodpovídajících údajů hrozní právní následky, takže si zákazník musí být jist, že to co přijímá, je opravdu od banky [63].

6.4.2 Kryptografické algoritmy

Pro hashovací funkce nesmí být použity funkce MD5 a SHA1, protože u nich již byly nalezeny kolize. Je tedy v pořádku používat funkce např. SHA256, SHA3 apod.

U šifrovacích algoritmů je výběr trochu omezenější, nesmí být použity šifry RC4 a DES. Pro RSA musí být délka klíče alespoň 3072 bitů, pro ECDSA alespoň 256 bitů [63].

6.4.3 Možné technické vektory útoku na BankID

Dá se předpokládat, že aplikace BankID je a bude vystavena řadě kybernetických útoků, které budou mít za cíl krádež osobních údajů, nefunkčnost aplikace apod. Proti řadě běžných útoků by měla být aplikace odolná. Některé možné vektory útoku a způsoby jejich eliminace jsou uvedeny níže:

- **Kompromitace soukromých klíčů –** prozrazení soukromých klíčů by umožnilo útočníkovi se vydávat za jejich majitele. Eliminací této hrozby je například u PKI revokace certifikátu a změna JWK šifrovacích klíčů.
- **CSRF útoky na /auth klienta** – Při útoku s názvem Cross-site request forgery útočník vynutí odeslání požadavku od autentizovaného klienta na webový server, který uživatel nezamýšlel. To může vést k úniku citlivých dat, změnám relace nebo ke neoprávněným změnám spojenými s účtem oběti. V tomto případě je eliminace dosažena tím, že autentizace a autorizace probíhá na straně serveru.

- **Útok přehráním relace (Replay attack)** – cílem tohoto útoku je zachycení informací mezi legitimními stranami komunikace (řadí se do útoků typu MitM) a pozměnění či přehrání informací a odeslání legitimnímu příjemci, který si myslí, že přijatá data odeslala legitimní strana. Způsob eliminace tohoto útoku spočívá v použití tzv. „nonce“ parametru v těle dotazu. To je náhodně vygenerované číslo, které zabraňuje zopakování zprávy či předvídání následující zprávy [63].

6.5 Prostředky pro bezpečnou autentizaci

Pro autentizaci jsou používány různé prostředky, které si může uživatel vybrat dle vlastního uvážení. Například v České spořitelně jsou využívány metody jako klíč mobilní aplikace, heslo a jednorázový autentizační kód v SMS zprávě a při volání do kontaktního centra je nastaveno ověření hlasem, kdy se nahraje vzorek hlasu a při dalším volání se hlas klienta porovnává s nahraným vzorkem [64]. Níže jsou rozebrány jednotlivé formy přihlášení.

6.5.1 Softwarový klíč

Je metoda pro přihlašování a potvrzování platebních příkazů. Je ve formě aplikace na mobilním telefonu, která se v rámci dodržení bezpečností musí stahovat z oficiální obchodů, jako Google Play pro telefony s operačním systémem Android, či App Store pro telefony s operačním systémem iOS. V dnešní době má většina bank svou mobilní aplikaci fungující jako klíč. Při potvrzování plateb nebo autentizaci se využívá buď znalostní faktor (heslo, PIN) nebo v případě, že to uživatel povolil, tak biometrie (zpravidla otisk prstu).

6.5.2 Heslo

Tajná kombinace znaků sloužící k autentizaci uživatele. V dnešní době je doporučováno heslo alespoň o 12 znacích s využitím malých a velkých písmen, čísel i speciálních znaků. Takové heslo by mělo být relativně bezpečné vůči útokům hrubou silou. Nicméně, PIN kódy bývají kombinací zpravidla čtyři nebo 6 čísel, což by bylo pro útoky hrubou silou vyřešitelné v rámci milisekund. Proto bývají pro PIN kódy a jiná hesla nastavené limity počtu přihlášení, po kterých je možnost autentizace zablokována.

6.5.3 Certifikát

Bližší popis technologie certifikátu je obsažen v kapitolách 1 a 6.2. Certifikát může být např. uložen na čipové kartě nebo v počítači, na kterém je nainstalován operační systém Windows, ve správci certifikátu.

6.5.4 Jednorázové heslo

Neboli „One-time password (OTP)“. Je to dynamicky měnící se heslo, konkrétní vygenerované heslo je použitelné jen jednou. Aby mohla být hesla vygenerována, musí být využity algoritmy, které obsahují generátor náhodných nebo pseudonáhodných čísel, tím je zajištěna nepředvídatelnost vygenerovaných hesel. Tento mechanismus znemožňuje opakované použití kompromitovaného hesla při jeho odposlechnutí.

Základních principů pro generování hesel je více, buď využívají řetězení hashovacích funkcí, které generují hesla na základě přechozích hesel, nebo na základě výzva-odpověď mechanismu. V dalším mechanismu je využívána časová synchronizace serveru a klienta, při kterých se vytváří heslo platné jen po krátkou dobu (např. v softwarových aplikaci jako je Google Authenticator a mnoha jiných). Dalšími používanými variantami jsou kódy doručené přes SMS, které jsou generovány na straně serveru a přes celulární síť jsou doručeny ke klientovi.

6.5.5 Hardwarový token

Dělí se na prostředky obsahující čip a hardwarové bezpečnostní moduly (HSM). Uvnitř čipových karet se nachází integrovaný obvod, který může přijímat a zpracovávat data, který jsou na něj odeslaná a následně může posílat odpověď. Jsou karty kontaktní (s kontaktní ploškou) nebo bezdrátové (obsahují RFID obvod obsahující kondenzátor, který je nabit v blízkosti daného magnetického pole, poté je schopen odesílat odpovědi na terminál).

Moduly HSM jsou přenosná fyzická zařízení obsahující zabezpečené kryptoprocesory a kryptografické klíče, které mají funkci šifrování, dešifrování a samozřejmě jsou také schopny výkonu dalších kryptografických funkcí. Do této kategorie spadají i tzv. „Trusted Platform Module (TPM)“ čip, což je zabezpečený kryptoprocesor integrovaný uvnitř nějakého zařízení.

7 WEBOVÁ APLIKACE

V praktickém výstupu této bakalářské práce byla vytvořena webová aplikace, která popisuje problematiku digitální identity, jejího aktuálního stavu a používání ve státním sektoru i komerční sféře a shrnutí získaných informací, které jsou k tomu relevantní. Účelem stránky je, aby sloužila jako studijní materiál, a to převážně pro studenty, ale vzhledem k veřejné dostupnosti může posloužit i části veřejnosti, kterou bude toto téma zajímat. V semestrální práci, na kterou navazuje tato bakalářská práce, byl vypracován návrh této webové aplikace.

Vytvoření webové stránky bylo dosaženo pomocí bezplatného nástroje pro vytváření stránek Google Sites. Ten nabízí uživatelsky přívětivé prostředí s řadou funkcí a možnosti pro vytvoření designově podařených stránek. Obrázky byly vytvořeny buď mnou, anebo pocházejí z databází obrázků pixabay.com, freepik.com či istockphoto.com. Tyto databáze obsahují obrázky s volnou licencí nebo s podmínkou uvedení autora. Pro vytváření obrázků a diagramů byla využita open-source webová aplikace diagrams.net.

Webová aplikace obsahuje strukturální rozdělení podobné bakalářské práci, jelikož zde byly využity informace získané při jejím zpracování.

Konkrétní struktura je uvedena níže:

- **Úvodní strana** – po srolování dolů obsahuje základní členění webové aplikace s krátkým popisem ve formě otázek pro vzbuzení zájmu (jako pojmy a definice, digitální identita, e-identita, bankovní identita, bezpečnostní hrozby).
- **Pojmy a definice** – tato strana obsahuje vysvětlení základních pojmů, které se vyskytují na webové stránce, aby nezasvěceným návštěvníkům zlepšily porozumění. Ve spodní části strany se nachází podstránka o legislativě, která je spjatá s tématem digitální identity.
- **Digitální identita** – vysvětlení pojmů digitální identita a digitální stopa, obsahuje podstránky, které pojednávají o využití dig. id., a to ve státní správě, komerčním sektoru a také jak je to s nastávající evropskou digitální identitou a státy, které již před příchodem EDI využívaly dig. id.
- **E-identita** – zde se nachází podstránky o identifikačních prostředcích, které jsou i nejsou definovány zákonem.
- **Bankovní identita** – tato část obsahuje popis bankovní identity, její strukturu, zde využívané protokoly, a její funkce.
- **Bezpečnostní hrozby** – dělení této sekce je na 4 podstránky (klasifikace, rizika, útoky, eliminace) a všechny rozebírají bezpečnostní hrozby z jiného úhlu pohledu.

Webová aplikace je veřejně dostupná z internetu přes tento odkaz:
https://sites.google.com/vutbr.cz/digitalni-identita

ZÁVĚR

Cílem bakalářské práce bylo zmapovat současný stav využívání digitální identity osob ve státním i soukromém sektoru, vysvětlit pojmy související s touto oblastí, popsat technické prostředky, jenž zajišťují chod těchto systémů a objasnit bezpečnostní hrozby, které se pojí s využíváním této technologie a uvést možnosti eliminace. Práce je koncipována tak, aby čtenáři poskytnula minimálně základní vhled do problematiky digitální identity a oblastí s ní spojených. Detailní zkoumání jednotlivých částí je možné dále díky uvedeným zdrojům.

Elektronická identita poskytuje mnoho výhod a úspory času i peněz. Přeci jen, zavedení nové technologie bývá finančně náročné, ovšem úspory tím zajištěné časem rostou. Nasazení elektronické identity ve státní správě je relativně nová věc, situace se často mění, například při změně e-identity na Identitu občana. Dá se předpokládat, že vzhledem k nárustu digitalizace státní správy a kontinuálního pronikání ICT systémů do lidských životů, budou lidé využívat více a více výhody této technologie. Státu to ušetří peníze, protože tím odpadnou fyzicky vykonávané byrokratické procedury na úřadech a lidem především jejich čas. V nadcházejících letech s tímto stavem ještě zamíchá Evropská digitální identita, jejímiž ambicemi je sjednotit formu všech národních elektronických identit a rozšířit ji mezi více občanů. Situace ohledně bankovní identity se také neustále mění, protože v Česku je to nová technologie, která se teprve zapracovává a ještě se nedočkala plného nasazení. Také zde se dá předpokládat, že postupem času se budou počty bank a jiných komerčních subjektů zvětšovat, stejně jako počty aktivních uživatelů BankID. Výhodou BankID je jeho jednoduchost pro pořízení. Většina dospělé populace již má svoje bankovní konto, při jehož otevření byly ověřeny osobní údaje jedince, takže není nutné ji ověřovat znova, jako u jiných možností identifikace. Konkurence mezi jednotlivými poskytovateli je vysoká, to může do budoucna zapříčinit zlepšování těchto služeb (stát se může rozhodnout hradit občanům čtečky pro eObčanky).

Vzhledem ke stále narůstají aktivitě lidí na internetu přibývá i útočníků, kteří mají za cíl získat finanční či informační výhodu nebo někoho poškodit. Sofistikovanost jejich útoků roste kontinuálně. Je nutné zabezpečit osobní údaje spojené s identitami ve všech směrech. Instituce musí zabezpečit data jejich uživatelů po technické stránce, bohužel to není dostačující, protože je v dnešní době jednodušší se zacílit na uživatele, jelikož řada z nich nemá to potřebně povědomí o bezpečném fungování na internetu. Proto je nutné edukovat co největší množství lidí o tzv. „internetové hygieně“, aby se tím eliminoval počet úspěšných útoků.

Některé informace, které se pojí se zabezpečením bankovní identity ze strany bank z technického hlediska, nebylo možné dohledat. Banky si střeží tento typ informací v rámci zajištění bezpečnosti a na své stránky poskytují jen zevrubné a obecné informace. I přes dostupnost části technické dokumentace nebylo možné dohledat více informací spojených s technickou stránkou bankovní identity. Dokumentace byla převážně míněna pro poskytovatele služby a jejich propojení s BankID skrze API.

Z informací, které byly zjištěny během zpracování bakalářské práce, byla vytvořena webová aplikace, jejímž primárním účelem je sloužit jako výukový materiál. Stránka je pro zlepšení porozumění doplněna obrázky a názornými schématy. Cíle uvedené v zadání práce se dle mne nakonec podařilo naplnit.

LITERATURA

[1] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2. aktualizované vydání. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

[2] SMETRIC2016. Soft Certificate vs Hardware based Certificates. Secure Metric Berhad [online]. Kuala Lumpur: Secure Metric Berhad, c2021 [cit. 2021-12-05]. Dostupné z: https://www.securemetric.com/article/2011/soft-certificate-vs-hardware-based-certificates/

[3] SARISOVÁ, Kristina a Ondřej NOVÁK. Identita (psychologie). Wikisofia [online]. Praha: Univerzita Karlova v Praze, Filozofická fakulta, c2013, 12. 11. 2013 [cit. 2021-11-24]. Dostupné z: https://wikisofia.cz/wiki/Identita_(psychologie)

[4] ITU-T X. 1252. Baseline identity management terms and definitions. 2.0. Ženeva, Švýcarsko: ITU-T, 04/2021 n. l.

[5] Zákon o elektronických komunikacích a o změně některých souvisejících zákonů. In: Sbírka zákonů. Praha: Poslanecká sněmovna ČR, 2005, ročník 2005, částka 43, číslo 127. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-127

[6] NAKIT [NÁRODNÍ AGENTURA PRO KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE], MV ČR [MINISTERSTVO VNITRA ČESKÉ REPUBLIKY], ČESKÁ POBOČKA AFCEA [ARMED FORCES COMMUNICATIONS & ELECTRONICS ASSOCIATION], ET AL. Doporučení pro bezpečné nakládání s Identitou občana [online]. Praha: NAKIT, 2021 [cit. 2021-11-29]. Dostupné z: https://nakit.cz/pruvodce-svetem-elektronicke-identity/

[7] Národní identitní autorita [online]. [cit. 2022-05-13]. Dostupné z: https://archi.gov.cz/nap:nia

[8] Identita občana [online]. Praha: Správa základních registrů, c2022 [cit. 2022-04-28]. Dostupné z: https://info.identitaobcana.cz/

[9] ČESKÁ REPUBLIKA. Zákon o elektronické identifikaci. In: Sbírka zákonů. Praha: Poslanecká sněmovna, 2017, ročník 2017, částka 89, číslo 250. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-250#

[10] O nás. Správa základních registrů [online]. Praha: Správa základních registrů, c2022 [cit. 2022-05-13]. Dostupné z: https://www.szrcr.cz/cs/urad/o-nas

[11] Portál občana [online]. Praha: Ministerstvo vnitra, c2022 [cit. 2022-05-21]. Dostupné z: https://obcan.portal.gov.cz/prihlaseni

[12] Nařízení o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. In: Brusel: Evropský parlament a Rada EU, 2014, ročník 2014, číslo 910. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910&from=CS

[13] ČESKÁ REPUBLIKA. Zákon o službách vytvářejících důvěru pro elektronické transakce. In: Sbírka zákonů. Praha: Poslanecká sněmovna, 2016, ročník 2016, částka 115, číslo 297. Dostupné také z: https://www.zakonyprolidi.cz/cs/2016-297
[14] Seznam poskytovatelů služeb. Identita občana [online]. Praha: Správa základních registrů, c2022 [cit. 2022-04-30]. Dostupné z: https://info.identitaobcana.cz/sep/
[15] Kódy pro ochranu občanského průkazu. Identita občana [online]. Praha: Správa základních registrů, c2022 [cit. 2022-04-28]. Dostupné z: https://info.identitaobcana.cz/eop/OchranneKody.aspx
[16] Zprovoznění aplikací eObčanka na PC. Identita občana [online]. Praha: Správa základních registrů, c2022 [cit. 2022-05-25]. Dostupné z: https://info.identitaobcana.cz/eop/InstalacePC.aspx
[17] Overview of pre-notified and notified eID schemes under eIDAS. Oficiální internetová stránka Evropské unie [online]. Brusel: Evropská komise [cit. 2022-05-12]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[18] ČESKÁ REPUBLIKA. Zákon o elektronických úkonech a autorizované konverzi dokumentů. In: Sbírka zákonů. Praha: Poslanecká sněmovna, 2008, ročník 2008, částka 98, číslo 300. Dostupné také z: https://www.zakonyprolidi.cz/cs/2008-300
[19] ČESKÁ REPUBLIKA. Zákon daňový řád. In: Sbírka zákonů. Praha: Poslanecká sněmovna, 2009, ročník 2009, částka 87, číslo 280. Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-280
[20] Podmínky Daňové informační schránky plus. Portál MOJE daně [online]. Praha: Generální finanční ředitelství, c2020 [cit. 2022-05-20]. Dostupné z: https://adisspr.mfcr.cz/pmd/dokumentace/podminky-dis-plus
[21] Čipové karty Starcos. První certifikační autorita, a.s. [online]. Praha: První certifikační autorita, a.s. (I.CA) [cit. 2022-04-27]. Dostupné z: https://www.ica.cz/karta-vlastnosti
[22] MojeiD [online]. Praha: CZ.NIC, z. s. p. o., c2022 [cit. 2022-04-27]. Dostupné z: https://www.mojeid.cz/cs/
[23] Česká bankovní asociace [online]. Praha: ČBA, c2021 [cit. 2021-12-06]. Dostupné z: https://cbaonline.cz/
[24] Nejčastější dotazy. Bankovní identita [online]. Praha: Česká bankovní asociace, c2021 [cit. 2022-05-23]. Dostupné z: https://web.archive.org/web/20210615190307/https://bankovni-identita.cz/nejcastejsi-dotazy/
[25] Diagram rozdělení Bankovní identity. Bank iD [online]. Praha: BankID, c2021 [cit. 2022-5-20]. Dostupné z: https://web.archive.org/web/20211204051824/https://www.bankid.cz/en
[26] BankID [online]. Praha: Bankovní identita, c2022 [cit. 2022-05-27]. Dostupné z: https://www.bankid.cz

[27] BankID pro firmy. BankID [online]. Praha: Bankovní identita, c2022 [cit. 2022-05-20]. Dostupné z: https://www.bankid.cz/pro-firmy
[28] Zákon, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a některé další zákony. In: Sbírka zákonů. Praha: Poslanecká sněmovna ČR, 2020, ročník 2020, částka 22, číslo 49. Dostupné také z: https://www.zakonyprolidi.cz/cs/2020-49
[29] VÁCLAVÍK, Lukáš. Připravuje se Evropská digitální identita. Občanku i řidičák přesune do mobilu. Živě.cz [online]. Praha: CZECH NEWS CENTER, c2021, 4. června 2021 [cit. 2021-12-06]. Dostupné z: https://www.zive.cz/clanky/pripravuje-se-evropska-digitalni-identita-obcanku-i-ridicak-presune-do-mobilu/sc-3-a-210530/default.aspx
[30] Komise navrhuje důvěryhodnou a zabezpečenou digitální identitu pro všechny Evropany. Evropská komise [online]. Brusel: Evropská komise, 2021, 3. červen 2021 [cit. 2021-12-06]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/ip_21_2663
[31] Evropská digitální identita. Evropská komise [online]. Brusel: Evropská komise [cit. 2021-12-06]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_cs
[32] E-Estonia [online]. Tallinn: Enterprise Estonia [cit. 2021-12-05]. Dostupné z: https://e-estonia.com/
[33] ID.ee [online]. Tallinn: Information System Authority [cit. 2021-12-06]. Dostupné z: https://www.id.ee/en/
[34] NemID [online]. Ballerup: Nets DanID [cit. 2021-12-06]. Dostupné z: https://www.nemid.nu/dk-en/
[35] Overview of the German identity card project and lessons learned (2020 update). Thales [online]. Paris: Thales Group, [2020] [cit. 2021-12-07]. Dostupné z: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/eid-in-germany
[36] AusweissApp2 [online]. Brémy: Governikus [cit. 2021-12-11]. Dostupné z: https://www.ausweisapp.bund.de/en/ausweisapp2-home/
[37] German eID. Federal Office for Information Security [online]. Bonn: Federal Office for Information Security [cit. 2021-12-07]. Dostupné z: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/german-eID_node.html
[38] BankID in numbers. BankID [online]. Stockholm: Finansiell ID-Teknik BID AB, c2021 [cit. 2021-12-05]. Dostupné z: https://www.bankid.com/en/om-oss/statistik
[39] BankID. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation 2001- [cit. 2021-12-06]. Dostupné z: https://en.wikipedia.org/wiki/BankID

[40] Electronic Identification. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2021-12-06]. Dostupné z: https://en.wikipedia.org/wiki/Electronic_identification#Belgium
[41] CIAMPA, Mark. CompTIA® Security+ Guide to Network Security Fundamentals. Seventh Edition. Boston: Cengage Learning, 2020. ISBN 978-0-357-42437-7
[42] ČERMÁK, Miroslav. APT: Jak probíhá cílený útok. CleverAndSmart [online]. Dolní Břežany: Miroslav Čermák, c2008-2021 [cit. 2021-12-09]. Dostupné z: https://www.cleverandsmart.cz/apt-jak-probiha-cileny-utok/
[43] Groups. MITRE ATT&CK [online]. McLean (Virginia, USA): The MITRE Corporation, c2015-2021 [cit. 2021-12-10]. Dostupné z: https://attack.mitre.org/groups/
[44] HOLMES, Aaron. 533 million Facebook users' phone numbers and personal data have been leaked online. Business Insider [online]. New York: Insider, c2021 [cit. 2021-12-08]. Dostupné z: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4
[45] Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Brusel: Evropský parlament a Rada (EU), 2016, ročník 2016, číslo 679. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS
[46] KOHOUT, Roman a Radek KACHRŇÁK. Bezpečnost v online prostředí [online]. Karlovy Vary: Biblio Karlovy Vary, 2016 [cit. 2021-12-11]. ISBN 978-80-260-9543-9. Dostupné z: https://www.internetembezpecne.cz/wp-content/uploads/2017/03/Roman-Kohout-Bezpecnost-v-online-prostredi.pdf
[47] SKOČEK, Jakub. Digitální identita v době služeb Google. Praha, 2015. Diplomová práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Papík, Richard.
[48] BOJANOVIČ, Bojan. A Not-So-Common Cold: Malware Statistics in 2021. DataProt [online]. DataProt, c2021 [cit. 2021-12-12]. Dostupné z: https://dataprot.net/statistics/malware-statistics/
[49] Decryption Tools. No more ransom [online]. NO MORE RANSOM, c2021 [cit. 2021-12-12]. Dostupné z: https://www.nomoreransom.org/en/decryption-tools.html
[50] NĚMEC, Matúš aj. ROCA: Vulnerable RSA generation (CVE-2017-15361). Centre for Research on Cryptography and Security [online]. Brno: Masaryk university, 16th October, 2017 [cit. 2021-12-09]. Dostupné z: https://crocs.fi.muni.cz/public/papers/rsa_ccs17¨

[51] BUCHANAN, Bill. So What Was The Problem With The Estonian ID System and TPMs? Weak Prime Number Generators (and RSA!). Medium.com [online]. 2019, Apr 11, 2019 [cit. 2021-12-08]. Dostupné z: https://medium.com/asecuritysite-when-bob-met-alice/so-what-was-the-problem-with-the-estonian-id-system-and-tpms-1ef02a9bde7f

[52] What we learned from the eID card security risk? *E-Estonia* [online]. Tallinn: Enterprise Estonia, May 14, 2018 [cit. 2021-12-08]. Dostupné z: https://e-estonia.com/card-security-risk/

[53] FOJTŮ, Martina. Objev roku: Vadné čipy způsobily poprask. *Zprávy z MUNI* [online]. Brno: Masarykova univerzita, 2005–2021, 22. května 2018 [cit. 2021-12-08]. Dostupné z: https://www.em.muni.cz/veda-a-vyzkum/10570-objev-roku-vadne-cipy-zpusobily-poprask

[54] Sociální inženýrství a kybernetická bezpečnost. *Eset* [online]. Bratislava: ESET, c1992-2021 [cit. 2021-12-12]. Dostupné z: https://www.eset.com/cz/socialni-inzenyrtsvi-a-bezpecnost-firmy/

[55] Phishing. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2021-12-12]. Dostupné z: https://cs.wikipedia.org/wiki/Phishing

[56] Vícefázové ověření. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2021-12-08]. Dostupné z: https://cs.wikipedia.org/wiki/V%C3%ADcef%C3%A1zov%C3%A9_ov%C4%9B%C5%99en%C3%AD

[57] Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. In: *IETF Datatracker* [online]. Reston: The Internet Society, c2002 [cit. 2022-05-24]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc3280

[58] HUNTER, Alex. OAuth vs SAML vs OpenID: Learn the Differences between Them. *Parallels* [online]. Bellevue: Parallels International, c2022, 2. 4. 2021 [cit. 2022-05-24]. Dostupné z: https://www.parallels.com/blogs/ras/oauth-vs-saml-vs-openid/?fbclid=IwAR1jMs8jdU4vyz18Erou8xRBXjui1nVHh1AwlTBOaukvSr_9BmBhM2gNajo

[59] What is OAuth 2.0?. *Auth0* [online]. Bellevue: Auth0, c2013-2022 [cit. 2022-05-20]. Dostupné z: https://auth0.com/intro-to-iam/what-is-oauth-2/

[60] InterSystems Learning Services. OAuth 2.0: An Overview. In: *Youtube video* [online]. 2016 [cit. 2022-05-24]. Dostupné z: https://www.youtube.com/watch?v=CPbvxxslDTU

[61] Security Assertion Markup Language. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-05-23]. Dostupné z: https://cs.wikipedia.org/wiki/Security_Assertion_Markup_Language

[62] Přehled pro poskytovatele služeb. *BankID* [online]. Praha: Bankovní identita, c2022 [cit. 2022-05-22]. Dostupné z: https://developer.bankid.cz/docs/high_level_overview_sep#bezpecnostni-aspekty

[63] BankID pro developery. *BankID* [online]. Praha: Bankovní identita, c2022 [cit. 2022-05-20]. Dostupné z: https://developer.bankid.cz/docs/security_sep

[64] Bankovní IDentita. *Česká spořitelna* [online]. Praha: Česká spořitelna, c2022 [cit. 2022-05-24]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita#

SEZNAM SYMBOLŮ A ZKRATEK

API	Application Programming Interface
APT	Advanced Persistent Threat
BTS	Base Transceiver Station
CA	Certifikační autorita
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans Apart
CD	Compact Disc
CIA	Confidentiality, Integrity, Availability
ČBA	Česká bankovní asociace
ČSOB	Československá obchodní banka
DES	Data Encryption Standard
DIS+	Daňová informační schránka
DMZ	Demilitarizovaná zóna
DNA	Deoxyribonukleová kyselina
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECDSA	Elliptic Curve Digital Signature Algorithm
EDI	Evropská digitální identita
EEG	Elektroencefalografie
eID	Elektronická identita
eIDAS	Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
EKG	Elektrokardiografie
ES	Evropské společenství
GDPR	Obecné nařízení o ochraně osobních údajů
GPS	Global Positioning Systém
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ID	Identifikátor
IIG	International ID Gateway
IP	Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JSON	JavaScript Object Notation
JWT	JSON Web Token
MD5	Message-Digest Algorithm
MFA	Multi-factor Authentication
MitM	Man-in-the-Middle
NIA	Národní identitní autorita
OAuth	Open Authorization
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastracture

PUK	Personal Unlocking Key
RAT	Remote Access Trojan
REST	Representational State Transfer
RFID	Radio Frequency Identification
ROCA	Return of Coppersmith's Attack
RSA	Rivest-Shadler-Adleman šifra
RSALib	RSA Library
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SOAP	Simple Object Access Protocol
SSO	Single Sign-On
S/MIME	Secure/Multipurpose Internet Mail Extensions
SW	Software
TLS	Transport Layer Security
TPM	Trusted Platform Module
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XML	Extensible Markup Language