Doporučení pro bezpečné nakládání s Identitou občana

NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

AFCEA

Na přípravě doporučení pro bezpečné nakládání s Identitou občana dále spolupracovali:

Národní úřad pro kybernetickou bezpečnost

Vojenské zpravodajství

Bezpečnostní informační služba

Úřad pro zahraniční styky a informace

CZ.NIC

Bank iD

Bankovní identita a.s.

Česká bankovní asociace

Správa základních registrů

První certifikační autorita, a.s.

Obsah

1. Úvod

Cílem tohoto doporučení je seznámit se s elektronickou identitou (dále také jako „Identita občana“ nebo „eID“). Jednoduše si tedy vysvětlíme, co elektronická identita garantovaná a podporovaná státem znamená.

Dozvíme se, k čemu Identitu občana můžeme využít a jak nám může zjednodušit a ulehčit život v dnešním digitálním světě. Popíšeme si prostředky zajišťující ověření autenticity (pravosti) Identity občana a také, jak Identitu občana chránit a zabezpečit, aby pro nás byla co největším přínosem. Seznámíme se s rozdíly mezi prostředky ověřujícími Identitu občana a s účely jejího použití. Je důležité si uvědomit, že Identita občana je jen tak důvěrná jako procesy, které ověřují její autenticitu.

Doporučení nám zodpoví běžné otázky, které souvisí s Identitou občana a těm zvídavým pomůže i s vysvětlením, které zákony vše upravují.

Protože přirozenou lidskou vlastností je potřeba zjednodušovat, používat zkratky apod., je i v tomto dokumentu v některých místech používán zjednodušený pojem Identita občana v situaci, kdy se jedná o prostředek pro její prokazování. Ty pojmy mají podobný, ale nikoliv stejný význam. Elektronická identita ve smyslu zákona je záznam údajů o občanovi či cizinci v Registru obyvatel a k této identitě může být teoreticky libovolný počet prostředků na její prokazování. Ty mohou být zřizovány, používány k autentizaci i zneplatňovány, což tvoří jejich přirozený životní cyklus. Pro mnoho lidí je uvedené zjednodušení postačující, a proto si dovolujeme požádat odborníky na danou problematiku o určitou toleranci našeho výkladu.

2. Co je vlastně elektronická identita

Elektronická identita je dána kombinací jednoho nebo více identifikátorů – osobních údajů (tzv. atributů), které jsou jako celek jedinečným způsobem spojeny s konkrétní osobou. S Identitou občana je spojen proces autentizace (někdy zjednodušeně označován jako přihlašování), kterým lze ověřit, že Identitu občana používá konkrétní osoba.

Z hlediska důvěryhodnosti spojení Identity občana a jejích atributů s konkrétní osobou rozlišujeme:

- Elektronické identity s prokázanou totožností osoby jejího držitele (tedy státem podporovaná Identita občana).

  Identita občana slouží k jednoznačné a nepopiratelné identifikaci konkrétní osoby v digitálním světě elektronických komunikací (fyzických osob nebo fyzických osob zastupujících právnické osoby). Definovány jsou tři úrovně záruk (detaily jsou rozepsány v kapitole 2.3) a tím i tři různé úrovně prokázání totožnosti osoby akreditovaným orgánem (poskytovatel identitní služby). Tato skupina je podpořena zákonem o elektronické identifikaci č. 250/2017 Sb., na jehož základě se ověřování totožnosti děje, a o prostředcích v rámci tohoto systému pojednává dále kapitola 2.3 Identita občana.

- Elektronické identity bez prokázání totožnosti osoby jejího držitele.

  Sem spadá většina elektronických identit (tzv. virtuálních identit nebo uživatelských účtů, viz kapitola 2.1a 2.1), které si člověk sám vytvoří přes internet u různých poskytovatelů, a sám uvede osobní údaje (atributy), které jej mají popisovat. Tyto neověřené elektronické identity se někdy označují jako virtuální identity, což naznačuje, že takových identit může mít jedna osoba více, a pokud daný poskytovatel vůbec ověřuje některé atributy, je to zpravidla přístup k dané emailové schránce (na základě emailové adresy), případně přístup k uvedenému telefonnímu číslu (zasláním ověřovacího kódu). Je tedy třeba být na pozoru, že skutečným držitelem takové elektronické identity může být i úplně jiná osoba než ta, za kterou se svými osobními údaji vydává.

Jak tedy elektronická identifikace pomocí Identity občana funguje? Při zakládání účtu poskytovatel identitní služby ověří naši totožnost, tedy, že se jedná právě o nás jako o jedinečnou a konkrétní osobu. Podle zvolené úrovně záruk pak budeme mít v okamžiku autentizace možnost používat některý prostředek pro elektronickou identifikaci, což může být např. jen uživatelské jméno a heslo, nebo navíc ještě využití chytrého telefonu, nebo

občanského průkazu s čipem a autentizačním certifikátem (případně jiný nosič autentizačního certifikátu).

Identita občana nám umožňuje elektronickou komunikaci s úřady a zprostředkovává přístup k online službám jak některých soukromých organizací (například sázkové kanceláře, na základě zákona o regulaci hazardu), tak k online službám státu (eGovernmentu), a to nejen v rámci ČR, ale na základě nařízení eIDAS z roku 2014, i ve všech členských státech EU.

2.1. Uživatelský účet

Uživatelský účet je účet spojený s uživatelem služby, u kterého není provedena jednoznačná a nepopiratelná identifikace. Identifikační údaje u uživatelského účtu nejsou ověřovány. Takový účet tedy nemůžeme nepopiratelně svázat s identitou konkrétní osoby. Dále není ověřen poskytovatelem identitní služby potvrzujícím jednoznačnost a nepopiratelnost osoby.

Za uživatelským účtem se může nacházet jiná osoba a většinou jde jednoduše takovouto identitu (uživatelský účet, na který se přihlašujeme jménem a heslem) zfalšovat, vytvořit náhradní, zcizit, nebo zneužít. Správci uživatelských účtu se často snaží své uživatele chránit různými metodami (např. ověřením přístupu k emailové adrese nebo svázáním a ověřením telefonním číslem) a tím identitu kontrolovat.

Rozdíl od výše uvedené virtuální identity je v tom, že uživatelský účet u daného poskytovatele nemá federativní schopnosti, tedy použitelnost autentizace (procesu přihlášení) a využití atributů (nastavených informací/parametrů) osoby je omezeno jen na jednoho daného poskytovatele.

Tvoříme si je při zakládání účtů, např. v internetových obchodech (e-shopy).

2.2. Virtuální identita

Jak již bylo uvedeno, virtuálních identit můžeme mít fakticky neomezeně. Virtuální identita je úzce svázaná s pojmem „*virtuální*“. Význam virtuální je vlastnost. Tato vlastnost označuje něco, co je nehmatatelné, materiálně neexistující, ale chovající se jako existující. Tvoříme si je při zakládání účtů např. na sociálních sítích (Facebook, Twitter, LinkedIn apod.) nebo při využívání služeb poskytovaných společnostmi jako je Google, Microsoft, Seznam, Apple apod.

Takové virtuální identity využívají ty osobní údaje, které při zřízení identity vyplníme (*s možnou kontrolou přístupu k emailové adrese a k telefonnímu číslu*). Obvykle nic nebrání tomu, aby různé virtuální identity téhož uživatele u různých poskytovatelů využívaly různé osobní údaje (bohužel i smyšlené).

V digitálním světě je tedy možné vystupovat pod různými virtuálními identitami. Takový přístup samozřejmě můžeme využívat i v běžném životě, kdy se jakákoliv osoba může vydávat za jinou smyšlenou osobu. Přesto mají virtuální identity obvykle schopnost provádět

autentizační služby a předání atributů osoby (s naším souhlasem) jiným poskytovatelům služeb, čímž mohou snížit náročnost při vytváření dalších a dalších uživatelských účtů zejména v oblasti nákupu na internetu.

Základním rozdílem mezi virtuální Identitou a Identitou občana garantovanou státem, nebo certifikovaným/uznávaným subjektem je tedy garance, že za Identitou občana se nachází existující ověřená/ztotožněná osoba, která byla ověřena Identity providerem (poskytovatelem služby ověření) vůči Národní Identifikační Autoritě (NIA). Naopak rozdíl mezi virtuální identitou a prostým uživatelským účtem u nějakého poskytovatele je v tom, že virtuální identita má "federativní" schopnosti vůči jiným poskytovatelům, tedy že dokáže poskytnout autentizační služby třetím stranám, a proto narůstá jejích popularita.

2.3. Identita občana

Identitu občana můžeme také považovat za uživatelský účet. Zásadní rozdíl je ve způsobu ověření atributů a potvrzení elektronické identity státem uznávanou autoritou. Jde tedy o jednoznačné, nepopiratelné ověření, že osoba, která nakládá s přihlašovacími údaji, je shodná s osobou, ke které se vztahují údaje vedené na jejím účtu Identity občana.

Jednoduše řečeno, je to uživatelský účet Identity občana ověřený důvěryhodnou autoritou proti Národnímu identifikačnímu bodu. Neznámějšími prostředky poskytující elektronickou identifikaci jsou Mobilní klíč eGovernmentu, NIA ID (dříve též nazývaný "jméno, heslo, SMS"), elektronický občanský průkaz s čipem, prostředky jednotlivých bankovních domů – nazývané souhrnně Bankovní identita, anebo prostředky soukromoprávních poskytovatelů, např. karta Starcos od společnosti I.CA nebo prostředek mojeID od společnosti CZ.NIC.

V souvislosti s Bank ID je důležité zmínit, že ve většině případů nám byla za splnění zákonných podmínek zřízena automaticky jako majitelům bankovních účtů u konkrétní banky. Postupy jednotlivých bank se ale liší, je třeba se informovat ve vaší bance.

Jak jsme se již dočetli, pro prostředky elektronické identifikace máme tři úrovně záruky: nízká, značná a vysoká. Každý prostředek je pak podle úrovně záruky (způsobu ověření a zabezpečení) zařazen do jedné z nich:

Nízká úroveň – nedochází k zaručenému ověření totožnosti, zvolíme si uživatelské jméno a heslo a svoji identitu pouze deklarujeme.

Značná úroveň – dochází k zaručenému ověření totožnosti, přihlásíme se přes jméno, heslo a další faktor (např. SMS, nebo autentizační aplikace v chytrém telefonu).

Vysoká úroveň – dochází k zaručenému ověření totožnosti, ověření je prováděno navíc přes fyzický identitní prostředek, při jehož vydání byla zaručeně ověřena totožnost a jsou vyžadovány přístupové údaje k jeho použití, a to na bezpečném zařízení (např. na kontaktním

čipu elektronického občanského průkazu, nebo čipové kartě Starcos nebo FIDO tokenu mojeID).

2.4. Další prostředky, které nejsou elektronickou identitou ve smyslu zákona

Dalšími prostředky, se kterými se můžeme v digitálním světě setkat, jsou ty níže uvedené prostředky v kapitolách 2.4.1–2.4.5. Tyto prostředky slouží také k identifikaci, nicméně autorizaci typicky nedovedou dostatečně zaručit, jelikož nenaplňují podstatu zákona o elektronické identifikaci. V mnoha případech se používají pro jiné účely (např. zaručený elektronický podpis pro ověřené odesílání potvrzující pravdivost/důvěrnost dokumentu).

Tyto prostředky se neřídí zákonem o elektronické identifikaci a nejedná se tedy o prostředky elektronické identity v jeho smyslu. V některých případech (kvalifikovaný certifikát a datová schránka) však do jisté míry nebo za určitých okolností mohou být použity pro komunikaci s eGovernmentem.

2.4.1 Kvalifikovaný certifikát

V České republice je používán také tzv. kvalifikovaný certifikát. Vydávat ho může pouze akreditovaná kvalifikovaná certifikační autorita na základě zákona o službách vytvářejících důvěru pro elektronické transakce (zákon č. 297/2016 Sb.). Kvalifikovanému certifikátu se v České republice často říká elektronický podpis. To proto, že jeho použitím je možné provést elektronický podpis, který jednoznačně prokazuje vůli dané osoby. Certifikát ale není primárně určen k autentizaci fyzické osoby.

2.4.2 Elektronický podpis

Elektronický podpis je, s respektem, co bylo řečeno v předchozím odstavci, defacto údaje v elektronické podobě, které jsou připojené k nějaké “datové zprávě” nebo jsou s ní logicky spojené a které umožňují ověření vůle podepsané osoby ve vztahu k datové zprávě. Za elektronický podpis se pak v širším významu považuje i prosté nešifrované uvedení identifikačních údajů (např. jména, IČ) na konci nějakého textu v elektronické podobě, které může dovolit identifikaci označené osoby. O identifikační prostředek se nicméně nejedná.

2.4.3 Datová schránka

Každý uživatel datové schránky má – kromě ovládání schránky samotné – také možnost využít svůj účet k přihlášení do celé řady dalších webových aplikací provozovaných státními úřady i samosprávou, tedy městy a obcemi. To je možné díky autentizační službě informačního systému datových schránek, která bezpečně ověří identitu uživatele a s jeho souhlasem předá údaje o datové schránce i uživateli samotném, klientské aplikaci. Tou může být např. ePortál České správy sociálního zabezpečení, portál Moje daně, Portál občana nebo například městský portál. **Přestože tedy datová schránka není identifikačním prostředkem ve smyslu zákona 250/2017 Sb.** o elektronické identifikaci a není jí tedy možné vybrat ve výčtu prostředků NIA, lze se popsaným způsobem přihlásit k několika, v zákoně přesně vyjmenovaným službám státu. Jakkoliv to může být výhodné pro fyzickou osobu, která tímto prokáže svou souvislost či disponibilitu s právnickou osobou, není tento způsob do budoucna

preferovaný, protože narušuje jinak jednotný princip elektronické identity dle uvedeného zákona. Proto je do budoucna možné očekávat pro přihlašování údaji spojenými s přístupem do datové schránky, spíše útlum této metody a její nahrazení získáváním mandátů pro jednání za právnickou osobu ze základního registru osob (ROS), nežli ze systému datových schránek.

Klientská aplikace se na základě předané sady údajů rozhodne, k jaké činnosti přihlášeného uživatele pustí (odborně řečeno „autorizuje“). Některé aplikace jsou určeny jen pro fyzické osoby, jiné dovolují přihlášení i uživatelů datových schránek právnických osob. Dále se aplikace mohou rozhodovat i podle role uživatele, tedy zda je uživatel držitelem schránky (u schránek fyzických osob), statutárním zástupcem (u schránek právnických osob) nebo pověřenou osobou či administrátorem, kterému byl účet u schránky zřízen následně. V neposlední řadě některé aplikace vyžadují, aby uživatel byl v datových schránkách takzvaně „ztotožněn“, tedy aby jeho identita byla jednoznačně svázána s konkrétním záznamem v Registru obyvatel.

Velkou výhodou autentizační služby datových schránek je právě předání údajů o „mandátu“ uživatele, tedy o jeho vztahu k dotčené datové schránce. Externí aplikace se tedy nedozví jen která konkrétní fyzická osoba se přihlásila, ale také jaký subjekt (např. právnickou osobu) reprezentuje.

Z pohledu uživatele je použití autentizační služby velmi snadné, stačí se přihlásit způsobem, jaký obvykle používá pro přístup do datové schránky, tedy buď jménem/heslem ze systému datových schránek, anebo kterýmkoliv prostředkem v rámci NIA, tedy například Mobilním klíčem eGovernmentu, občanským průkazem nebo některým z prostředků bankovní identity.

2.4.4 Daňová informační schránka (DIS+)

Daňová informační schránka (DIS+) podle § 69 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, poskytuje prostřednictvím dálkového přístupu daňovému subjektu vybrané informace shromážděné v jeho spisu a na osobním daňovém účtu poplatníka. Přístup do DIS+ je umožněn pouze autentizovaným a také autorizovaným uživatelům.

DIS+ obsahuje vybrané informace z daňového řízení. Naleznete zde informace o stavu osobního daňového účtu v členění podle jednotlivých druhů daní, přehled písemností mezi daňovým subjektem a správcem daně a daňový kalendář s přehledem daňových povinností. Z důvodu potřeby přihlašování cizinců má Finanční správa k DIS+ možnost vydávat i vlastní (proprietární) přístupové údaje. Pro všechny ostatní je samozřejmě výhodnější se do ní hlásit přes Identitu občana.

2.4.5 EDU ID

EDU ID je česká akademická federace identit, provozovaná sdružením CESNET. Studenti a akademičtí pracovníci z různých škol a organizací mohou pomocí služby přistupovat k externím zdrojům a aplikacím. Federace identit umožňuje uživatelům z různých organizací přistupovat k externím zdrojům s využitím svých „domovských“ přihlašovacích údajů. Samotné

přihlášení (zadávání přihlašovacích údajů uživatelem) probíhá pouze na přihlašovacím serveru domovské organizace a citlivé údaje jsou ve větším bezpečí. EDU ID je určeno akademickým pracovníkům a studentům a je na druhé straně uznáváno pouze akademickými institucemi. V případě, že by tyto byly schopné garantovat, že v okamžiku přidělení prostředku byla daná osoba ověřena pomocí identifikačního dokladu s fotografií, bylo by možné z tohoto prostředku vytvořit další prostředek v rámci Identity občana. Aktuálně tomu ale tak není.

3. Přínosy Identity občana

V této kapitole se seznámíme s přínosy Identity občana podporované státem. Samotné přínosy budou s elektronizací státu růst, zejména s rozšiřováním počtu služeb, ke kterým je možné se přihlásit.

Zásadním přínosem prostředků elektronické identity, které jsou garantované státem, je ustavení centralizovaných služeb identifikace a autentizace. V této souvislosti se sníží počet uživatelem používaných prostředků pro komunikaci se státem, protože prostředky jsou sdíleny všemi službami centrálních úřadů i obcí a nebude již nadále třeba se u každé služby registrovat zvlášť. Tím poklesne počet potřebných „*virtuálních a uživatelských účtů*“ a dalších „*nástrojů*“, které doposud používáme pro práci/komunikaci ve světě komunikačních technologií/internetu/veřejné správy. Nebude tedy třeba si nadále pamatovat, jakým jménem a heslem se občan kde zaregistroval, protože bude používat typicky jeden svůj oblíbený na všechny služby. Zapamatovat si znalostní kód (PIN např.) k několika málo často používaným prostředkům je úloha, která je pro běžného člověka zvládnutelná, stejně jako třeba u platebních karet, zatímco předchozí uspořádání vyžadovalo mít doma seznam s různými přihlašovacími údaji do mnoha konkrétních služeb, protože při počtu několika desítek takových nebylo prakticky možné si je zapamatovat.

Zásadní výhodou je také zlepšení bezpečnosti, neboť v běžných „nekoordinovaných službách“ se téměř vždy jedná o jednofaktorová řešení typu „jméno a heslo“ a téměř nikdy pro účely těchto přístupů neproběhl jednoznačným způsobem proces nepopiratelného přiřazení prostředku konkrétní fyzické osobě, což je velmi důležité pro poskytnutí jistoty v komunikaci mezi subjekty. Identifikační prostředky jsou schvalovány v souladu s nařízením eIDAS (nařízení č. 910/2014/EU) a jsou až na výjimky dvoufaktorové, tedy typicky jeden je faktor vlastnictví (fyzický prostředek – karta, USB token atd.) a druhý je faktor znalostní (heslo, jednorázový SMS kód atd). Taktéž přiřazení prostředku konkrétní fyzické osobě je striktně řízený a popsaný proces, založený na ztotožnění nějakou úřední či jinou osobou proti předloženému identifikačnímu dokladu s fotografií biometrické kvality.

Jak již bylo naznačeno, jednoznačným přínosem státem garantovaných prostředků elektronické identity je jejich vyšší bezpečnost a z toho vyplývající větší ochrana soukromí. Uvědomme si, že v běžném životě své údaje velmi často poskytujeme velkým nadnárodním, ale i menším technologickým společnostem, u nichž máme z nějakého důvodu uživatelské účty, např. provozovatelům sociálních sítí či elektronických obchodů. Tyto společnosti však nemusí vždy naše údaje vhodným způsobem zabezpečit, a tak jsou téměř na denním pořádku informace o uniklých seznamech přihlašovacích údajů do všech možných služeb či společností. A hlavně, velké společnosti mají svůj podnikatelský záměr založený typicky na vyhodnocování dat o chování uživatele a jejich prodej (doufejme, že anonymní) komerčním

zájemcům, často rekrutovaným z reklamního trhu. Státní Identita občana v tomto srovnání není komerčním produktem, a proto uvedenými riziky, či stěží akceptovanými vlastnostmi, netrpí. Nepotřebuje ani prodávat reklamu, ani sledovat či vyhodnocovat naše chování. Byla zřízena jako státní sdílená služba eGovernmentu. Primární činností státní elektronické identifikace je zabezpečit možnost elektronického přihlašování občanů, a to s nejvyšší možnou bezpečností. Vzhledem k tomu, že u legislativního oprávnění jde primárně o Evropské nařízení, budou některé identifikační prostředky Identity občana z ČR (po jistém procesu notifikace ostatním členským státům) postupně akceptovány i pro transakce v jiných členských státech EU. Tutéž možnost mají i občané EU jako klienti služeb českého eGovernmentu.

Dalším důležitým přínosem elektronizovaných služeb je také rychlost komunikace mezi občanem a úřadem, což se může projevit snížením časové zátěže a nákladů spojených s např. tiskem dokumentů a jejich fyzickou archivací. Je-li agenda správně zdigitalizována, již není třeba tisknout, podepisovat ani ověřovat dokumenty a odnášet na poštu nebo na úřad. Vše lze zvládnout z počítače připojeného na internet, což může znamenat i tablet či mobilní telefon. Ani není třeba připomínat, že elektronický úřad funguje 24 hodin denně, a tak čas využití služby můžete zvolit zcela svobodně, stejně jako místo, odkud služeb budete využívat. Výjimkou tedy není například podávání daňového přiznání ze zimní dovolené na horách, možnosti přístupu k dokumentům ve své datové schránce např. ze služební cesty atd.

Vyvstává samozřejmě otázka přiměřeného počtu prostředků elektronické identity, které si občan má zřídit. Musíme je používat všechny? Nikoliv. Zásadně platí, že je na každém z nás, jaké prostředky si zřídíme a na jaké činnosti je budeme používat. Určitě je doporučeno nemít prostředek jen jeden, protože při jeho ztrátě či zablokování pak nemáte jinou alternativu než běžet na úřad fyzicky. Určitě ale nemusíte mít zřízené všechny prostředky, které v národním identitním schématu existují, ale jen ty, které si podle popisu vyberete a z nějakého důvodu vás zaujmou více než ty ostatní.

Prostředek elektronické identity je bezesporu klíčem k vyřízení komunikace s veřejnou správou. Výčet služeb a možností, kam všude je možné se elektronickou identitou přihlásit, nelze seriózně zachytit, neboť každým dnem vzrůstá. Nejlepším vodítkem je centrální služba, vytvořená Ministerstvem vnitra – Portál občana (https://obcan.portal.gov.cz). Ten je vlastně vstupní branou k aktuálním službám eGovernmentu. Jednotlivé služby jsou zde prezentovány formou dlaždic. Dlaždice jsou, zjednodušeně řečeno, internetové odkazy na další agendové portály, kterých jsou desítky až stovky. Například portál Ministerstva zdravotnictví pro získání certifikátu o očkování proti nemoci Covid-19, portál živnostenského rejstříku, portál České správy sociálního zabezpečení, portál e-Recept, portál sdílení zdravotní dokumentace, Katastr nemovitostí, evidence vozidel, občanské, cestovní a řidičské průkazy atd.

Ve výčtu výhod státem garantované Identity občana bychom neměli zapomenout na fakt, že systém byl od počátku připravován s myšlenkou usnadnit co nejvíce používání běžným občanům. Proto byl do procesů centrálního prvku (NIA) implementován proces tzv. jednotného

přihlášení (single sign-on, SSO), který pohyb mezi jednotlivými provozovateli online služeb velice zpříjemňuje. Jedná se o to, že v případě přihlášení k prvnímu portálu v rámci federace portálů je samozřejmě vyžádána volba identitního prostředku, uživatel zadá příslušné údaje (zvolený PIN, kód ze SMS atd.) a pokračuje jako přihlášený uživatel v první službě. Pokud v rámci stejného prohlížeče přistoupí, například pomocí dlaždice v Portálu občana, k nějakému dalšímu portálu, tak po stisku tlačítka „přihlásit“ se není třeba znovu přihlašovat, ale další portál/služba přebírá pro přihlášení stejné identifikační údaje občana jako předchozí přihlášení. Pokud následně na kterémkoliv z přihlášených portálů stiskne uživatel tlačítko odhlásit, stejně jako když ukončí celý prohlížeč, jednotné přihlášení se zruší a příští přihlášení se opět chová jako to první.

4. Jaká jsou rizika zneužití Identity občana – rizika pro občany

Základní riziko zneužití elektronické identity je „dočasná ztráta kontroly nad svou identitou“. Tedy pokud její oprávněný uživatel nebude dostatečně chránit své identifikační prostředky (jméno, heslo, další přihlašovací prostředek – telefon či USB klíč), může se jeho jménem připojit i někdo jiný (útočník), který se za původního držitele bude vydávat. Pokud by se to stalo, tak prvním zásadním rizikem je, že se jiná osoba může dostat k údajům původního oprávněného uživatele, což mohou být i velice citlivé informace např. o zdravotním stavu, diagnózách, infekčních a jiných nemocech, ale i majetkových poměrech atd. Druhým zásadním rizikem pak je, pokud se ona jiná osoba rozhodne za uživatele začít jednat a jeho jménem provádět transakce vůči veřejné správě. Například by se mohlo jednat o zaslání podání vůči nějakému úřadu, například celnímu, které by zavazovalo k následné platbě částky cla za obchod, který ale daný oprávněný držitel prostředku identity nikdy neučinil. Nebo by se mohlo jednat o pokus převodu majetku na jinou osobu za nepřiměřeně nízkou hodnotu, například v rejstříku motorových vozidel či teoreticky i v katastru nemovitostí. Mohlo by se ale jednat i o vyzvednutí receptu na drahý lék z centrální databáze nevydaných receptů jinou osobou, která se pomocí zneužité identity dostane k čárovým kódům ještě nevyzvednutých receptů daného oprávněného uživatele. I z výše uvedeného příkladného výčtu je zřejmé, že následky zneužití elektronické identity mohou být velmi vážné, a proto je ve výsostném zájmu oprávněného držitele prostředku elektronické identity si prostředek, a tím vlastně i svoji identitu, chránit.

S možností zneužití prostředku elektronické identity je to obdobné, jako s možností zneužití např. platební karty. Pokud jí budu nosit jen tak v zadní kapse kalhot a budu na ní mít ještě fixem napsaný PIN, mohu jí snadno ztratit a útočník pak může okamžitě vyzvednout z bankomatu hotovost. Je tedy třeba se k prostředkům el. identity chovat s respektem a dbát příslušných bezpečnostních zásad. Zásadně své prostředky nesmíte dávat k využití jiným osobám a zásadně nesmíte sdělovat nikomu jejich znalostní faktor (heslo, PIN), aby při případné ztrátě či odcizení nebylo jednoduše možné se daným prostředkem přihlásit. Dále je dobré pravidelně kontrolovat, zda prostředky stále máte pod svou dispozicí (někdo vám je fyzicky neukradl), nikdy je pak nenechávejte bez dozoru na veřejných místech, neukládejte si jejich přístupová hesla na mobilní telefon či jiná elektronická zařízení atd. Je třeba přísně dbát o bezpečnost svých prostředků, zejména pak tajit jejich přístupové údaje. A pokud se již nějaký prostředek ocitne mimo vaší dispozici či mimo vaši kontrolu, ať již z titulu ztráty či odcizení, je třeba jej okamžitě zablokovat, nebo rovnou zneplatnit, případně nahlásit na Policii jejich ztrátu.

Velmi výhodným pro bezpečnost vaší elektronické identifikace se také může stát jeden ze státních prostředků elektronické identifikace, konkrétně Mobilní klíč eGovernmentu.

Podrobně je o něm pojednáno v příslušné kapitole tohoto dokumentu, nicméně v kontextu této kapitoly je možné zdůraznit jednu jeho významnou bezpečnostní vlastnost. Je jí schopnost notifikace, tedy sdělení informace do mobilní aplikace, že došlo k přihlášení k systému národní identity, a to jakýmkoliv prostředkem, kterého jste za normálních okolností oprávněným uživatelem. Například tedy pokud by došlo k přihlášení prostředkem poskytovatele XY, tak do mobilního klíče na vašem telefonu můžete dostat okamžitě notifikaci, že k přihlášení došlo. Pokud jste se přihlásili sami, je to v pořádku a pak je taková notifikace dobrá pouze pro kontrolu, že systém máte nastaven správně a že funguje. Pokud by se ale teoreticky přihlásil někdo za vás (tj. neoprávněně), protože např. našel vaši peněženku s přístupovým prostředkem, u kterého jste omylem nechali i papírek s heslem, můžete se tak dozvědět, že ke zneužití identity došlo. To je v každou chvíli velmi podstatná a ceněná funkce a je to jeden z důvodů, proč byste měli zvážit její používání ve svém telefonu. Součástí informace v mobilní aplikaci je i telefonní číslo na Helpdesk Správy základních registrů, kam můžete zavolat pro další informace, a hlavně pro odpojení daného prostředku. Popsaná notifikační služba funguje na všechny prostředky připojené do národního identitního schématu, tedy jak na ty státní, tak i na soukromoprávní prostředky, včetně prostředků bankovních.

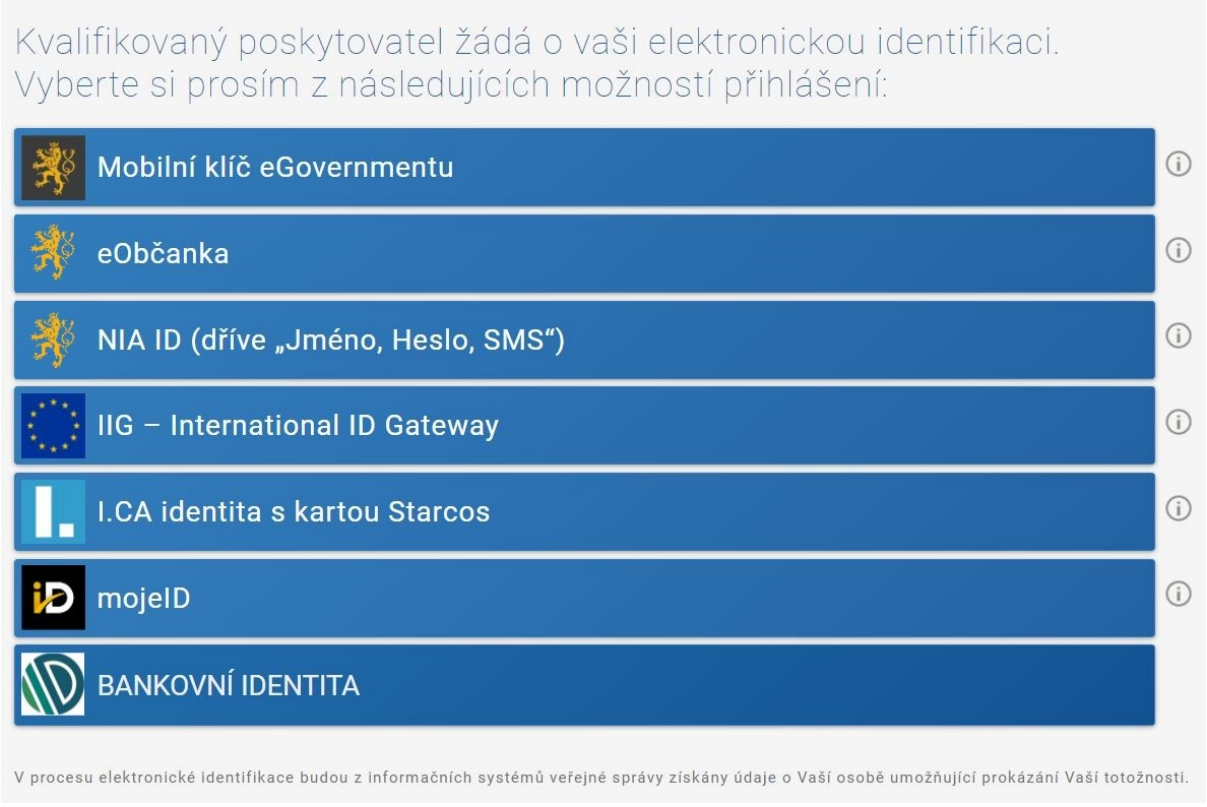
Protože elektronické prostředky se používají elektronickým způsobem, není také dobré se připojovat k internetu na neznámých a nedůvěryhodných místech, například k neznámé Wi-Fi síti bez, nebo se slabým zabezpečovacím heslem. V takových místech typicky mohou číhat útočníci, kteří se mohou včlenit do vaší komunikace s úřadem, rozšifrovat i původně zabezpečenou komunikaci a odposlechnout vaše data či přístupové údaje. Pokud se budete naopak přihlašovat jen k důvěryhodným sítím, zabezpečeným silnějšími hesly, je riziko včlenění se cizí osoby do komunikace minimalizováno.

5. Stávající prostředky pro Identitu občana

Národní bod pro identifikaci (dále jen „NIA“) slouží v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci, jako důvěryhodný nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb veřejné správy.

K prokazování totožnosti online je možné využít různé elektronické identifikační prostředky. Jedná se o identifikační prostředky vydávané státem nebo o soukromoprávní identifikační prostředky, jejichž poskytovatelé získali akreditaci od Ministerstva vnitra a jsou napojeni na NIA. Přehled udělených akreditací je kdykoliv dostupný na webu (https://info.identitaobcana.cz/idp/).

Poskytovatelé online služeb potřebují zaručenou informaci o tom, kdo se jako klient přihlašuje k jimi poskytovaným službám a využívají tak služby elektronické identifikace poskytované prostřednictvím NIA. Každý poskytovatel online služby si tak pouze stanovuje, jakou úroveň záruky identitního prostředku požaduje pro elektronické prostředky. V rámci procesu identifikace se po přesměrování na NIA uživateli zobrazí všechny dostupné prostředky pro elektronickou identifikaci, které splňují požadavek na danou a vyšší úroveň záruky, kterou určil poskytovatel online služby.



Je důležité upozornit, že veškeré údaje jsou poskytovatelům online služeb předávány prostřednictvím NIA pouze v případě, že k tomu v procesu přihlašování udělíte souhlas. Souhlas může být jednorázový nebo trvalý a je možné jej kdykoliv odvolat ve svém profilu na portálu Národního bodu. Jako uživatel tak máte vždy přehled o tom, komu jste dali souhlas s předáváním Vašich osobních údajů.

5.1. Mobilní klíč eGovernmentu

Úroveň záruky: Značná

Mobilní klíč eGovernmentu (aplikace pro mobilní telefon či tablet) původně vznikl jako jedna z možností přihlašování k Informačnímu systému Datových schránek. Pro jeho snadné použití, a také možnost využít již existující mobilní aplikaci, proběhlo rozšíření o možnost přihlášení i přes Národní bod.

Nosičem Mobilního klíče eGovernmentu je zařízení, na kterém je naistalována aplikace „Mobilní klíč eGovernmentu“. Aplikaci je možné naistalovat z obchodu s aplikacemi (dostupné pro Google Play a Apple App Store). Aplikace funguje na principu sejmutí QR kódu z obrazovky zařízení, na kterém se někam přihlašujete. Není tedy nutné si pamatovat často složité přihlašovací údaje, ani opisovat dlouhé kódy ze SMS, zaslané do vašeho mobilního telefonu.

Pro umožnění přihlašování je třeba danou instanci jednorázově navázat (registrovat) na fyzickou osobu. To je možné provést několika způsoby, pro každý způsob je v rámci aplikace připraven jednoduchý návod, jak postupovat.

- Založení prostřednictvím portálu Národního bodu
- Založení skrze Informační systém Datových schránek
- Udělením souhlasu s poskytnutím údajů jiným osobám, v tomto případě Správě základních registrů, prostřednictvím kontaktního místa veřejné správy CzechPoint. Jeho využití je v tomto případě zdarma.

Jakmile je účet aktivní, tak již nic nebrání jej využívat pro přihlašování k elektronickým službám státu. Jednou z výhod je možnost zasílání upozornění, že Vaše identita byla použita k přihlášení k nějaké online službě prostřednictvím Národního bodu a přispívá tak k případnému odhalení zneužití některého z prostředků. Vyjma zasílání upozornění z Národního bodu umožňuje aplikace zasílání upozornění i z Informačního systému Datových schránek, a uživatel tak má přehled, zda obdržel datovou zprávu.

Využití: Přihlašování pomocí Mobilního klíče eGovermentu lze využít pro přihlašování k online službám státu na úrovni značná a nižší. Jednou z největších výhod je snadnost použití, kdy po odemčení aplikace stačí prosté sejmutí obrazovky fotoaparátem a celý přihlašovací proces již nevyžaduje další zadávání hesel či nějakého uživatelského jména. V případě přihlašování na zařízení, kde je vlastní aplikace nainstalována (na vlastním mobilním telefonu) je situace

ještě jednodušší a odpadá kopírování různých SMS kódů a podobně mezi okny aplikací. Jak již bylo zmíněno, tak další výhodou je získávání upozornění, ať už z Národního bodu, tak z Informačního systému Datových schránek.

Více informací: https://info.identitaobcana.cz/mep/

5.2. eObčanka

Úroveň záruky: Vysoká

Popis: Občanský průkaz vydávaný od 1. července 2018 (tzv. „eObčanka“) je možné využít pro elektronickou identifikaci a autentizaci, pokud si držitel v okamžiku jeho vyzvednutí na úřadě aktivoval jeho elektronický čip. Aktivaci může provést osoba starší 15 let tím, že na úřadě příslušném k vydávání občanských průkazů zadá identifikační osobní kód (IOK) a deblokační osobní kód (DOK). Pokud chceme využívat všechny vlastnosti eObčanky, je nutné si na svůj počítač, tablet či mobilní telefon naistalovat obslužný software (obsahující aplikace „eObčanka – Identifikace“ a „eObčanka - Správce karty“), který je volně ke stažení na internetové adrese: https://info.identitaobcana.cz/Download/, a mít k němu připojenu příslušnou čtečku čipových karet (tu je potřeba si dokoupit). Čtečka čipových karet by měla splňovat základní parametry – soulad s normou ISO 7816, CCID (Chip Card Interface Device), komunikační standard PC/SC a být kompatibilní s operačním systémem počítače. U mobilních platforem, které většinou nedisponují USB konektorem pro připojení běžné čtečky, je možné použít čtečku s rozhraním Bluetooth, která je o něco dražší, a je potřeba jí samostatně nabíjet.

Občanský průkaz lze použít také pro účely podepisování elektronických dokumentů a dále pro přihlašování do informačních systémů s využitím autentizačních certifikátů. Za tímto účelem je držitel občanského průkazu oprávněn uložit do kontaktního elektronického čipu kvalifikované certifikáty pro elektronické podpisy a autentizační certifikáty. Pokud chce občan využít svoji eObčanku jako úložiště svého elektronického podpisu nebo autentizačních certifikátů, musí nastavit také další přístupové kódy – PIN, QPIN a PUK, jejichž popis a postup nastavení je popsán na https://info.identitaobcana.cz/eop/OchranneKody.aspx. Pro účely správy kvalifikovaných certifikátů pro elektronické podpisy, autentizačních certifikátů a změny přístupových kódů, je k dispozici zmiňovaná aplikace "eObčanka – správce karty", která je součástí instalačního balíčku s obslužným softwarem.

Využití: eObčanku s aktivovaným čipem lze použít jako prostředek pro elektronickou identifikaci s vysokou úrovní záruky a rovněž jako úložiště svého elektronického podpisu a autentizačních certifikátů. eObčanka, jako zatím jediný prostředek pro elektronickou identifikaci vydávaný v ČR, je notifikována do EU v souladu s nařízení eIDAS. Tj. občané mohou svoji eObčanku s aktivovaným čipem používat i pro přístup k online službám, které jsou poskytovány jinými členskými státy v EU, při splnění podmínek daných nařízením eIDAS.

Více informací o eObčance je k dispozici na adresách: https://info.identitaobcana.cz/eop/ a https://www.mvcr.cz/clanek/podminky-pouziti-obcanskeho-prukazu-se-strojove-citelnymi-udaji-a-s-kontaktnim-elektronickym-cipem-pro-ucely-elektronicke-identifikace-a-doporucena-bezpecnostni-opatreni.aspx

5.3. NIA ID

Úroveň záruky: Značná

Popis: Prostředek NIA ID je spjatý s Národním bodem již od jeho počátku v roce 2018 (původně se prostředek jmenoval „jméno, heslo a SMS“). Občané ČR a cizinci vedení v Registru obyvatel a zároveň starší 18 let, si mohou založit prostředek, ať již skrze odkaz pod oknem pro přihlášení tímto prostředkem, či přímo na webové stránce https://niaid.cz/. Pro založení prostředku je vyžadováno výhradní vlastnictví emailové adresy a mobilního telefonního čísla pro příjem SMS (přičemž číslo musí mít českou předvolbu +420).

Samotné založení prostředku je prvním krokem do elektronického světa přihlašování k online službám státu. Účet je třeba aktivovat připojením k identitě konkrétní fyzické osoby. Dokud není účet aktivován, tj. navázán na fyzickou osobu, tak je umožněno přihlášení pouze k portálu Národního bodu. Možností, jak navázat identifikační prostředek NIA ID na fyzickou osobu, je několik:

- Přihlášením jiným prostředkem úrovně Značná nebo Vysoká,
- Přihlášením přes Informační systém Datových schránek, schránkou fyzické, nebo podnikající fyzické, osoby,
- Udělením souhlasu s poskytnutím údajů jiným osobám, v tomto případě Správě základních registrů, prostřednictvím kontaktního místa veřejné správy CzechPOINT.

Jakmile je účet aktivní, tak již nic nebrání jej využívat pro přihlašování k elektronickým službám státu.

Využití: NIA ID je možné využít jako identifikační prostředek, kterým je možné se přihlásit ke všem online službám Kvalifikovaných poskytovatelů, které akceptují úroveň značná, což je dnes drtivá většina. Pro použití prostředku není potřeba speciálních zařízení, ale uživatel si vystačí se znalostí přihlašovacích údajů a výhradním vlastnictvím mobilního telefonního čísla, registrovaného v České republice. Tato metoda přihlášení usnadňuje použití NIA ID napříč všemi věkovými kategoriemi obyvatelstva.

Více informací: https://info.identitaobcana.cz/ups/

5.4. I.CA

Garant: I.CA

Úroveň záruky: Vysoká

Popis: Čipová karta Starcos 3.5 a vyšší s komerčním identitním certifikátem je stejně jako občanské průkazy vydávané od 1. 7. 2018 nástrojem, kterým se prostřednictvím NIA prokazuje, že přihlašující se uživatel je skutečně tím, za koho se vydává.

Čipová karta Starcos od výrobce Giesecke&Devrient je v České republice poskytována společností První certifikační autorita a. s. (I.CA), a to především jako nástroj pro splnění některých požadavků nařízení eIDAS.

Ve spojení s komerčním identitním certifikátem splňuje požadavky na kvalifikovaný prostředek pro elektronickou identifikaci.

Z hlediska uživatele je proces získání identitního certifikátu jednoduchý – je obdobný, jako při vydání kvalifikovaného certifikátu pro elektronický podpis s uložením soukromého klíče v bezpečném hardwarovém prostředku, tj. čipové kartě nebo tokenu. Stejně tak je jednoduché jeho používání. Certifikáty vydávají tytéž registrační autority I.CA, které vydávají i jiné typy certifikátů a kterých je v ČR více než 30. Jejich aktuální seznam je na webových stránkách I.CA – www.ica.cz.

Zájemci mají možnost zvolit využití čipu pro uložení

- komerčního identitního certifikátu pro elektronickou identifikaci
- komerčního identitního certifikátu pro elektronickou identifikaci a kvalifikovaného certifikátu pro elektronický podpis (produkt Identitní TWINS, tj. TWINS pro elektronickou identifikaci).

U varianty TWINS je výhodou vydání obou certifikátů na základě jedné žádosti a jednoho ověření totožnosti žadatele.

Čipová karta Starcos je zabezpečena PIN a PUK. Citlivé operace na kartě je možné realizovat vždy pouze po zadání PIN. PUK lze využít v případě zablokování karty pro získání dalších pokusů pro zadání PIN. Při dodávce čipových karet je možné si vybrat ze dvou možných nastavení PIN a PUK:

- PIN a PUK je generován při personalizaci a je umístěn do tzv. PIN obálky
- karta není po personalizaci vybavena PIN a PUK a klient je při prvním použití karty požádán o jejich zadání.

Čipová karta Starcos umožňuje:

- zadat informace o majiteli karty, doplnit identifikační údaje vlastníka karty a fotografii

- zvolit podporované (důvěryhodné) Certifikační autority, jejichž klientské certifikáty může klient využívat (standardně certifikáty I.CA); jiné klientské certifikáty pak není možné na kartu umístit, čímž se významně omezuje možnost použití karty k nepovoleným operacím.

Čipová karta ve standardní velikosti je určena pro použití se čtečkou čipových karet. Oblíbená je varianta plug-in, tj. s vylamovacím čipem. V tomto případě si klient samostatnou čtečku čipových karet nepořizuje.

Některé z nabízených čteček umožňují kromě připojení k USB portu PC rovněž bezdrátové připojení prostřednictvím Bluetooth.

Využití: V současné době se čipová karta Starcos 3.5 a vyšší s komerčním identitním certifikátem využívá například v systému Zákaznické samoobsluhy systému elektronického mýtného a v Informačním systému technických prohlídek. Stala se také jednou z možností registrace do dotačních programů COVID pro firmy a OSVČ. Samozřejmě je možné použít tento prostředek i pro přihlášení do datové schránky či Portálu občana.

Více informací: https://www.ica.cz/ica-identity-provider, https://www.ica.cz/kvalifikovany-prostredek-uroven-vysoka

5.5. MojeID

Garant: CZ.NIC

Úroveň záruky: Nízká, značná a vysoká

Popis: Služba mojeID vznikla již v roce 2010 a patří tak k jedné z prvních široce dostupných služeb elektronické identifikace v Česku. V roce 2020 prošla služba mojeID akreditačním procesem na MV ČR. S mojeID je možné se přihlašovat k mnoha službám v ČR, a dokonce také v zahraničí.

Ověřené údaje uživatelů

Již od vzniku služby mojeID byl jednou z jejích hlavních předností důraz na ověřování údajů, které o sobě uživatel uvádí. U všech účtů dochází k ověření e-mailového a telefonického kontaktu. Dobrovolně je pak možné ověřit i korespondenční adresu a jako nejvyšší stupeň ověření je možné provázat účet s registrem obyvatel a díky tomu je možné působit jako identitní prostředek v rámci Identity občana. V takovém případě lze ověřit totožnost několika způsoby – návštěvou pobočky Czech POINT, systémem datových schránek nebo eOběankou, případně dalšími prostředky elektronické identifikace.

Bezpečnost

Druhým klíčovým znakem služby mojeID je od začátku snaha nabídnout nejmodernější a nejbezpečnější prostředky elektronické identifikace pro vícefaktorové přihlašování. Již krátce po spuštění se objevila možnost využití generátoru jednorázových hesel, následovala vlastní mobilní aplikace pro jednoduché potvrzování jedním kliknutím. V roce 2019 byla do služby mojeID implementována možnost přihlašovat se bezpečnostním klíčem podle standardu FIDO. Technologie FIDO zajišťuje maximální ochranu proti útokům typu MITM (nabourání útočníka do komunikace mezi dvěma účastníky). Pro její použití v nejběžnějších zařízeních, jako jsou ty s operačním systémem Windows 10 nebo Android, není nutné nic dalšího pořizovat a je možné použít bezpečnostní klíč zabudovaný přímo v operačním systému. Bezpečnostní klíč FIDO je možné nahradit nebo doplnit o přihlašování pomocí mobilní aplikace MojeID Klíč, která je k dispozici zdarma pro telefony a tablety využívající systémy Android nebo iOS. Přihlašování je tak nejen maximálně bezpečné, ale zároveň maximálně pohodlné. Pro nejvyšší úroveň záruky je možné použít externí HW klíč s odpovídající certifikací.

Využití: S prostředkem mojeID je možné se přihlašovat nejen ke službám eGovernmentu, ale také do různých elektronických obchodů, zpravodajských portálů, městských knihoven a do mnoha portálů obcí a měst a řady dalších služeb. Přehled smluvních partnerů je k dispozici v katalogu služeb dostupném na https://www.mojeid.cz/cs/kde-pouzit/katalog-sluzeb/. Účet je také možné použít pro správu domény u některých doménových registrátorů. Od září 2020 je možné používat účet mojeID také pro přihlašování ke službám veřejné správy. Více informací: https://www.mojeid.cz/cs/

5.6. Bankovní identita

Úroveň záruky: Značná

Popis: Bankovní identita je metoda digitálního ověření v online světě provozovaná bankami. Stejně jednoduše jako se občané přihlašují do svého internetového bankovnictví, se s bankovní identitou mohou identifikovat při vstupu na webové portály se službami státu (eGovernmentu) nebo i do služeb soukromých společností jako jsou eShopy a další portály.

Princip fungování bankovní identity je jednoduchý a bezpečný, prověřený řadou let úspěšného užívání v severských státech a dalších digitálně vyspělých zemích.

Občané si pro využití bankovní identity nemusí nic zřizovat, nikam chodit ani se nic nového učit – většina z nich již totiž svou bankovní identitu u své banky má a aktivně ji používá při přihlašování do svého internetového bankovnictví. Využití bankovní identity je zdarma, v případě jakýchkoli problémů s použitím se občané navíc mohou spolehnout na klientský servis své banky.

Klíčovým prvkem při používání bankovní identity je její bezpečnost, na níž si banky obecně dlouhodobě zakládají, a to nejen z důvodů přísných regulatorních pravidel, ale i za účelem udržení důvěry svých klientů. Díky propracovanému systému vícefaktorového ověření, které je v případě bank naprostým standardem a jehož součástí je dnes zpravidla i biometrická identifikace v rámci mobilní potvrzovací aplikace, zajišťují banky svým klientům při využívání tohoto druhu elektronické identity maximální možnou bezpečnost.

Každé ověření je provedeno pouze na základě iniciativy a souhlasu občana. Banky uskutečňují pouze identifikaci, tím jejich zapojení končí. To znamená, že banky přihlašovací údaje svých klientů nikomu nepředávají, dále je pečlivě chrání, a samozřejmě ani nevidí, jaké úkony klient následně po úspěšné identifikaci realizuje a na jakém portálu.

Využití: Bankovní identitu je možné využít jako identifikační prostředek, kterým je možné se přihlásit k většině online služeb (agend) státu, které jsou na odpovídající úrovni záruk (značná), jakožto i službám soukromých společností, pokud se tento identifikační prostředek rozhodnou svým klientům nabídnout a implementovat do svých systémů.

Více informací: www.bankovni-identita.cz, webové stránky jednotlivých českých bank a www.bankid.cz společnosti Bankovní identita, a.s, zprostředkovávající implementaci tohoto řešení soukromým společnostem pod názvem BankID.

6. Srovnání druhů elektronických identit

Pro srovnávání jednotlivých druhů identitních prostředků je nejdůležitější navrhnout správně kritéria, podle kterých budeme jednotlivé prostředky posuzovat.

Jedním z možných kritérií je tzv. úroveň záruky daného prostředku, level of assurance (LoA – úroveň zajištění identity). Dělení na tři úrovně zavedlo přímo nařízení eIDAS, a to na úroveň nízkou (low), značnou (substantial) a vysokou (high). Úroveň nízká je typicky splněna jednofaktorovou autentizací, tedy jméno a heslo. Úroveň značná je již povinně vybavena dvoufaktorovou autentizací, tedy "něco mám" a "něco znám". Úroveň vysoká je navíc ještě ve většině případech založena na tzv. kvalifikovaném zařízení (QSCD), což znamená prostředek, který má certifikaci osvědčující některé principy kybernetických bezpečnostních zařízení, například že heslo není za žádných okolností možné z daného zařízení vyčíst ven a zmocnit se jej. Úroveň záruky je předmětem certifikace, aby bylo garantováno splnění podmínek. V ČR máme jen několik málo prostředků na úrovni vysoká (elektronický občanský průkaz s čipem, vydávaný od 1. 7. 2018, karta Starcos společnosti I.CA a také prostředek MojeID společnosti CZ.NIC). Všechny ostatní prostředky vyjma jednoho bankovního jsou pak akreditovány pro úroveň značnou.

Dalším z možných kritérií porovnávání prostředků mezi sebou je jejich snadnost použití v mobilním prostředí, které co do četnosti používání již dávno převýšilo původně široce rozšířené prostředí desktopových PC. A právě proto, že mobilní zařízení mají optimalizované vlastnosti i operační systémy tak, aby se lépe používaly, je spojení některých prostředků elektronické identity na nich o něco složitější. Důvodem může být například to, že k mobilnímu prostředku nejde běžným způsobem připojit čtečka čipových karet s rozhraním USB. Týká se to typicky prostředků, které spoléhají na čip na kartě, například elektronického občanského průkazu s čipem, prostředku Starcos od dodavatele I.CA, případně se to může týkat i některých dalších. Velká většina prostředků již vlastní čip na fyzické kartě či tokenu nepotřebuje, protože v této roli vystupuje mobilní telefon či tablet uživatele, na kterém je nainstalovaná registrovaná aplikace. Těmto prostředkům se většinou říká mobilní klíče. V tomto smyslu jsou tedy moderní prostředky v podobě mobilní aplikace o něco výhodnější a jejich používání je zpravidla pro uživatele méně náročné, i když jsou certifikovány jen pro úroveň značná, zatímco fyzické prostředky typicky disponují certifikací na úroveň vysoká.

Důležitým kritériem je také využitelnost daného prostředku. Téměř všechny prostředky je možné využít pro přihlášení k online službám připojených prostřednictvím národního bodu podle zákona o elektronické identifikaci. Výjimku tvoří bankovní prostředky, které prostřednictvím národního bodu mohou poskytovat přihlášení pouze ke službám státu a samosprávných celků. Využití prostředků státu (tedy eOběanky, NIA-ID a mobilního klíče eGovernmentu) je naopak striktně omezeno pouze pro služby dostupné prostřednictvím

národního bodu. Ostatní nestátní prostředky (tedy prostředky I.CA, mojeID nebo bankovní identita) navíc umožňují využití v řadě soukromoprávních online služeb (telekomunikace, e-shopy, knihovny apod.)

A konečně dalším možným kritériem pro porovnání prostředků je jejich cena a také snadnost získání. Zatímco státní prostředky Mobilní klíč eGovernmentu, elektronický občanský průkaz s čipem nebo NIA ID je možné získat zcela zdarma, některé jiné prostředky, typicky od soukromoprávních provozovatelů jsou komerčními projekty a musí si tedy na sebe vydělat. Cena za jich získání se může pohybovat v malých částkách za kus. Zvláštní skupinou jsou v tomto srovnání prostředky Bankovní identity, které jsou poskytovány klientovi zdarma jako doplňková služba k bankovnímu účtu, má-li k němu zpřístupněnu službu elektronické bankovnictví. Banky jsou ale komerční subjekty, pro které zdroj příjmů v tomto případě představují smlouvy na poskytování identifikačních služeb se soukromoprávními provozovateli online služeb. Těmi mohou být např. telefonní operátoři, dodavatelé energií či jiných komodit, nebo třeba pojišťovací společnosti atd.

7. Jak zabezpečit svou Identitu občana

Identitu občana je druh uživatelského účtu, který je svázaný s jednoznačně identifikovanou osobou, která prostřednictvím tohoto účtu – Identity občana může dále komunikovat zejména se státní správou.

Prostřednictvím Identity občana je možné mít dálkový přístup k údajům konkrétního uživatele-občana, takže pokud útočník získá přístup k Vaší Identitě občana, může získat informace o Vás (výpis z rejstříku trestů, z katastru nemovitostí, ze zdravotní dokumentace a dalších připojených služeb). Tedy co můžete získat za informace od státní správy Vy, bude moci i úspěšný útočník.

Útočník bude moci mít přístup do Vaší datové schránky a jejím prostřednictvím podávat žádosti na úřady, komunikovat Vaším jménem, číst doručené datové zprávy.

S ukradenou Identitou občana může útočník přenastavit různá upozornění, která můžete mít nastavena (vypršení platnosti občanského průkazu, ohlášení změn v katastru nemovitostí apod.).

Pro ověření identity je využíváno celé řady prostředků, je tedy třeba zajišťovat bezpečnost všech prostředků, které s Identitou občana souvisí. Běžně používanými prostředky jsou např. chytrý mobilní telefon, počítač, notebook, mobilní klíč (aplikace), USB klíč (token) nebo čipová karta.

Zabezpečení Identity občana je tedy přímo úměrné bezpečnosti používaných prostředků.

Zneužití Identity občana je však mnohem složitější a vyžaduje značnou míru znalostí a technických prostředků, lze tedy obecně konstatovat, že je mnohem bezpečnější používat Identitu občana než běžné užívání fyzických dokladů jako občanský průkaz nebo přihlašovací údaje k běžnému uživatelskému účtu.

7.1. Rizika z pohledu bezpečnosti prostředků

Různé prostředky elektronické identifikace jsou spojeny s různou úrovní zabezpečení proti potenciálnímu útočníkovi. Jisté vodítko dává samotná úroveň záruky daného prostředku, která v hrubém měřítku popisuje, co může uživatel od úrovně zabezpečení prostředku očekávat. Požadavky na bezpečnost jsou v tomto případě ukotveny v prováděcím nařízení Komise (EU) 2015/1502, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci.

Ministerstvo vnitra tyto požadavky ještě více rozpracovalo do dokumentu konkretizujícího požadavky na poskytovatele identitních služeb (DKP-IDP) - s dokumentem je možné se seznámit zde:

https://www.mvcr.cz/clanek/ministerstvo-vnitra-zverejnuje-dokument-konkretizujici-minimalni-pozadavky-na-kvalifikovane-eid-systemy-a-eid-prostredky.aspx).

Pro posouzení bezpečnosti prostředků se primárně pracuje s termínem faktor autentizace, což je termín odkazující na to, jakým způsobem uživatel prokazuje, že je oprávněným vlastníkem prostředku. Obvykle se používají tři kategorie těchto faktorů, je to faktor na základě vlastnictví, faktor na základě znalosti a inherentní faktor. Faktor na základě vlastnictví spočívá v ověření faktu, že něco uživatel vlastní (čipová karta, telefon, bezpečnostní klíč). Faktor na základě znalostí ověřuje, že uživatel něco ví (Heslo, PIN). Inherentní faktor ověřuje nějakou fyzickou vlastnost osoby (typicky jde o biometrické údaje – nejčastěji otisk prstu, obraz obličeje, méně často pak oční duhovka nebo sítnice či infračervený obraz krevního řečiště lidské dlaně).

Pro nízkou úroveň záruky platí, že autentizační prostředek používá jen jeden faktor autentizace. Typicky se bude jednat o heslo. Pro značnou úroveň záruky je nutné, aby prostředek kombinoval minimálně dva faktory ze dvou různých kategorií. Zde můžeme mezi prostředky najít celou řadu variant využívajících všechny kategorie. Pro nejvyšší úroveň záruky je nutné, aby prostředek efektivně zabraňoval možnosti vytvořit duplikát, a zde se již objevují pouze HW prostředky se silnou ochranou uloženého kryptografického materiálu.

7.2. Bezpečnost hesel

Heslo je nejběžnějším znalostním faktorem autentizace. Používá se buď samostatně anebo se kombinuje s jinými faktory. Nejběžnějšími způsoby útoku na hesla jsou buď hádání, snaha o jejich odchycení za pomocí útoku typu „*MITM*“ (Man-In-The-Middle), případně off-line útoky. Útočník využívající hádání předpokládá, že uživatel používá slabé heslo. Jako ochrana se doporučuje použít silné dlouhé heslo v kombinaci s tím, že služba by měla být schopná detekovat opakované pokusy o zadání hesla a nějakým způsobem útočníkovi takové hádání zamezit (lze rozpoznat například tak: pokud služba umožnuje více jak 3x zadat heslo, aniž by třeba dočasně znemožnila přístup nebo nevyžadovala další reakci uživatele). Existují také různé metody uchovávání hesel na straně služeb, přičemž bohužel některé nejsou dostatečně bezpečné. Existuje služba, která se snaží tyto přístupy kategorizovat a uživatele o nebezpečných metodách informovat. Příkladem může být služba na této adrese: https://pulse.michalspacek.cz/passwords/storages. V případě útoku typu MITM může sofistikovaný útočník uživatele přesvědčit, že se přihlašuje ke správné službě, přestože komunikuje s falešnou stránkou. K tomu se používají různě techniky sociálního inženýrství například známý phishing. Uživatel v takovém případě heslo předá útočníkovi nevědomky. Je třeba být maximálně obezřetný, kam se uživatel přihlašuje a pečlivě kontrolovat URL adresu

v záhlaví internetového prohlížeče, zejména doménovou část (např. „*mojebezpecnasluzba.cz*“). Off-line útok bývá často prováděn v případě, kdy unikne databáze uživatelských jmen (emailových adres) a hesel (obvykle jejich hashů nebo jiného typu zašifrování) a útočník tak má možnost pokoušet se uhádnout heslo masivní výpočetní silou (brute force). Určitou ochranou je nezadávat stejná hesla u více služeb, čímž se zamezí útočníkovi, který např. tímto způsobem získal heslo od nějaké konkrétní služby, aby toto heslo úspěšně použil jinde.

7.3. Bezpečnost SMS autentizace

Pro dosažení vícefaktorové autentizace se často používá ověření faktoru vlastnictví telefonního čísla na základě SMS zaslané na toto číslo. I pro takto koncipovanou autentizaci platí, že v případě MITM útoku má útočník možnost kromě hesla odchytit i kód zaslaný SMS a platí stejná opatření zmiňovaná výše. V případě SMS autentizace hraje velkou roli také zabezpečení telefonu, na který SMS přichází. Bohužel oprávnění přístupu ke čtení SMS zpráv je často udělováno velkému množství aplikací na chytrých telefonech. Je nutné, aby tyto aplikace byly důvěryhodné. V poslední době se objevují útoky typu SIM swap, který obchází zabezpečení telefonního operátora, určené pro případ, kdy zákazník SIM kartu ztratí. Útočník, který přesvědčí operátora, že SIM kartu ztratil a získá novou s číslem oběti, tak může bez problémů odchytit autentizační SMS. Útočníci mohou také využít k přímému odposlechnutí komunikace zranitelnosti signalizačního protokolu SS7, používaném telefonními operátory.

7.4. Bezpečnost mobilních potvrzovacích aplikací

Mobilní aplikace pro potvrzení autentizací vynechávají z komunikace telefonního operátora a tím eliminují některá rizika popsaná výše. Navíc typicky umožňují zapouzdření dvou různých faktorů autentizace. Faktor vlastnictví je zde řešen tak, že v mobilním zařízení je uložen kryptografický klíč, použitý pro podepisování zpráv. Druhý faktor je buď znalostní (typicky PIN) nebo inherentní (otisk prstu nebo obraz obličeje). Aplikace tak nevyžadují zadávání hesla. Ani v tomto případě nicméně není uživatel plně chráněn proti MITM útoku a musí být opatrný při hlídání, kam se přihlašuje. Pro vybuzení autentizace stačí často zadat informaci, která z principu není tajná (číslo smlouvy, email, datum narození atd.). To dává útočníkovi prostor pokusit se v době, kdy se uživatel přihlašuje, zaslat paralelně jiný autentizační požadavek a zmást uživatele tak, aby autorizoval takovýto požadavek místo oprávněného. Toto je možné eliminovat kontrolou ověřovacího kódu, který by měl být pro uživatele stejný jak na webu, tak v mobilní aplikaci. Klíčovou vlastností bezpečnosti je také uložení kryptografického klíče. Moderní verze chytrých telefonů již obsahují tzv. Secure Element, který znesnadňuje zneužití

uloženého klíče. Některé starší verze Android telefonů nicméně tento systém nepodporují a bezpečnost je zde tak snížena.

7.5. Bezpečnost FIDO tokenu

Technologie FIDO je, podobně jako u mobilních potvrzovacích aplikací, postavena na kryptografii. Navíc v sobě ale nese prvek, který tuto technologii dělá odolnou vůči phishingu. FIDO bezpečnostní klíče jsou k dispozici v mnoha variantách od softwarového řešení po vysoce zabezpečená hardwarová úložiště. Uživatelům k rozlišení slouží FIDO certifikace, která ukazuje, jak důsledně je chráněn kryptografický klíč zabezpečující vlastní přihlášení. V každém případě je rizikem používat necertifikované klíče. Na trhu jsou naopak k dispozici i FIDO bezpečnostní klíče integrující čtečku otisku prstů, jejímž použitím dojde ještě ke zvýšení bezpečnosti.

7.6. Bezpečnost čipových karet

Čipové karty umožňují nejvyšší míru zabezpečení. Kryptografické klíče zabezpečující komunikaci jsou i zde uloženy v certifikovaném hardwarovém úložišti bez možnosti jednoduše vytvořit kopii takového klíče. Ve většině případů vyžaduje čipová karta navíc doprovodný software, který je nutné nainstalovat na klientské zařízení a který zajišťuje bezpečnou komunikaci mezi klientem a ověřovacím serverem. Obvykle se nicméně nejedná o otevřené technologie, takže míra důvěry je závislá na důvěře v technologického dodavatele. I zde jsou známé případy selhání, jako např. chyba v systému firmy Infineon, dodavatele pro technologie čipových karet Estonských a Slovenských občanek, která způsobila vysoké riziko zneužití těchto dokladů a vedla k hromadné výměně kryptografických klíčů uložených na těchto kartách.

Jednotlivé faktory autentizace mohou být implementovány různými technologiemi. V následující tabulce je vyznačeno, jaké technologie jsou použité v existujících bezpečnostních prostředcích.

	Heslo	SMS	Mobilní aplikace	FIDO klíč	Čipová karta
eOP					X
NIA-ID	X	X			
MEG			X		
I.CA					X
mojeID	X		X	X	
Bankovní identita	X	X	X		

8. Obecná doporučení (pro širokou veřejnost)

V oblasti on-line transakcí s využitím elektronické identifikace a autentizace mějte na paměti, že výběr způsobu a prostředku elektronické identifikace by měl odpovídat hodnotě transakce, kterou hodláte provést přes Internet. V reálném „digitálním světě“ využíváme pro různé typy online transakcí mnoho virtuálních identit a zdaleka ne všechny nám technicky umožňují využít státem garantovanou Identitu občana. Kromě toho zdaleka ne všechny transakce si zasluhují (z hlediska možných rizik), abychom tu nejvíce zabezpečenou Identitu občana využívali všude ve spotřebitelských službách – i proto, že využití více faktorové nebo vícestupňové autentizace bývá o něco pracnější, a přece jen trochu „zdržuje“.

Vaše elektronická identita bude v bezpečí v případě, že budete mít dostatečně zabezpečená zařízení, která budete pro používání elektronické identity používat stejně tak, jako tato zařízení chráníte při přístupu např. do Vašeho internetového bankovnictví.

- Používejte zdravý selský rozum a pečlivě rozmýšlejte, kam zadáváte své údaje (nejen přihlašovací)
- Nikdy nesdělujte přihlašovací údaje a nepůjčujte autentizační prostředky (eOP, tokeny) jiným osobám.
- Nenechávejte druhý autentizační nástroj bez dozoru (USB token, eOP, mobil). Pokud používáte mobil jako autentizační prostředek, mějte vždy nastaveno zamykání obrazovky. Mějte na paměti, že používání speciálních aplikací pro generování a případně i předávání jedinečných přihlašovacích kódů je bezpečnější než zasílání přihlašovacích kódů prostřednictvím SMS. Příjem SMS není chráněn dalších heslem (PINem), a navíc je možné jej u pokročilých útoků „odposlechnout“. Pokud můžete, převeďte dodatečnou autentizaci s využitím mobilu na mobilní aplikaci a zabezpečte její spuštění biometrickým faktorem nebo dodatečným heslem.
- Nainstalujte si antivirový program a pravidelně jej aktualizujte. I ty, které jsou zdarma, nabízí kvalitní ochranu počítače. V poslední době se objevují již i antivirové programy pro ochranu chytrých telefonů – některé z nich jsou i ve „free“ verzi. Používejte ale jen takové, které byly schváleny výrobcem Vašeho mobilního telefonu, resp. jeho operačního systému.
- Zabezpečte přístup na domácí síť Wi-Fi silným heslem (použijte kombinaci velkých a malých písmen, číslic a dalších zvláštních znaků, a celkem doporučujeme délku alespoň 12 znaků) a přesvědčte se, že používáte nyní nejsilnější běžně používanou metodu šifrování přenosu WPA3 (pokud není podporován, tak WPA2; nepoužívat WEP a WPA).
- Nepoužívejte veřejné sítě Wi-Fi, pokud hodláte provést jakoukoli transakci se svojí elektronickou identitou; pokud můžete, použijte připojení přes mobilní data.

- Přesvědčte se, že webová stránka poskytovatele zobrazuje obvyklou URL adresu (že se nejedná o napodobeninu Vaší známé stránky, kterou ale vlastní někdo jiný). Pokud se URL neshoduje s oficiální internetovou adresou služby, kterou hodláte využít, okamžitě stránky opusťte.
- Zkontrolujte, že jste připojeni přes zabezpečené připojení TLS/SSL. Váš prohlížeč to obvykle potvrzuje symbolem visacího zámku vlevo od URL adresy, která musí začínat „https://....“ a nikoli jen „http://....“. Moderní prohlížeče již kliknutím na zámek zobrazí výsledek sady kontrol spojení a dají vodítko typu “spojení je zabezpečené”, nebo Vás naopak varují o opaku.
- Ověřte, že certifikát šifrovaného spojení TLS/SSL byl vydán pro subjekt (organizaci), který má poskytnout zamýšlenou službu. To ověříte (podle typu prohlížeče) rozkliknutím symbolu zámečku, následně “více informací” (nebo podobné) - prohlédnout certifikát. V informačních polích certifikátu pak uvidíte v poli “Subject name” nebo “Common name” jméno subjektu, komu byl certifikát vydán. Toto jméno se musí shodovat s poskytovatelem služby (nebo jeho mateřskou firmou).
- Pokud můžete, aktivujte přes veřejné sítě zabezpečené tunelování VPN (Virtual Private Network). VPN dávají obvykle k dispozici firmy svým zaměstnancům pro jejich práci odkudkoli a pro běžné spotřebitele to může být obtížně splnitelné doporučení.
- Na stránkách s problematickým obsahem vždy pečlivě zvažte, na jaký odkaz kliknete. Obecně platí, že čím „zajímavější“ je obsah poskytnutý zdarma na dané webové stránce (a není to renomovaný poskytovatel), tím vyšší pravděpodobnost je, že na takové stránce je skrytý škodlivý kód nebo Vám nabízí stažení softwaru, který je pozměněn a obsahuje škodlivý kód.
- Jestliže využíváte svůj emailový účet pro příjem výzvy k resetování hesla, aktivujte si vícefaktorovou nebo alespoň vícestupňovou autentizaci pro přístup do Vašeho emailu, čímž výrazně znesnadníte zneužití Vašeho emailu útočníkům. Kvalitní poskytovatelé elektronické pošty využívají inteligentní „podmíněný přístup“ s průběžným vyhodnocováním rizika každého přihlášení, který si vyžádá druhý faktor např. jen v případě, kdy se jedná o pokus o přístup z neznámého zařízení, prvně použitého prohlížeče nebo z neznámé lokality (IP adresy). Používejte u svého poštovního klienta spamový filtr a antivirovou ochranu. U zavedených poskytovatelů emailu jsou tyto filtry již součástí standardních nabídek.
- Chraňte mobilní telefon či tablet heslem, PINem a lépe otiskem prstu před "volným přístupem".
- Pro přístup na internetové bankovnictví nebo přihlašování k elektronické identitě zadávejte internetovou adresu dané instituce ručně, neklikejte na zaslané nebo zobrazené odkazy.
- V podezřelých e-mailech neklikejte na žádné odkazy. Pamatujte, že banky a platební systémy **NIKDY** nevyžadují osobní údaje ani důvěrná uživatelská data e-mailem.
- Nevyužívejte sdílené počítače/případně využívejte alespoň anonymní režim.

- Využívejte silná a neopakující se hesla.
- Instalujte aplikace pouze z ověřených zdrojů (aplikace odjinud mohou být závadné).
- Pokud si nejste schopni zapamatovat hesla, využívejte správce hesel.
- Nezadávejte hesla na cizích zařízeních.
- Při ztrátě jakéhokoliv prostředku si okamžitě změňte heslo, případně aktualizujte své telefonní číslo. Je tedy nutné vždy zabezpečit všechny prostředky, které se podílí na autentizaci.
- Šifrujte obsah vašich zařízení (full disk encryption jak u mobilního zařízení, tak počítače) za využití silného hesla. Šifrováním prostoru/harddisku/úložného prostoru zařízení zajišťujeme ochranu dat (hesel, klíčů, veškerých dat/informací) proto, aby je případný útočník nebo osoba, která dané zařízení (NB, PC, telefon) získá, nemohla jednoduše přečíst/získat data na něm uložená. Data jsou šifrována obvykle pouze při vypnutém zařízení. Šifrováním zajišťujeme, že informace nebudou jednoduše a ihned dostupné případnému útočníkovi a bude muset použít nějakou technicky nebo časově náročnou metodu k prolomení zvoleného šifrování. Tuto dobu je pak nezbytné využít ke změně hesel, zablokování přístupů.
- Aktualizujte nejen operační systém (mobilu, počítače), ale i všechny aplikace na těchto zařízeních instalované.
- U souborů, které to umožňují, nepovolujte makra, pokud si nejste jisti, že jsou od důvěryhodného odesílatele a neobsahují škodlivý kód.
- Heslo použité pro Identitu občana nepoužívejte u jiné služby. Jedním z nejjednodušších způsobu útoků je „hádání hesel“, zejména s dnešním světem digitálních technologii není složité zjistit Vaše zájmy, jména rodinných příslušníků, data narození, domácí mazlíčky a podobně. Zejména pokud se podíváte na zprávy, velmi často se objevují informace o zcizených databázích od různých poskytovatelů služeb. Pokud tedy budete mít stejné heslo na více účtech, útočník, má pak jednoduchou cestu k vašemu účtu, neboť první, co vyzkouší, je již jemu známé heslo.
- Vždy požívejte bezpečná dlouhá hesla. Dlouhá hesla se sice špatně pamatují, ale ztěžují případný útok typu brute force (útok hrubou silou). Jde většinou o automatizovaný typ útoku, kde útočník zkouší veškeré kombinace písmen, číslic a znaků, nebo se používají takzvané slovníkové útoky, kdy jsou používány slova nebo jejich kombinace. Běžný počítač je teoreticky schopen otestovat 3.000.000.000 kombinací za sekundu. Pokud vezmeme heslo tvořené 6 znaky (abeceda s možností velkých a malých písmen, jde tedy o 52 znaků). Jde tedy o 19.770.609.664 možných kombinací. Takové heslo jde zjistit za 7sekund. U 8 znakového hesla s možností použití číslic a speciálních znaků (98 znaků), pak bude teoretický čas 32 dnů 19 hodin 44 minut 37 sekund (jde samozřejmě o modelový příklad). Proto je třeba používat na hesla velká a malá písmena, číslice, speciální znaky (*-?@÷, atd…)
- Silné přihlašovací heslo do zařízení. Zde jde o stejnou analogii jako u obecného konstatování dlouhých a bezpečných hesel, kterou je třeba doplnit o vazbu na počítač/

zařízení. Ten, pokud by Vám byl odcizen, nebo jste náhodou nechali někde bez dozoru nějaký prostředek (počítač, telefon, tablet), ztížíte případnému útočníkovi možnost buď získat vaše data, nebo jej minimálně zpomalíte.

- Oddělené účty od účtů dětí. Významným rizikem jsou děti a další členové domácnosti. Ne každý musí být vždy obeznámen s bezpečným nakládáním a chováním v elektronickém světě anebo nemusí dodržovat všechna pravidla. Koneckonců i únava a stres mohou vést k nedostatečné pozornosti. A právě proto, aby se snížila pravděpodobnost chyby způsobené jinou osobou, která má přístup na váš počítač, je vhodné alespoň používat oddělené účty, čímž se sníží pravděpodobnost ztráty nebo poškození dat na vašem účtu na počítači.
- Nepoužívejte administrátorská oprávnění (privilegované účty) na svém běžném účtu do počítače. Oprávnění správce/administrátora vám umožňují, v případě potřeby, provádět změny důležitých částí vašeho systému, instalovat programy a nastavovat zařízení. Pokud tedy nebudete používat účet s administrátorským oprávněním, zásadním způsobem tím snížíte možnosti případného útočníka provést nežádoucí aktivitu na vašem zařízení.
- Pro zabezpečení nepoužívejte gesta, ale buď PIN s minimální délkou 6 číslic nebo biometriku. U této problematiky jde zejména o jednoduchost získání přístupu. Nejjednodušeji lze odpozorovat gesto, následuje PIN, přičemž jeho délkou se bráníte zejména proti útokům hrubou silou. Biometrické údaje se však velmi složitě získávají nebo obchází.
- Vypněte automatické přihlašování k uloženým Wi-Fi sítím

8.1. Doporučení podle úrovně dopadu zneužití eID

Obecně lze z hlediska rizik a možných dopadů naše identity fyzické osoby rozdělit asi do 3 úrovní:

8.1.1 Nejnižší dopady:

Identity ve formě uživatelských účtů ve spotřebitelských službách, při kterých nedochází k platbám přes internet, ve kterých nejsou uloženy údaje o kreditních kartách a se kterými nejsou spojeny žádné citlivé osobní údaje. Toto jsou např. přihlašovací účty do cenových srovnávačů, nákupních portálů, které nás svým obsahem nijak nekompromitují a kde případná platba probíhá přes platební bránu třetí strany. Ve všech těchto případech bývají osobní údaje pouze základní identifikační údaje fyzické osoby – typicky jméno, příjmení, adresa bydliště, emailová adresa a telefon. Zneužitím těchto uživatelských účtů tedy může dojít maximálně k prozrazení těchto údajů, spolu s historií transakcí, provedených s tímto uživatelským účtem – tedy historie nákupů, historie hodnocení produktů, historie příspěvků na sociálních sítích. Ve většině případů lze považovat tyto účty za „anonymní“, kdy se neprovádí kontrola, zda Vámi používané identifikační údaje (jméno, adresa) jsou pravé. Systémy často kontrolují jen Váš přístup k zadané emailové adrese, a někdy i přístup ke sdělenému číslu mobilního telefonu.

Doporučení: u těchto uživatelských účtů je možné využívat mnemotechnická, avšak delší textová hesla (min. 12 znaků) nebo schopnosti prohlížečů zapamatovat si Vaše přihlašovací údaje (jméno, heslo), které souvisí s danou Internetovou stránkou. U těchto použití lze při ztrátě hesla z paměti počítače nebo při jeho zapomenutí provést jednoduchý reset hesla obvykle zasláním výzvy k nastavení nového hesla na Vaši emailovou adresu.

- V případě nejnižších úrovní dopadů lze s výhodou využít i moderní vestavěné funkce typu **“správce hesel” dnešních webových prohlížečů,** které si nejen dokážou zapamatovat uživatelské jméno a heslo, dokážou i vygenerovat “silné” heslo, odlišné pro každý přihlašovací účet. Tato funkce může být třeba aktivována v “Nastavení”, a podle typu prohlížeče je obvykle dále v uživatelském profilu, volba např. “hesla”. Zde je typicky možné spravovat všechny “zapamatované” kombinace jména/hesla pro jednotlivé webové stránky – je možné je smazat, a po znovu potvrzení hesla k účtu prohlížeče je někdy možné i hesla zobrazit v otevřeném textu. Kromě zjevných výhod má využití vestavěného správce hesel i svoje nevýhody: (i) paměť hesel je vázána na konkrétní typ prohlížeče – pokud chcete nebo potřebujete pro jiné webservery použít jiný prohlížeč, hesla nebudou automaticky k dispozici; (ii) hesla se obvykle replikují do cloudu k danému poskytovateli (typicky Google Account, Microsoft Account, Apple ID). To má výhodu v tom, že při použití stejného typu prohlížeče máte “svoje hesla” k dispozici na všech zařízeních (notebooky, tablety, chytré telefony) i po jejich výměně, avšak s tímto musíte mít důvěru k danému poskytovateli, že celý

obsah správce hesel bude trvale uložen (samozřejmě v zašifrované formě) u daného poskytovatele.

- **Vazba na evropské nařízení eIDAS:** zde používané prostředky elektronické identifikace (obvykle jen „anonymní“ jméno a heslo) nelze přiřadit ani k nejnižší úrovni „nízká“ dle eIDAS, protože s nimi obvykle není spojeno předání údajů a čísla občanského průkazu nebo jiného průkazu vydávaného státem. Běžně tyto identity považují za identity bez fyzické kontroly skutečné identity uživatele.

8.1.2 Střední dopady:

Identity spojené se službami, které ukládají údaje o Vašich platebních kartách a případně i bankovních účtech, avšak ne s takovou transakční hodnotou, která by Vám mohla způsobit existenční potíže – a to jak finančně, tak z hlediska osobní reputace, nebo z hlediska právní odpovědnosti za provedené úkony (tedy nikoli transakce typu převod vozidla, podpis obchodní smlouvy, nebo výpisy z Vaší zdravotnické dokumentace). Omezení zneužití Vaší identity v oblasti elektronického bankovnictví nebo platebních karet je zde obvykle limitováno maximální hodnotou jednotlivých transakcí, nebo sumy denních / týdenních finančních transakcí. Do této úrovně patří oblíbené identity se schopností federace typu Microsoft account, Google account či Apple ID, pokud je skutečně využíváme pro přihlašování do různých dalších Internetových služeb, a pokud se rozhodneme přímo v této službě uložit údaje o platební kartě (pro jednoduchost nákupu přes napojené tržiště aplikací). Obdobně sem lze zařadit uživatelské účty ve službách typu PayPal, Uber, Booking.com a podobným, pokud sem ukládáme i údaje o platebních kartách. Do této úrovně lze zařadit také mnoho podání vůči státní správě, část komunikace přes systém datových schránek a transakce provedené přes Portál občana, které nevyžadují správcem systému elektronickou identifikaci dle úrovně záruk (eIDAS) „vysoká“.

Doporučení: využití těchto elektronických identit by mělo být vždy podmíněno vícefaktorovou nebo alespoň vícestupňovou autentizací (tedy dodatečným ověřením přihlašující se osoby). V současné době již téměř všichni poskytovatelé služeb s takovou transakční hodnotou umožňují vícefaktorovou autentizaci prostřednictvím chytrého telefonu. Služby elektronického bankovnictví jsou dobrým příkladem poskytovatele vlastní služby (správy bankovního účtu) a kromě toho i poskytovatelem ověřené identity. Použití kreditních karet v EU je dnes na tlak vydavatelů (bank) převáděno na metodu platby „SecureCode“ (VISA/MasterCard) nebo podobnou, tedy kdy uživatelské nastavení využití kreditní karty vyžaduje v průběhu transakce ověření pomocí dodatečné autentizace zadavatele (obvykle mobilní aplikace nebo jedinečný SMS kód). O něco nižší míru zabezpečení než „dvoufaktorová“ vykazuje „dvoustupňová“ autentizace, která nemusí být vázána na jiný prostředek, ale využívá se typicky zasláním dalšího transakčního kódu na Vaši emailovou adresu. Přístup k takovému emailu ale není

vázán na daný prostředek, a proto může být pro útočníka snadnější si takový přístup předem zajistit.

- U služeb veřejné správy se naopak očekává, že orgány veřejné moci budou akceptovat a vyžadovat elektronickou identifikaci jednotně prostřednictvím systému Identita občana, a to v úrovni záruk nejméně „značná“ (dle eIDAS), kde je uplatnění příslušné úrovně ověření fyzické identity i mechanismu autentizace dáno prováděcími předpisy.
- Jako typické příklady práce s elektronickou identitou pro tuto úroveň záruk je Mobilní klíč eGovernmentu ČR, nebo různé tokeny pro generování jedinečných hesel nebo mobilní aplikace pro bezpečnější přihlašování do elektronického bankovnictví.
- Využití chytrých telefonů a jejich mobilních aplikací je dnes mnoha uživateli využíváno s přihlašováním pomocí biometriky (otisk prstu nebo scan obličeje / oční duhovky). V nejslabším případě tak je možné prolomit celý systém např. krádeží takového chytrého telefonu a schopností napodobit Vaše biometrické údaje útočníkem, který odemkne biometrikou samotný telefon, pak ještě bankovní aplikaci, a potom ještě funkci pro druhý faktor (např. onu speciální autentizační aplikaci). Obecně se v úrovni záruk „značná“ považuje dodatečná autentizace biometrikou za dostatečnou a je spíše na výrobci toho kterého chytrého telefonu, jak obtížné je příslušný biometrický senzor přelstít.
- Jak zde naložit (kromě prostředku druhého faktoru autentizace) s přihlašovacími hesly nebo PINy? Jistěže nejlepší je nikam si je nezapisovat, používat „neslovníková“ hesla, k jejich zapamatování používat mnemotechnické pomůcky a ke každé takové identitě použít jiné uživatelské heslo, To však pro mnoho z nás může být problém si tato hesla zapamatovat, a to tím více, kdy některé identitní systémy vyžadují pravidelnou obměnu hesla. Možná řešení:
  - **použít speciální program typu „password manager“** pro správu a zabezpečené ukládání hesel. Takový program přímo vygeneruje silné heslo pro každou novou identitu (uživatelský účet) a uloží si je do zašifrovaného úložiště. Uživatel si pak pamatuje jen jedno heslo do této zvláštní aplikace, pravděpodobně opět s využitím dvoufaktorového přihlašování. Ověřené speciální programy typu “password manager” mají obvykle vyšší úroveň zabezpečení uložených hesel než pouhý prohlížeč, ale mohou mít další požadavky na zálohování a přenos funkce na jiná zařízení. Doporučujeme zvážit výhody a nevýhody konkrétních řešení, zejména proto, že jde většinou o placenou službu. Přehled těchto programů a jejich porovnání lze nalézt např. zde: Přehled těch nejlepších správců hesel - PCWorld.cz; 5 nejlepších správců hesel pro Windows v roce 2021 [s kupony] (safetydetectives.com); Best password manager in 2021 for business & personal use | ZDNet; 🔧 Nejlepší Správce Hesel AKTUALIZOVÁNO2021 | srovnání a zkušenosti (5nej.cz)
  - Běžné **automatické ukládání hesla do paměti Vašeho internetového prohlížeče lze doporučit jen v případě**, že využíváte vestavěnou funkci

prohlížeče, díky které máte hesla zabezpečena hlavním heslem a máte celý disk počítače nebo mobilu kvalitně zašifrovaný (např. nástrojem BitLocker který je součástí Windows apod.), a kdy máte nastaveno automatické zamykání obrazovky (lock screen) a silnější přihlašování do počítače nebo mobilu rovněž s využitím dvoufaktorové nebo jinak inteligentně řízené autentizace.

- Kdo nechce jít bezpečnější cestou kvalitního správce "password manager", může si hesla alespoň zapisovat do šifrovaného souboru s uživatelským heslem (např. u MS Word s využitím funkce „Soubor", dále „Info", dále „zabezpečit dokument", volba „šifrování heslem"). Předpokladem je dodatečná ochrana šifrováním celého disku a zajištění záložní kopie tohoto zašifrovaného souboru na externí médium a jeho uložení na fyzicky bezpečném místě. Přitom je třeba mít na paměti, že vlastní heslo není vhodné přenášet z jiného zobrazení (např. z onoho dokumentu) pomocí copy&paste, protože obsah clipboardu může být lehce cílem útoku skrytého malwaru. Tento zašifrovaný soubor je také třeba pravidelně zálohovat – nejlépe mimo primární zařízení.

- **Vazba na evropské nařízení eIDAS:** tyto transakce odpovídají využití prostředků elektronické identifikace v úrovni „**značná**", neboť použití identity zde předpokládá ověřenou fyzickou identifikaci osoby (v bance nebo u orgánu veřejné moci, např. CzechPoint).

8.1.3 Vysoké dopady:

Identity spojené nebo využívané s elektronickými službami, které mohou mít na uživatele nejvyšší až existenční dopady. Zde se obecně předpokládá, že tyto kategorie služeb eGovernmentu budou do těchto dopadů zařazeny již správci takových služeb veřejné správy, a budou v souladu s nařízením eIDAS vyžadovat použití prostředku elektronické identifikace s úrovní záruk „vysoká". Sem budou pravděpodobně patřit služby typu elektronický výpis ze zdravotnické dokumentace a služby veřejné správy s vysokou transakční hodnotou (např. převod vlastnictví automobilu, převod nemovitosti). Dále sem patří scénáře vyžadování kvalifikovaného elektronického podpisu, a případně další scénáře, kdy takové elektronické služby se sami rozhodneme využívat pouze s prostředkem elektronické identifikace v úrovni záruk „vysoká", tedy zejména eOP. Jak je již uvedeno výše – některé služby budou vyžadovat úroveň „vysoká" rozhodnutím správce. U jiných služeb, zejména u soukromoprávních poskytovatelů, by mělo být možné si ve svém uživatelském profilu nastavit, jaký způsob a prostředek elektronické identifikace budu sám pro danou službu vyžadovat, tak aby k této službě nemohl získat přístup útočník, který by alternativně využil přihlašování jiného prostředku pro elektronickou identifikaci s nižší úrovní záruk.

Doporučení: pro úroveň záruk „vysoká" bude ve většině případů třeba použít interní nebo externí čtečku eOP (přes USB port) nebo USB token jako kvalifikovaný prostředek pro elektronický podpis s kvalifikovaným elektronickým certifikátem. Použití externího a

jednoúčelového zařízení má velký vliv pro odizolování útočníka, který by mezitím mohl ovládnout Váš osobní počítač, tablet nebo chytrý telefon. Zjednodušeně řečeno se má za to, že vygenerování jedinečného kvalifikovaného el. podpisu nebo autentizačního hashe pomocí externího prostředku v úrovni záruk „vysoká“ představuje značnou ochranu, kterou dnes můžeme systémově zavést proti nejvíce sofistikovaným kybernetickým útokům na elektronickou identitu.

- Jediné, co je třeba k provedení elektronické identifikace v této nejvyšší bezpečnostní úrovni, je mít u sebe příslušný externí token nebo čtečku smart karty, a PIN pro odemknutí podpisového nebo autentizačního certifikátu. Tento PIN je již třeba si zapamatovat a rozhodně nedoporučujeme si jej kamkoli zapisovat (maximálně si zapsat do šifrovaného souboru jen jako mnemotechnický opis, kterému neporozumí jiné osoby).
- **Vazba na evropské nařízení eIDAS: Vazba na evropské nařízení eIDAS:** tyto transakce odpovídají využití prostředků elektronické identifikace v úrovni „**vysoká**“.

8.2. Známé typy útoků

Pro stanovení známých typů útoků v kyberprostoru, které mohou vyústit v ohrožení elektronické identity, lze využít popis nejčastějších vektorů útoku, které kybernetičtí útočníci nejčastěji užívají k dosažení svých cílů:

- **backdoor** lze definovat jako zneužití přístupu do zařízení instalací škodlivého kódu umožňujícímu vytvoření zadních vrátek pro následné neoprávněné aktivity ze strany útočníka, ochranou proti tomuto typu útoku je zejména komplexní antivirové řešení;

- **cross-site scripting** nastává za předpokladu zneužití webové aplikace ze strany útočníka ke spuštění nežádoucího kódu v zařízení, ochrana je obdobná jako v případě backdooru, kdy ji lze doplnit bezpečnými webovými prohlížeči;

- **man-in-the-middle** je typ útoku, při kterém je útočníkem zachycena komunikace mezi dvěma zařízeními a neoprávněně nahrazena zcela nebo zčásti daty útočníka, čímž dojde k narušení důvěrnosti a integrity přenášených dat, ochranou je využívání důvěryhodného (vyhnutí se veřejným Wi-Fi sítím) a bezpečného internetového připojení (s dostatečnou úrovní šifrování – na u př. Wi-Fi sítí přinejmenším WPA2), kdy jej lze doplnit VPN službami od důvěryhodných poskytovatelů;

- **sociální inženýrství** je v současnosti jedna z nejčastějších technik využívajících sociální zranitelnosti oběti pro získání informací využitelných pro široké spektrum následných neoprávněných aktivit v kyberprostoru, ochranou proti tomuto typu útoku je zejména obezřetnost uživatele a dodržování zásad kybernetické bezpečnosti (nesdělování údajů, které by mohly být zneužity při následném kybernetickém útoku);

- **phishing** je útok za využití e-mailových zpráv, ve kterých je obvykle zastřen skutečný odesílatel pro získání informací od oběti, kdy je obvykle doplněn technikami sociálního inženýrství, obranou proti tomuto typu útoků je užívání bezpečné e-mailové služby (s kontrolou přijímaných e-mailů v aspektech odesílatele, šifrování, manipulací se záhlavím e-mailu, bezpečnosti obsažených odkazů, příloh a dalších prvků e-mailové zprávy), vlastní kontrola záhlaví e-mailu (IP adresa odesílatele, servery přes který byl e-mail zaslán), kontrola obsažených odkazů (skutečná adresa uvedeného odkazu), případně i zpětné ověřování validity zaslaného e-mailu (kontaktování subjektu odesílající e-mail jinou formou);

- **spear phishing** označení pro cílený phishing na konkrétní jednotlivce, případně organizace pro následné neoprávněné aktivity, ochrana proti tomuto typu útoku je obdobná jako u phishingu;

- **útoky na hesla** je využíván útočníky pro neoprávněné získání přístupu do koncového zařízení, případně uživatelského účtu, přičemž jsou útočníkem užívány různé kombinace hesel (získaných např. v rámci slovníků nejčastěji používaných hesel, ale i informací získaných o oběti jinými způsoby) pro jeho odhalení, ochranou může být užívání silného hesla, které bude zároveň odlišné pro každou službu (včetně jeho pravidelné změny, s možností nastavení kontroly úniku přístupových údajů vázaných na konkrétní uživatelský účet na službách monitorujících úniky uživatelských účtů na internetu) a rovněž doplněného o vícefaktorovou autentizaci pokud je provozovatelem služby k dispozici;

- **zranitelnost nultého dne** je vektor útoku, u kterého útočník neoprávněně zneužívá zranitelnosti hardwaru zařízení nebo softwaru, o kterých obvykle v době útoku nemá povědomí jejich výrobce, je tudíž proti němu velmi obtížná obrana, obecně však lze doporučit využívání nejaktuálnějších produktů jak z hlediska hardwaru, tak softwaru a preference bezpečných výrobců z pohledu historického výskytu známých zranitelností a dalších aspektů.

- **vishing** – vzniklo slovním spojením z anglického "voice" a "phishing". Jedná se o telefonickou obdobu phishingu, kdy útočník obvolává své oběti, vydává se za zástupce určité instituce a následně se z nich snaží vylákat citlivé údaje. Útočník často zneužívá služeb Voice-over-IP pro podvržení telefonního čísla. Obdržený hovor tak vypadá, jako by byl realizován z legitimní klientské linky dané instituce.

- **útoky typu MITM na zařízení** – Útočník se snaží získat přístup k zařízení své oběti. Pokud se mu to podaří může nainstalovat nějaký software na dané zařízení, ať už je to

počítač, tablet nebo telefon a toto zařízení může odchytávat komunikaci, kterou generují aplikace na počítači nebo sám uživatel. Útočník tak může např. odchytit heslo nebo PIN zadávané přes klávesnici nebo může nainstalováním nějaké závislé knihovny získat citlivé údaje přenášené mezi aplikacemi. Tento přístup může útočník získat využitím zranitelnosti v neaktuálním software na počítači, přesvědčením uživatele, že má otevřít nějaký email nebo stáhnout nějaký software z webu (phishing). Jediná možnost, jak se tomuto bránit, je kontrolovat přístup k zařízení, mít vždy aktuální verzi operačního systému a antivirus a neotevírat neznámé přílohy mailů.

- **útoky typu MITM mimo zařízení** – Útočník se může pokusit odchytit komunikaci mezi zařízením oběti a serverem poskytujícím služby. Nejčastější postup je, že útočník vytvoří webovou stránku, která se velmi podobá cílové službě a oběť si tak myslí, že komunikuje s touto službou, zatímco komunikuje s útočníkem. Následně např. phishingem útočník přesvědčí oběť, že je nutné se ke svému účtu přihlásit. Útočník pak sám napřímo komunikuje se službou a předstírá, že je oběť. V průběhu komunikace může útočník vylákat nejen heslo, ale i jednorázové kódy zaslané na telefon nebo souhlas vydaný autentizační aplikací. Uživatel by měl znát a důsledně hlídat doménové jméno v adresním řádku prohlížeče na webové stránce, kde provádí autentizaci. Útočník se může snažit maskovat název domény za podobně vypadající např. (flo.cz místo fio.cz).

- **útoky typu sim swap** – Jelikož je SIM karta pouhý identifikátor, kterým se zákazník prokazuje svému telefonnímu operátorovi, existuje možnost převést telefonní číslo na jinou SIM kartu. Telefonní operátoři mají mechanismy, jak umožnit zákazníkům získat zpět číslo, pokud například ztratili telefon. Tyto mechanismy mohou být různou měrou odolné proti tomu, aby útočník získal telefonní číslo oběti na svojí SIM kartu. Útočník obvykle opět technikou sociálního inženýrství vyláká na oběti některé soukromé informace, které následně využije při komunikaci s telefonním operátorem. Přestože není jednoduché se takovémuto typu útoku bránit, je možné to útočníkovi ztížit např. tím, že operátor umožní nastavit požadavek, že jakékoliv změně SIM musí předcházet fyzická kontrola.

9. Právní úprava Identity občana

Na základě všeho, co jsme se výše dozvěděli, je jasné, že Identita občana nám slouží k jednoznačné a nepopiratelné identifikaci v digitálním světě elektronických komunikací. Je jasné, že s rozvojem informačních a komunikačních technologií se postupem času nikdo z nás bez využití takového nástroje neobejde.

Proto, abychom mohli zjistit, jaké prostředky Identity občana můžeme využít, jaký prostředek je nejvhodnější pro konkrétní osobu s ohledem na službu, kterou chce využít, ale také jaké prostředky nám nabízí právní úprava, můžeme se podívat do platných právních předpisů. Zákony potřebujeme nejen pro naši informaci, která nás ujistí o výhodách využití Identity občana, ale také jako záruku právní jistoty, která nám umožní důvěřovat jednotlivým prostředkům.

Základem naší platné právní úpravy je nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, tzv. nařízení eIDAS. Ačkoliv se jedná o předpis Evropské unie, tak platí na celém jejím území včetně České republiky. Na tento evropský předpis navazuje naše národní legislativa, a to zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Nařízení eIDAS reguluje rovněž oblast elektronické identifikace, samotnou elektronickou identifikaci (prostřednictvím Národního bodu pro identifikaci – NIA) pak upravuje zákon č. 250/2017 Sb., o elektronické identifikaci, který např. stanovuje, za jakého předpokladu jsou systémy kvalifikovanými systémy elektronické identifikace nebo upravuje NIA jako informační systém veřejné správy podporující proces elektronické identifikace a autentizace.

Mezi další důležité zákonné normy řadíme zákon č. 111/2009 Sb., o základních registrech, který upravuje mimo jiné související identifikátory fyzických osob. Zákonných i podzákonných právních předpisů vztahujících se k možnostem naší elektronické identifikace, je více. Jistě není potřeba je uvádět všechny. Pro příklad můžeme ještě zmínit zákon č. 12/2020 Sb., o právu na digitální služby, zákon č. 328/1999 Sb., o občanských průkazech, zákon č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

Stanovení zákonných pravidel a jejich dodržování zajistí ve spojení s Vámi nastavenými bezpečnostními postupy, že vám Identita občana ulehčí každodenní činnosti, zabezpečí Vaše osobní údaje a ochrání Váš rodinný život.

10. Otázky a odpovědi

Vyplatí se mi Identita občana?

ANO, vyplatí

Kromě možnosti vyřešit řadu administrativních úkonů kdykoliv z pohodlí domova, bez objednávání a čekání na úřadě či na poště mi Identita občana může ušetřit i finanční prostředky. Např. získání výpisu z trestního rejstříku stojí na Czech POINTu cca 100,- Kč. Získání elektronické verze výpisu prostřednictvím služby Portál občana je zdarma a do 10 minut.

Mohu si vybrat, jaký elektronický identifikační prostředek budu využívat?

Tzv. "prostředky pro elektronickou identifikaci" prochází (dle nařízení eIDAS) schvalovacím řízením, a z hlediska míry zabezpečení jsou pak použitelné některé ze tří úrovní záruk (nízká, značná, vysoká). Při použití státní Identity občana je povinností poskytovatele služby (Service Provider), aby pro svoji transakci (službu) označil minimální požadovanou úroveň záruk (nízká nebo značná nebo vysoká). Jako uživatel si pak pro dané přihlášení můžete vybrat prostředek, který splňuje tuto minimální požadovanou úroveň záruk. V průběhu přihlašování by Vám systém správně neměl nabídnout přihlášení prostředkem, který tuto požadovanou úroveň záruk nesplňuje.

Je elektronická identifikace přes Identitu občana bezpečná?

Identifikace přes Identitu občana vykazuje vysokou míru důvěryhodnosti díky zaručenému ověření totožnosti a využívání druhého faktoru při přihlášení. Samotná bezpečnost je ale také závislá na zařízení a síti, ze které se uživatel přihlašuje. Proto není například vhodné přihlašování z nedůvěryhodných sítí (např. veřejná síť v kavárně) nebo ze sdílených počítačů, kde hrozí, že je zařízení napadeno škodlivým kódem. Dále neinstalovat na zařízení nedůvěryhodný software.

Jaké jsou moje náklady za využívání Identity občana?

Zřízení státní Identity občana je zdarma, není třeba ani platit žádné další poplatky. Státní identita má za účel urychlit, zlevnit, zjednodušit, a hlavně digitalizovat přístup občanu ke službám státu. To však nemusí platit u soukromoprávních.

Proč nemohu pro styk s veřejnou správou používat moje stávající eID (Google Account, Microsoft Account, Apple ID, Facebook ID a další)?

Základním nedostatkem těchto virtuálních identit je nedostatečné ověření totožnosti jejího skutečného držitele. Protože velká většina transakcí (byť jen výpisů) v rámci služeb veřejné správy vyžaduje jistou minimální míru ověření totožnosti jejího držitele, není bez řádného ověření totožnosti subjektu (dle požadavků nařízení eIDAS) možné tyto virtuální identity využívat – pravděpodobně by neprošly schvalovacím procesem. Přitom je možné, že např. územní samospráva nabídne pro jednoduchou personalizaci určité služby využití těchto virtuálních identit – např. pro rezervaci termínu návštěvy úřadu. Musí to být však takové použití, které nemá praktické dopady z důvodu negarantované skutečné identity jejího držitele.

Mám obavu ze státu jako "Velkého bratra". Mají jednotlivé úřady přehled o transakcích, které jsem prostřednictvím státní Identity občana provedl?

Požadavky na jednotlivá přihlášení, která provádíte prostřednictvím Identity občana v různých službách různých úřadů, se ukládají v rámci Národní identitní autority pouze z auditních důvodů a v minimální nutném rozsahu informací (např. kdy, jakým prostředkem, a pro který úřad/službu byla autentizace provedena). Tyto informace jsou přístupné pouze pro účely možných vyšetřování a auditů. Obsah vlastní transakce, kterou uživatel pod svojí Identitou občana provedl v dané službě daného úřadu, se neukládá nikde jinde než na tomto úřadu, a NIA ani žádný jiný úřad k obsahu transakce nemá přístup.

Mohu svoji státní Identitu občana využít i pro styk s veřejnou správou v jiných zemích EU?

Nařízení eIDAS (čl. 6) předpokládá vzájemné uznávání elektronických identit mezi členskými státy, za předpokladu, že Vámi využívaný prostředek je publikován v rámci systému elektronické identifikace, který je uveden na oficiálním seznamu v Úředním věstníku EU (viz čl. 9 odst. 2). Ostatní členské státy mají uznávat naše prostředky v úrovních "značná" a "vysoká" do 12 měsíců od jejich publikace a naopak.

Mají prostředky bankovní identity, vydávané bankami, nějaké nevýhody?

Ano, jednu nevýhodu mají. Na základě novely zákona o bankách, která bankám používání jejich prostředků reguluje, nemohou být tyto prostředky poskytnuty skrze státní systém NIA pro přihlášení ke všem poskytovatelům online služeb, ale jen určitým kategoriím. Konkrétně je možné, na základě § 38ad odst 3), poskytnout bankovní prostředky jen těm poskytovatelům, kteří patří do skupiny, vymezené termínem "státní orgán nebo orgán územního samosprávného celku". To znamená, že provozovatelé, kteří jsou na hranici této definice, nebo dokonce za ní, jako například portály nemocnic či školských zařízení, bankovní prostředky přes státní sytém NIA nebudou moci využít. Je samozřejmě možné, že si daný provozovatel nasmlouvá použití bankovních prostředků na komerční, tedy placené bázi, ale to se například u dvou výše jmenovaných dá očekávat jen výjimečně. Této nevýhodě se dá čelit tak, že si uživatel pomocí prostředku bankovní identity zřídí některý ze dvou státních prostředků (Mobilní Klíč eGovermentu, NIA ID), které popsanou regulací nejsou zasaženy. Touto regulací nejsou zasaženy ani ostatní nebankovní soukromoprávní prostředky, tedy I.CA a mojeID.

Je třeba mít více identifikačních prostředků?

Stačí mít zřízenou jednu, ale z praktických důvodů se doporučuje mít identity dvě. neboť druhá může být náhradou v případě ztráty přístupových údajů nebo nějakého prostředku sloužícího pro přístup.

11. Slovník, zkratky a pojmy

Odkaz na aktuální Výkladový slovník kybernetické bezpečnosti:

https://www.cybersecurity.cz/glossary.html

nebo
https://www.nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovnik_KB_3_vydani.pdf

Zkratky a pojmy:

Zkratka	Vysvětlení
Autentizace	Proces ověření, tj. že identita patří právě a jen osobě, která jí předkládá.
Autorizace	Proces získávání souhlasu s provedením nějaké operace, povolení přístupu někam nebo k něčemu.
CCID	Chip Card Interface Device
Credentials	Přihlašovací údaje. Data, požadovaná systémem pro ověření práva přístupu (většinou jméno a heslo)
ČNB	Česká národní banka
ČR	Česká republika
DIS+	Daňová informační schránka
DKP	Dokument konkretizujícího požadavky
DOK	Deblokační osobní kód
Doména	Nebo také doménové jméno. Je unikátní jmenná adresa na internetu odkazující na (typicky) server nebo počítač.
eID	Elektronická identita
eIDAS	Nařízení EP a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
eOP	Občanský průkaz s elektronickým čipem, vydávaný od 1.7.2018
EU	Evropská unie
Faktor autentizace	Důkaz prokázání identity založený na předložení znalosti nějakého důkazu (SMSky, jména, hesla).
Federativní	Sloučení nezávislých subjektů do celku s jedněmi pravidly

FIDO	Platforma FIDO, jež slouží k bezpečnému přihlašování k (webovým) službám a aplikacím.
IČ	Identifikační číslo
ID	Identita
Identifikace	Zjišťování totožnosti, ztotožnění někoho.
Inherentní	Charakterizuje atributy věcí. Obsažený v něčem, pevně spjatý, v jiném smyslu ale také zůstatkový.
IOK	Identifikační osobní kód
IP	Internet Protocol, jeden ze způsobu komunikace mezi zařízeními
ISO	International Organization for Standardization (Mezinárodní organizace pro normalizaci)
Level of assurance	Úroveň zajištění (identity), s níž lze důvěřovat identitě během procesu autentizace.
MITM	Man-in-the-Midle
NB	Notebook
NIA	Národní bod pro identifikaci a autentizaci, Národní identitní autorita
PC	Personal Computer, osobní počítač
PID	Poskytovatel identitních služeb
PIN	Personal Identification Number, Osobní identifikační kód
PUK	Personal Unlocking Key, Osobní odblokovací kód
QR	Quick response
ROS	(Základní) Registr osob
SMS	Short message service, krátká textová zpráva
SSL	Secure Socket Layer
SSO	Single sign-on
TLS	Transport Layer Security
URL	Uniform Resource Locator (jednotný lokátor zdroje)
USB	Universal serial bus, Univerzální sériová sběrnice nebo také port, přes který se připojují zařízení ve světě počítačů
WEP	Wired Equivalent Privacy
WiFi	Wireless (bezdrátová komunikace)
WPA	Wi-Fi Protected Access

12. Přílohy

12.1. Grafické znázornění – prostředky Identity občana

12.2. Grafické znázornění – bezpečnostní doporučení

Verze dokumentu

Datum	Verze	Změněno	Změna
28. 6. 2021	1.0	NAKIT, MV ČR, AFCEA, spolupracující organizace	Vytvoření dokumentu
25. 11. 2021	1.1	NAKIT	Přechod z eIdentita na Identita občana