Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Vícefaktorová autentizace a autorizace

Tadeáš Hájek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Tadeáš Hájek

Informatika

Název práce

Vícefaktorová autentizace a autorizace

Název anglicky

Multi-factor authentication

Cíle práce

Bakalářská práce je tématicky zaměřena na problematiku vícefaktorové autentizace a autorizace. Hlavním cílem práce je analýza možností a současných řešení pro vícefaktorovou autentizaci s použitím mobilního telefonu včetně porovnání jednotlivých aplikací.
Dílčí cíle práce jsou:
- vypracování přehledu zpracovávané problematiky a
- vypracování přehledu různých způsobů vícefaktorové autentizace pomocí mobilního telefonu.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část bude věnována různým způsobům vícefaktorové autentizace s použitím mobilního telefonu. Vlastní práce spočívá v analýze a porovnání jednotlivých aplikací pro vícefaktorovou autentizaci pomocí mobilního telefonu včetně charakteristiky těchto aplikací. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40 – 50 stran textu

Klíčová slova

autentizace, biometrie, mobilní aplikace, mobilní telefon, otisk prstu, rozpoznání obličeje, zpráva, verifikace, heslo

---

Doporučené zdroje informací

DASGUPTA, Dipankar, Arunava ROY a Abhijit NAG. Advances in User Authentication. Springer, 2017. ISBN 978-3-319-58808-7.

KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Věra Motyčková, MA

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 22. 02. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Vícefaktorová autentizace a autorizace" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3. 2023 _____

Poděkování

Rád bych touto cestou poděkoval vedoucí mé bakalářské práce Věře Motyčkové, MA za odborné vedení a cenné rady, které mi pomohly tuto práci zpracovat.

Vícefaktorová autentizace a autorizace

Abstrakt

Bakalářská práce se zabývá problematikou vícefaktorové autentizace a autorizace, blíže je zaměřena na rozdělení způsobů autentizace jako ověření na základě toho, co uživatel zná, vlastní, čím je nebo kde se nachází, dále je zaměřena také na jejich využití, vzájemné kombinování a bezpečnost. V teoretické části bakalářské práce jsou objasněny základní pojmy této problematiky, dále jsou také uvedeny rozdílné způsoby autentizace, kterým se práce podrobně věnuje. V praktické části bakalářské práce jsou charakterizovány mobilní aplikace určené k vícefaktorové autentizaci. Tyto mobilní aplikace jsou následně na základě předchozí charakterizace spolu porovnány a zhodnoceny.

Klíčová slova: autentizace, biometrie, mobilní aplikace, mobilní telefon, otisk prstu, rozpoznání obličeje, zpráva, verifikace, heslo

Multi-factor authentication

Abstract

The bachelor's thesis deals with the issue of multi-factor authentication, it is focused on the types of authentication methods such as verification based on what the user knows, owns, what he is or where he is and is also focused on their use, combination, and security. In the theoretical part of the bachelor's thesis the basic concepts of this issue are clarified and various kinds of methods of authentication are presented and explained in detail. In the practical part of the bachelors's thesis mobile applications intended for multi-factor authentication are characterized. These mobile applications are then compared and evaluated based on the previous characterization.

Keywords: authentication, biometrics, mobile application, mobile phone, fingerprint, facial recognition, message, verification, password

Obsah

1 Úvod

Vícefaktorová autentizace realizovaná s pomocí mobilního telefonu nebo mobilní aplikace se stala jednou z nejpoužívanějších metod zabezpečení nejrůznějších služeb. Ať už se jedná o internetové bankovnictví, emailové účty nebo účty na sociálních sítích. Způsobů vícefaktorového ověřování mobilním telefonem existuje několik. Mezi ty nejpoužívanější se řadí buď zaslání speciálního kódu prostřednictvím SMS na telefonní číslo uživatele nebo do emailové schránky uživatele. Oba tyto způsoby se však v dnešní době považují za méně bezpečné a více náchylné k útokům. Proto se dnes za nejlepší možnou variantu považují aplikace v chytrém telefonu. Autentizace může probíhat například opsáním speciálně vygenerovaného jednorázového hesla, potvrzením notifikace nebo také otiskem prstu či skenem obličeje. Potvrzení pomocí notifikace často obsahují přímo služby, kam se chce uživatel přihlásit, tento způsob nabízí například Seznam při přihlašování do emailové schránky, a to za použití jejich aplikace. Ostatní zmíněné způsoby mohou vyžadovat speciální aplikace určené k tomuto účelu. V dnešní době nabízí možnost vícefaktorové autentizace použitím k tomu určené mobilní aplikace stále větší množství služeb a některé to dokonce i vyžadují. Navíc s nárůstem mobilních zařízení s podporou biometrického ověřovaní bude tento počet jen stoupat. Biometrické ověřování nejen dělá celý proces více bezpečný, ale i ho výrazně zrychluje a zpříjemňuje. Některé služby například od Microsoftu dokonce podporují přihlašování bez hesla. Uživateli stačí zadat pouze uživatelské jméno a přihlášení potvrdit v mobilní aplikaci. Problematika vícefaktorové autentizace se ale netýká pouze mobilních telefonů a aplikací, jedná se o téma mnohem obsáhlejší, které má své využití v mnoha různých oblastech.

2 Cíl práce a metodika

2.1 Cíl práce

Bakalářská práce je tematicky zaměřena na problematiku vícefaktorové autentizace a autorizace. Hlavním cílem je analýza možností a současných řešení pro vícefaktorovou autentizaci s použitím mobilního telefonu včetně porovnání jednotlivých aplikací.

Dílčí cíle práce jsou:

- vypracování přehledu zpracované problematiky
- vypracování přehledu různých způsobů vícefaktorové autentizace pomocí mobilního telefonu

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část bude věnována různým způsobům vícefaktorové autentizace s použitím mobilního telefonu. Vlastní práce spočívá v analýze a porovnání jednotlivých aplikací pro vícefaktorovou autentizaci pomocí mobilního telefonu včetně charakteristiky těchto aplikací. Pro tento účel bude vybráno 8 nejpoužívanějších aplikací pro vícefaktorovou autentizaci pro iOS. Aplikace budou nejprve obecně charakterizovány a poté zhodnoceny použitím bodovací metody s váhami. K charakteristice a zhodnocení bude použit iPhone 13 s iOS ve verzi 16.2. Nejprve bude zvoleno 7 kritérií podle kterých budou aplikace hodnoceny a poté budou Saatyho metodou určeny jejich váhy. Po vypočtení vah budou aplikacím bodovací metodou přiřazeny body v jednotlivých kritériích. Minimální bodové ohodnocení bude zvoleno 1 a maximální 5. K vypočtení celkového počtu bodů aplikace budou použity váhy určené Saatyho metodou. Součet těchto bodů bude určen jako výsledné hodnocení aplikace, podle kterého budou aplikace porovnány. Podle výsledného hodnocení bude rovněž určeno pořadí aplikací. Následně na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

3 Teoretická východiska

3.1 Autentizace

Podle (Dasgupta, a další, 2017) je autentizace proces ověření identity uživatele, který omezuje přístup nelegitimních uživatelů do systému. A obecně se pro ověření identity uživatele používají čtyři typy autentizace.

- Co uživatel zná
    - Přihlašovací jméno, heslo, PIN kód, gesto, bezpečnostní otázka
- Co uživatel vlastní
    - HW token, SW token, občanský/řidičský průkaz, platební karta
- Čím uživatel je
    - Otisk prstu, sken oční sítnice, sken obličeje
- Kde se uživatel nachází
    - GPS, IP adresa

Tyto typy lze navzájem kombinovat a tím poskytovat lepší a bezpečnější způsob autentizace. Kombinace těchto typů se pak využívají ve vícefaktorové autentizaci

3.2 Autorizace

Autorizace je proces ověření přístupových oprávnění uživatele vstupujícího například do informačního systému a specifikuje, co daný uživatel může nebo nemůže. Tento proces ve většině případů navazuje na proces autentizace. Podstatou autorizace je tedy ověřit, zda daný uživatel má oprávnění provést příslušnou akci. (Matyáš, a další, 2008)

3.3 Vícefaktorová autentizace

Vícefaktorová autentizace je metoda ochrany přístupu k prostředku – například webu či informačního systému. O vícefaktorové autentizaci se mluví v případech, kde je třeba zajistit ověření identity více způsoby. Větší bezpečnosti se zde dosáhne diverzifikací zabezpečení – nejen co do počtu, ale i co do různých faktorů. Pro potencionálního útočníka je snazší získat přístup do systému, který je chráněn pouze autentizací na základě toho, co uživatel zná (heslo, PIN kód) a obtížnější, pokud systém vyžaduje potvrzení, u kterého je nutné použití něčeho, co uživatel vlastní (HW token, SW token). Standartní situace při přihlášení pomocí vícefaktorové autentizace může vypadat takto. Uživatel zná svoje přihlašovací jméno ve

specifickém tvaru (i to lze považovat za formu znalostního faktoru) a heslo (znalostní faktor). U sebe má SW token (například mobilní telefon s autentizační aplikací, faktor vlastnictví), který může být zároveň zabezpečený PIN kódem (znalostní faktor). Existují zde tedy tři informace, které musí uživatel znát a jedna věc, kterou musí mít při sobě. Na takovém principu funguje například přihlášení do emailu (pokud je zapnuté vícefaktorové ověření). (IDG, 2014)

3.3.1 Ověření uživatele na základě toho, co zná

Tento typ ověření je v praxi nejběžnější a nejpoužívanější. Informace používané k ověření by měly být a známy pouze danému uživateli. Jedná se například o hesla, PIN kódy, odpovědi na bezpečností otázky (například – jméno mazlíčka, jméno matky za svobodna, přezdívka …), nakreslení gesta pro odemčení mobilního telefonu, ale i o znalost uživatelského jména. Výhodou tohoto typu autentizace je, že se nejedná o fyzický objekt, ale o abstraktní znalost, kterou lze snadno přenášet či zadávat například do mobilního zařízení nebo počítače. Systémy pro tuto metodu autentizace lze také snadno ovládat a nevyžadují složitou údržbu. Nevýhoda tohoto typu autentizace spočívá v tom, že daná informace může být zjištěna, a to i bez vědomí uživatele. Další nevýhodou je fakt, že uživatel je nucen si informace pamatovat, což negativně ovlivňuje celkovou bezpečnost této autentizační metody především v případě, kdy se jedná složitá hesla. (Matyáš, a další, 2008)

Heslo

Heslo se skládá ze sekvence znaků používaných k ověření identity uživatele za účelem přístupu k různým zdrojům ve výpočetním systému. Hesla zároveň představují nejrozšířenější způsob autentizace uživatelů a používají se například k přihlašovaní do informačních systémů, emailů a jiných osobních účtů.

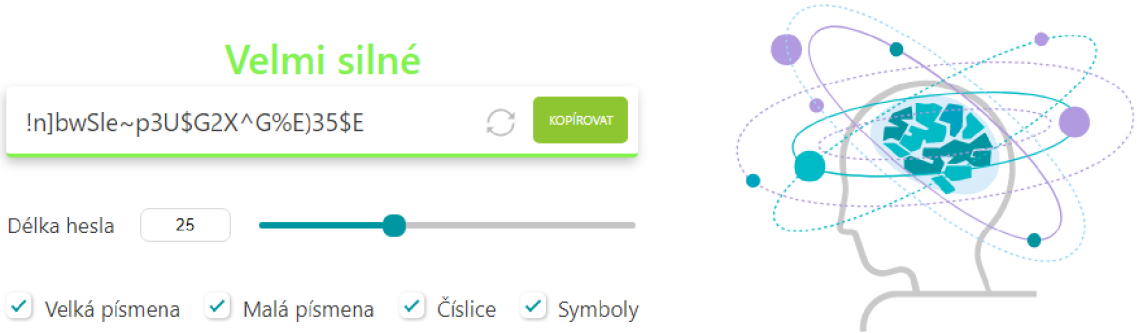
Výhodou hesel je jejich snadné použití a snadná implementace do systému. Čím je ale heslo kvalitnější, tím je obvykle pro uživatele hůře zapamatovatelné. Nevýhodou hesla je, že jej lze odpozorovat či ukrást. Další problém spočívá v procesu uložení hesla do systému tak, aby se k němu nedostal útočník, pokud se mu podaří do systému proniknout. Další potencionální riziko představuje i oprávněný správce systému, který mý přístup do celého systému a mohl by si tak heslo přečíst a následně jej zneužít. (Kolouch, a další, 2019)

Bezpečné heslo

Pro vytvoření bezpečného hesla by se měl uživatel řídit následujícími pravidly. Heslo by:

- mělo být minimálně 8 znaků dlouhé, ale je doporučeno vytvoření ještě delšího
- nemělo obsahovat uživatelské jméno, reálné jméno nebo název instituce (např. anonym123, pepanovak79 apod.)
- nemělo obsahovat lehce uhodnutelné nebo zjistitelné číselné kombinace (např. datum narození, výročí svatby, 123456, …)
- nemělo obsahovat ani žádná obecná slova (např. maminka, babicka, banka, …)
- mělo být odlišné od jiných používaných hesel hesel, tedy nepoužívat stejné heslo na internetové bankovnictví, sociální sítě, emaily apod.
- mělo obsahovat minimálně jeden z následujících znaků
    - Malá písmena (např. A, B, C, D, E, F)
    - Velka písmena (např. a, b, c, d, e, f)
    - Čísla (např. 0123456789)
    - Speciální znaky (např. ?!@&%#*/<>)

Další možností pro vytvoření silného a bezpečného hesla je použití generátoru náhodných hesel. Takový generátor automaticky vygeneruje bezpečné heslo pro požadovaný počet znaků.



Obrázek č. 1 - Generátor náhodných hesel od ESET

Z obrázku je patrné, že nejbezpečnějším heslem jsou náhodně seřazená malá a velká písmena spolu s číslicemi a symboly. Hesla takového typu jsou považována za nejlepší, protože jsou prolomitelná pouze takzvaným útokem hrubou silou (což je systematické kombinování

možností), který by, ale podobné heslo dokázal prolomit až za několik miliónů let. Problém takových hesel, ale spočívá v obtížnosti jejich zapamatování, proto je doporučeno využít například nějakou písničku, říkanku nebo citát a podobným způsobem si heslo vytvořit. Heslo na motiv písničky „Být stále mlád“ od Karla Gotta by mohlo mít následující podobu: ?By09St11Ml-17. Heslo je složeno z počátečních písmen písničky a k nim přiřazených symbolů a číslic. Při tvorbě hesla je doporučeno nepoužívat diakritiku, protože při pokusu o přihlášení z cizí země je možné že tamní zařízení nebudou obsahovat znaky pro českou diakritiku. Jak již bylo zmíněno, uživatel by měl pro každý účet používat jiné heslo a zapamatování takového množství hesel i přes různé mnemotechnické pomůcky může být obtížné. Řešením tohoto problému může být používání jednoho silného hesla, ale modifikovaného pro různé stránky. Například přidání počátečních písmen dané stránky ke stávajícímu heslu:

- ?By09St11Ml-17Em – Email
- ?By09St11Ml-17Fa – Facebook
- ?By09St11Ml-17In – Instagram
- ?By09St11Ml-17St – Steam

Takové řešení sice není ideální, ale je bezpečnější než používání stále stejného hesla. Dalším ulehčením může být zapamatování hesla prohlížečem. Ovšem i toto řešení má své nevýhody, postupem času může uživatel své heslo zapomenout nebo se do uloženého účtu může dostat někdo nežádaný, a to například při uložení hesla na dočasném zařízení nebo odcizeném zařízení. (CZ.NIC)

Podle dat firmy NordPass z roku 2021 bylo v České republice nejčastěji používáno těchto 30 hesel. (Nordpass)

Pořadí	Heslo	Pořadí	Heslo	Pořadí	Heslo
1	123456	11	123123	21	beruska
2	12345	12	maminka	22	1234567890
3	123456789	13	1234	23	123321
4	password	14	1234567	24	qwerty123
5	qwerty	15	michal	25	daniel
6	martin	16	milacek	26	martina
7	heslo	17	monika	27	lucinka
8	111111	18	sparta	28	159753
9	12345678	19	veronika	29	qwertyuiop
10	654321	20	slunicko	30	dominik

Tabulka č. 1 - Nejčastěji používaná hesla v České republice v roce 2021

PIN kód

Obecně platí, že PIN kódy slouží nejčastěji pro přístup k různým fyzickým zařízením např. k bankomatům, jsou krátké a pro zadávání se nejčastěji používá číselná klávesnice (použitelné znaky jsou pouze číslice 0-9). PIN kódy jsou ale obecně považovány za slabé zabezpečení. (Dasgupta, a další, 2017)

Přesto PIN kódy využívá část uživatelů k zabezpečení svého mobilního telefonu. A to z toho důvodu, že PIN kódy se na dotykové obrazovce zadávají lépe než hesla, která mohou být složena jak z číslic, tak písmen. Děje se tak, proto že při zadávání PIN kódu, který obsahuje jen číslice, se obvykle objeví obrazovka s velkými čísly, na které stačí kód jen naklepat. Naopak při zadávání hesla se objeví celá klávesnice, u které zadávání není tak rychlé, pohodlné a častěji dochází k překlepům. Přestože v dnešní době většina zařízení nabízí odemknutí telefonu pomocí bezpečnějších způsobů jako otisku prstu nebo skenu obličeje, tak přesto vyžadují sekundární zabezpečení jako PIN kód nebo heslo pro případ nefunkčnosti otisku prstu nebo skenu obličeje. (Spector, 2016)

Bezpečný PIN

Pro vytvoření bezpečného PIN kódu platí podobná pravidla jako pro vytvoření bezpečného hesla. Pravidla jsou následující: (ESET, 2019)

- PIN kódy by měly být unikátní – tedy jeden pro odemčení telefonu, jiný k platební kartě apod.
- Nepoužívat osobní informace – často se používají kódy, které mají pro uživatele nějaký význam. Například datum narození nebo výročí svatby. Tyto informace si může útočník většinou lehce dohledat, a to například přes sociální sítě.
- Náhodná série čísel – ideálně by měl být PIN kód náhodná posloupnost čísel – potenciální útočník pak nemůže heslo uhádnout nebo zjistit ze sociálních sítí, ale bude ho muset prolomit hrubou silou
- Používat šestimístné kódy – šestimístné kódy jsou bezpečnější než ty čtyřmístné, a to z důvodu většího možného počtu kombinací kódu – kód je tedy obtížnější prolomit
- Obměňovat kódy – uživatel by měl kódy po určité době měnit – kód mohl například někdo bez vědomí uživatele zjistit nebo vidět

Podle (ESET, 2019) jsou nejčastěji používané PIN kódy následující:

0000	4444	8888	1010	2000
1111	5555	9999	1122	2001
2222	6666	1234	1212	1004
3333	7777	4321	1313	6969

Tabulka č. 2 - Nejčastěji používané PIN kódy

Z dat firmy ESET (viz. Tabulka č.1) vyplývá, že využití PIN kódů jako způsobu zabezpečení mobilních telefonů postupem let v České republice klesá. V roce 2016 používalo PIN kód 39 % uživatelů, v roce 2017 32 %, v roce 2018 28 % a v roce 2019 už pouze 25 % uživatelů. Od roku 2016 do roku 2019 tedy klesl počet uživatelů o 14 %. V roce 2020 naopak počet Čechů používajících PIN kód vzrostl na 28 %. Je ale jasné, že obliba PIN kódů klesá, a to hlavně kvůli možnosti odemčení zařízení pomocí otisku prstu nebo skenu obličeje.

Bezpečnostní otázka

Bezpečnostní otázky jsou kladeny během autentizačního procesu s cílem poskytnout další úroveň zabezpečení pro ověření přihlašovacích údajů uživatele. Otázky většinou souvisí s osobním nebo profesním životem. Mnoho webových stránek používá bezpečnostní otázky například k obnovení hesla. Odpověď na bezpečnostní otázku mohou vyžadovat i pracovníci IT podpory, a to pro ověření totožnosti například při telefonátu. Problém bezpečnostních otázek spočívá v jejich obecnosti a v tom, že řadu z nich si je útočník schopen zjistit nebo uhádnout (např. název střední školy nebo první navštěvované školy, město narození, jméno partnera, oblíbená barva, jméno prvního mazlíčka apod.). Právě kvůli jejich obecnosti může nevědomky poskytnout odpověď i sám uživatel. Řešením by bylo zvolení těžší otázky nebo záměrně chybně odpovědět na danou otázku. Obě tyto možnosti ale nesou riziko, že uživatel odpověď po čase zapomene. (Dasgupta, a další, 2017)

Podle článku (Sham, 2021) by měla mít odpověď na dobrou bezpečnostní otázku tyto charakteristiky:

- Nikdo by ji neměl být schopný uhádnout, vyhledat nebo jinak zjistit. Toto je nejdůležitější vlastnost, kterou má odpověď mít – pokud lze odpověď snadno zjistit tak je ohroženo zabezpečení celého účtu.
- Měla by být snadno zapamatovatelná, aby si jí uživatel pamatoval ještě dlouho po samotném vytvoření účtu.
- Odpověď na danou otázku by se neměla v průběhu času měnit a měla zůstat stále stejná. Proto je dobré vyhnout se odpovědím, které jsou platné pouze v daném okamžiku jako jsou různé oblíbené věci – například jídlo či film.
- Zároveň by odpověď měla být jednoduchá, přesná a pro uživatele jasná. Otázky s nejednoznačnými odpověďmi, které vyžadují rozlišování malých a velkých písmen nebo konkrétní formátování mohu být po delší době obtížnější na správné zodpovězení.
- Na otázku by mělo být i více možných odpovědí, protože čím je více možných odpovědí na otázku tím je menší šance, že se někomu podaří odpověď uhádnout nebo ji získat „hrubou silou“.

3.3.2 Ověření uživatele na základě toho, co vlastní

Tento způsob ověření bývá realizován držením určitého tokenu uživatelem (např. čipové karty, klíče, osobních dokladů apod.). Tuto funkci ale v dnešní době může zastávat i mobilní telefon, a to například pomocí aplikace určené k tomuto účelu. Nevýhodou ověření na základě vlastnictví je skutečnost, že i tato zařízení je možné předat, zcizit nebo ztratit. Navíc jsou s jejich použitím často spojeny výrazně vyšší náklady než při ověření na základě toho, co uživatel zná. (Kolouch, a další, 2019)

Podle literatury (Rak, a další, 2008) vlastnictví uměle získaných nebo přidělených identifikačních charakteristik patří k nejrozšířenějšímu způsobu určovaní vnější identity člověka. Určení identity člověka je důležité pro umožnění jeho oprávněného přístupu (nebo naopak jeho odmítnutí) mezi další lidi, do společnosti (organizace, instituce) uzavřenějšího charakteru, k různým hmotným objektům, technickým zařízením, prostředkům, finančním a jiným zdrojům, a v poslední době zejména k informacím a informačním technologiím. Nezanedbatelné jsou i důvody administrativní, ekonomické a bezpečnostní, včetně výkonu státní správy, činnosti policie, kriminální služby. Z důvodu identifikace jsou člověku uměle přisvojovány vnější identifikační znaky jinými lidmi (státními zaměstnanci, personálními pracovníky, zaměstnavateli nebo bezpečnostními specialisty), nebo si je daný člověk sám vědomě a dobrovolně vybírá a přivlastňuje. Mezi identifikační charakteristiky za zařazují:

- Jméno a příjmení
- Osobní doklady
- Identifikační čísla a kódy
- Identifikační karty a čipy
- Biočipy

Osobní doklady

Osobní doklady jsou nejběžnějším příkladem ověřovaní uživatele na základě toho, co vlastní. Obsahují osobní údaje jako – jméno a příjmení, datum narození, adresu, identifikační číslo, rodné číslo, fotografii a další údaje k identifikaci osoby. Typický příklad je občanský nebo řidičský průkaz. (Dasgupta, a další, 2017)

Přístupové karty

Přístupové karty se nejčastěji používají při automatické autentizaci. Proces ověření je automatizovaný, a tedy i výrazně rychlejší ve srovnání s těmi neautomatizovanými (např. ověřování pomocí osobních dokladů) u kterých je nutnost ruční kontroly. Nicméně neautomatizované systémy jsou schopny například ověřit identitu držitele karty což mnohé jednoduché automatizované systémy nedokáží. (Dasgupta, a další, 2017)

Obrázek č. 2 - Přístupová karta

Hardwarové tokeny

Klasickým představitelem HW tokenu je RSA token, který používá pro generování kódu čas. Další variantou je například Yubikey, který slouží jako jednoúčelová klávesnice a ke generování přístupového kódu používá sekvenční metodu. Princip fungování je následující:

- Každý token je unikátně identifikován
- Autentizační server má tento token přiřazen k uživateli
- Token generuje přístupový kód dle definovaného algoritmu (na základě času či sekvenční metodou
- Server zaslaný kód porovná na své straně s kódem, který si vygeneruje stejným algoritmem
- Pokud se kódy shodují, je uživatel tímto faktorem ověřen

Výhoda tohoto přístupu je zjevná, aby někdo zfalšoval přístup někoho jiného, musí kromě uživatelského jména a hesla získat i fyzický přístup k tokenu. Nevýhody HW tokenů spočívají především v nenulové pořizovací ceně a potřebě fyzicky spravovat životní cyklus tokenu (vydání, obměna, skartace). V případě osamostatněných tokenů je též vyšší riziko man-in-the-middle útoků. (IDG, 2014)

Obrázek č. 3 - Hardwarový token

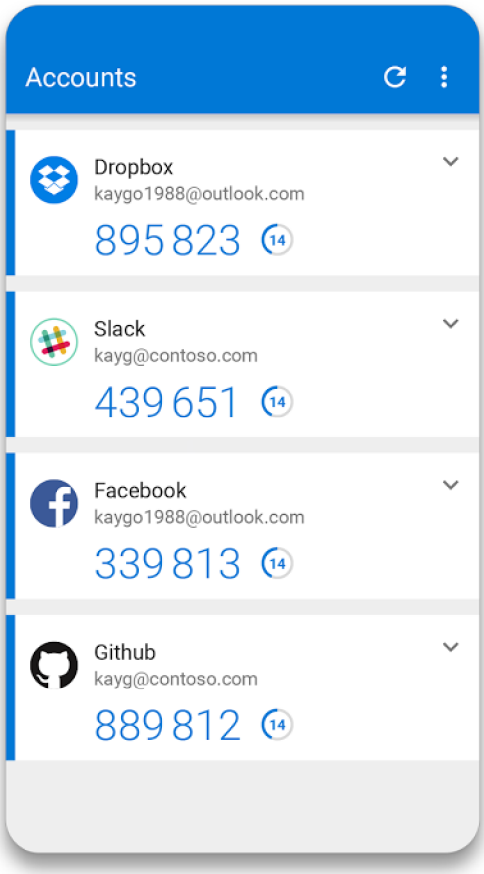
Softwarové tokeny

Trendem, řešící některé nevýhody svých hardwarových protějšků, jsou softwarové tokeny. Jedná se typicky o aplikace na chytrém telefonu. Použití je shodné. Software v telefonu se spáruje s autentizačním serverem a od té doby generuje klíče kterým autentizační protějšek rozumí. Výhodou je, že tento přístup umožňuje kombinovat autentizační tokeny pro více služeb v jednom zařízení. Není tedy nutné pro každý server mít vlastní hardwarový token, vše obstará aplikace, která generuje kódy pro všechny zaregistrované služby najednou. Ovšem i SW tokeny mají své nevýhody. Například rizika jsou podobná jako u HW tokenu. Dopady ztráty zařízení však mohou být vyšší, což je spojenu s tím, že SW tokeny se častěji používají online (na rozdíl od korporátní sféry u HW tokenů), kde je složitější reautorizace. Přistup k tomuto problému je různý:

- Některá řešení vyžadují mít záložní jednorázové kódy. V takovém případě je možné se po ztrátě/reinstalaci zařízení znovu autorizovat vůči cílové aplikaci, kterou je třeba následně znovu propojit s generátorem autentizačních kódů (reautorizace)

- Jiná řešení si poradí i s reinstalací chytrého telefonu, neboť jim pro reautorizaci stačí SIM karta. Zde při ztrátě mobilního telefonu stačí získat zpět své původní mobilní číslo. Některé aplikace také nabízejí možnost zálohy do cloudu
- Poslední možností je kontaktování poskytovatele služby. Ten pro ověření uživatele jiným způsobem (např. PIN, sken dokumentů) provede vypnutí vícefaktorové autentizace a umožní její reinicializaci uživatelem

Velkým rizikem u tohoto faktoru je ale samo zařízení, na němž aplikace SW tokenu funguje. Bezpečnost faktoru je totiž závislá na zabezpečení celého přístroje. Jaké nebezpečí může hrozit, je vidět například u autorizačních SMS – pokud má škodlivá aplikace právo ke čtení těchto zpráv, může se útočník ovládající aplikaci vydávat za legitimního uživatele. (IDG, 2014)



Obrázek č. 4 - Softwarový token – Microsoft Authenticator

3.3.3 Ověření uživatele na základě toho, čím je

Tímto způsobem ověření se zabývá biometrie (obor zabývající se měřením a vyhodnocováním biologických charakteristik a charakteristik chovaní lidí), která rozpoznává jedinečné biologické charakteristiky daného uživatele. Existuje několik charakteristik, u nichž se předpokládá nebo je prokázáno, že jsou pro každého člověka unikátní. Tyto charakteristiky jsou často využívány jinými vědními obory (např. kriminalistika) k jedinečně identifikaci člověka. (Kolouch, a další, 2019)
Uživatele je možné ověřit například podle:

- Otisku prstu
- Obličeje
- Dynamiky při psaní
- Hlasu
- Geometrie ruky
- Podpisu
- DNA
- Mozkových vln
- Oční duhovky
- Oční sítnice
- Krevního řečiště

Tento typ autentizace je považován za více bezpečný ve srovnání s ostatními typy. Zatímco u ověřovaní na základě toho, co uživatel zná nebo co vlastní je informace možné sdílet, tak u tohoto typu ověřovaní je to téměř nemožné nebo velmi obtížné. Díky obtížnosti padělaní údajů se tento způsob autentizace využívá pro přístup k vysoce zabezpečeným systémům či zařízením. Navíc je tento způsob autentizace zcela automatizovaný, tudíž i velmi rychlý. Nicméně jeho nevýhodou je nutnost pořízení často nákladného speciálního hardwaru, který zaznamená dané biologické charakteristiky. Narozdíl od ostatních typů autentizace nemusí zadávaný údaj přesně odpovídat tomu uloženému v databázi se kterým se srovnává. Vstupní údaj musí spadat do přijatelného procenta správnosti, které je pro daný systém nastaveno. Čím nižší je procentuální úroveň, tím vyšší je šance že systém vrátí falešně pozitivní výsledek (uživatel, který by neměl mít přístup ho dostane). Naopak čím vyšší je procentuální úroveň tím

vyšší je šance že sytém vrátí falešně negativní výsledek (uživatel, který by měl mít přístup ho nedostane). (Dasgupta, a další, 2017)

Biometrická autentizace se rozděluje do dvou kategorií:

- Založená na behaviorálních charakteristikách – to jsou ty atributy, které souvisí s určitým vzorem chování člověka. Například:
    - Způsob, jakým člověk mluví (hlas)
    - Způsob, jakým člověk chodí (chůze)
    - Způsob, jakým člověk píše (údery na klávesnici)
- Založená na fyziologických charakteristikách – to jsou ty atributy, které souvisí s lidským tělem a nelze je snadno změnit. Tyto atributy jsou spolehlivější než ty behaviorální. Řadí se do nich například:
    - Rozpoznání obličeje
    - Otisk prstu
    - Sken oční sítnice

Rozpoznání stylu chůze

Rozpoznávání chůze je vizuální typ rozpoznávání, který člověka autentizuje na základě toho, jakým stylem chodí. Existují dva způsoby, jak rozeznat styl chůze. Prvním je člověka při chůzi natočit a změřit trajektorii kloubů a úhly pohybů nohou a v průběhu času tak generovat unikátní šablonu chůze daného člověka. Druhý způsob využívá radarovou technologii k zaznamenání cyklu chůze člověka během jeho chůze a na základě toho opět generuje unikátní šablonu. Několik výzkumů ukázalo, že styl chůze jde identifikovat i pomocí různých nositelných senzorů. (Dasgupta, a další, 2017)

Rozpoznání stylu psaní

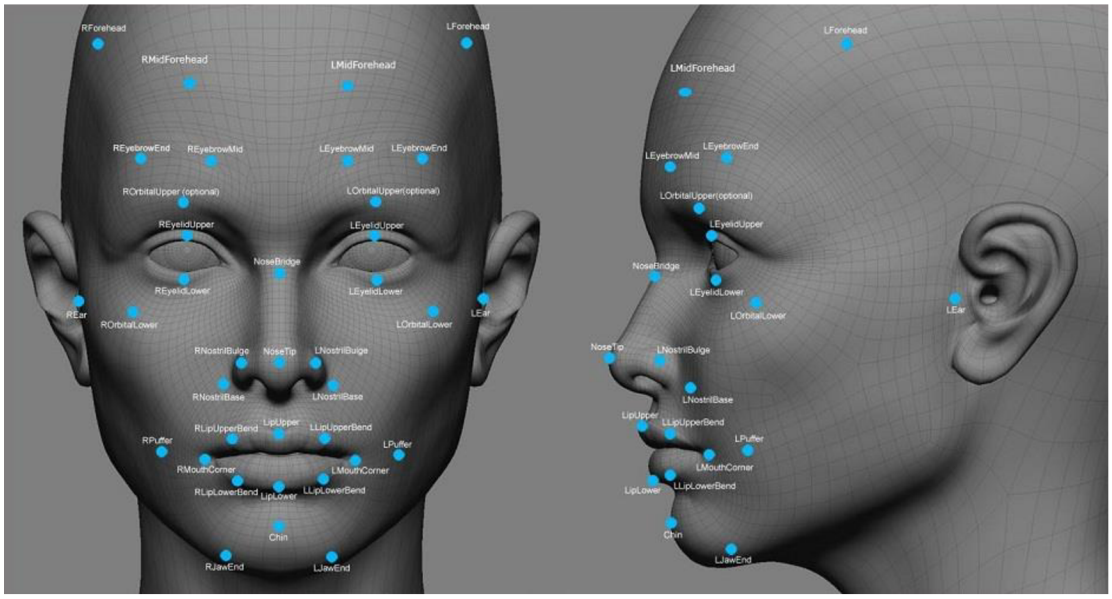
Rozpoznávání na základě úhozů na klávesnici je dalším typem behaviorální autentizace, který porovnává vzorce psaní uživatelů. Toho lze dosáhnout sledováním toho, jak dlouho uživateli trvá přesun mezi klávesami, jakou silou jsou klávesy stiskávány a jaká je doba mezi stisknutím a uvolněním klávesy. (Dasgupta, a další, 2017)

Rozpoznání hlasu

Jedná se o zvukový typ autentizace, který využívá styl mluvy člověka (tón, výšku, rychlost atd.) pro měření zvukových vln. Konkrétně se jedná o způsob rozpoznávání mluvčího (identifikace toho kdo mluví) spíše než rozpoznávání řeči (rozpoznávání toho co je mluveno). Systém rozpoznávání mluvčího se dá rozdělit do dvou kategorií. Textově závislý a textově nezávislý. Pokud při zápisu/registraci zazní stejný text pro účely verifikace tak se jedná o textové závislý autentizační systém.

Rozpoznání obličeje

Rozpoznávání obličeje je vizuální typ rozpoznávání, který bere obraz obličeje a měří například vzdálenost očí, šířku nosu, vzdálenost lícních kostí, rty (polohu, tvar, orientaci), relativní výšku čela a mnoho dalších charakteristických znaků. Rozpoznávání obličeje má sice své nedostatky jako například – citlivost na změny ve světelných podmínkách nebo úhel kamery, ale jeho velkou výhodou je, že zaručuje jednoznačnou identifikaci osoby a tím zabraňuje krádeži identity. (Dasgupta, a další, 2017)



Obrázek č. 5 - Významné body na obličeji

Dvojrozměrné snímání

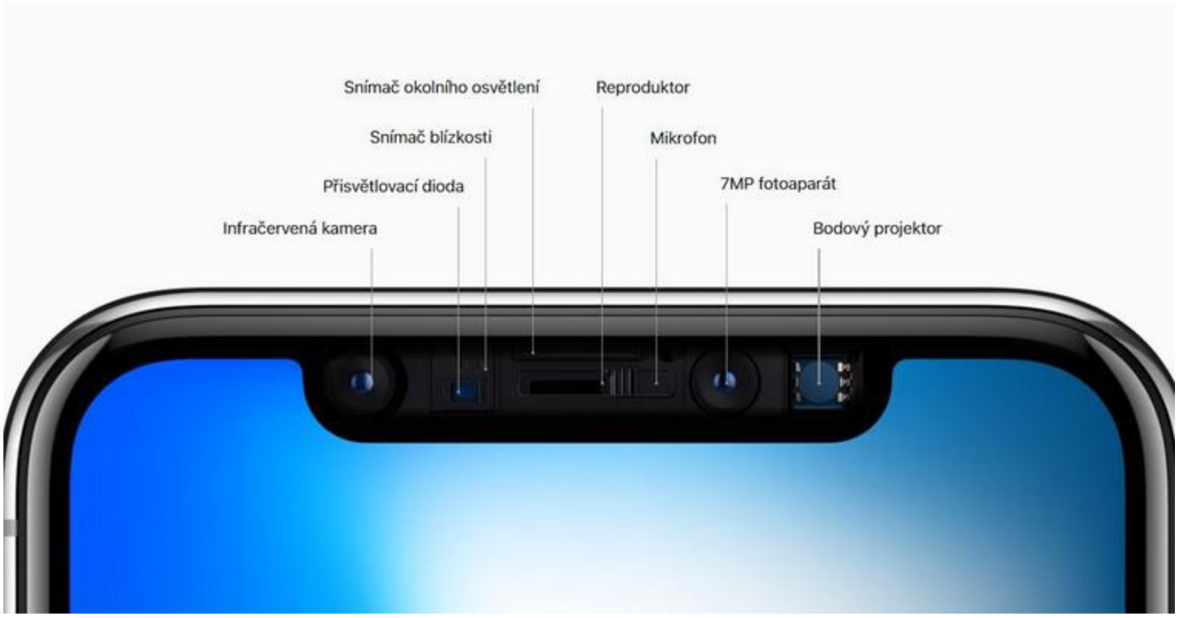
Dvojrozměrný sken obličeje obecně funguje tak, že telefon pomocí přední kamery vyfotí fotky z několika úhlů, které se uloží. Pří následném přihlašování telefon porovnává tyto fotky s nově pořízenými a pokud nenajde výrazné rozdíly telefon se odemkne. Ovšem existují rozdíly

v přístupu k 2D odemykání obličejem. Některé telefony k odemykání využívají jen obyčejné fotky, jiné i infračervenou kameru či ToF senzor (Time-of-flight senzor, který používá k výpočtu vzdálenosti čas) a některé počítají i s tím, že se člověk pohne a z videa jsou schopné pracovat částečně i s trojrozměrným obrazem. Nevýhoda snímání pouze na základě fotky spočívá v tom, že systém většinou není schopný určit, zdali se jedná o skutečný obličej nebo pouze jeho fotografii. Řešením tohoto problému může být například infračervené rozpoznávání obličeje které ale vyžaduje k přední kameře další hardware. Telefon v tomto případě opět pořídí snímek obličeje, ale v infračerveném spektru. Výhoda tohoto způsobu spočívá v tom, že infračervené kamery nepotřebují, aby byl obličej dobře osvětlený a dokáží fungovat i za špatných světelných podmínek. Jsou také mnohem odolnější vůči pokusům o prolomení, protože infračervené kamery využívají k vytvoření obrazu tepelnou energii. Bezpečnost, rychlost a spolehlivost se tedy liší v závislosti na daném telefonu. Dvojrozměrné snímání se využívá především kvůli nižším výrobním nákladům oproti trojrozměrnému snímání. (Alza, 2020) (Kos, 2022)

Trojrozměrné snímání

Trojrozměrné snímání obličeje představuje bezpečnější mechanismus, který nelze oklamat fotografií obličeje. Vyžaduje další senzory, např. infračervený promítač, který vytváří takzvanou hloubkovou mapu uživatelova obličeje. Dochází při něm k výpočtu, za jak dlouho se světlo vydávané kamerou odrazí od tváře a vrátí se zpět k telefonu. Následně pak systém vytvoří 3D model obličeje. Zkoumání obličeje uživatele je tak podrobnější a tím pádem i bezpečnější než dvojrozměrné snímání. Trojrozměrné snímání obličeje pak funguje dobře i za špatných světelných podmínek. Tento způsob snímání využívá například Face ID od Apple.

Face ID využívá řadu senzorů k zachycení trojrozměrné reprezentace obličeje. Přední kameru používá jen částečně, protože většinu údajů získávají ostatní senzory skenující tvář. Je zde využíván osvětlovač, infračervený bodový projektor a infračervená kamera. Osvětlovač jako první nasvítí obličej infračerveným světlem, bodový projektor na něj promítne na 30 tisíc infračervených teček, které snímá infračervená kamera. Ta z nich vytvoří hloubkovou mapu tváře a tím získá přesné údaje o obličeji. Vyhodnocování pak provádí neuronový engine, který mapu porovnává s nasnímanými daty při aktivaci funkce. (Alza, 2020) (Kos, 2022)



Obrázek č. 6 - Snímače na iPhone X

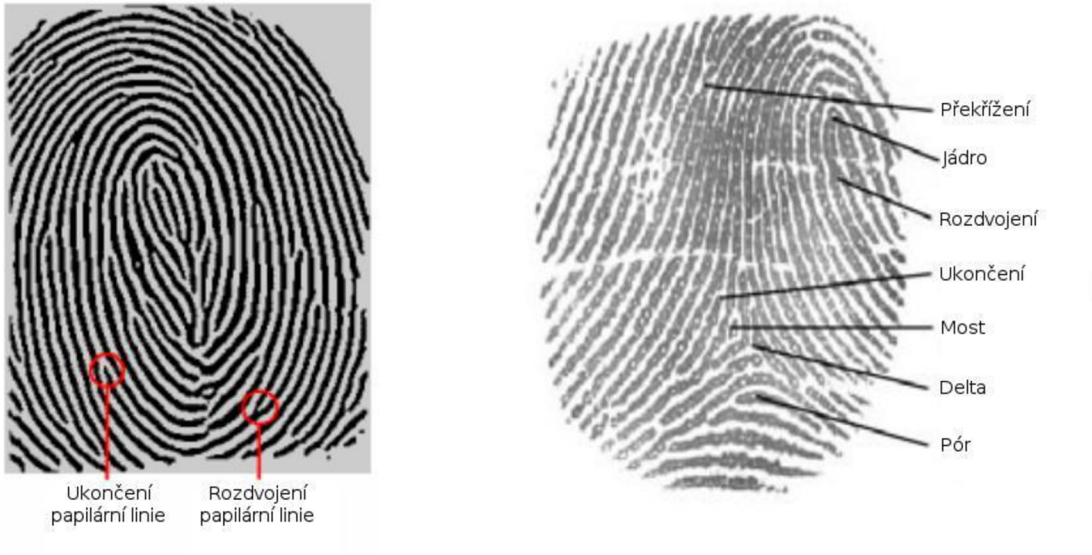
Bezpečnost

Odemykání obličejem se považuje za bezpečný způsob ochrany telefonu, zejména pak varianta trojrozměrného snímání. Podle Apple je u Touch ID (odemykání otiskem prstu od firmy Apple) šance na odemknutí telefonu náhodným prstem 1:50 000. Naopak u Face ID je riziko podstatně menší a to 1:1 000 000. Face ID je tedy dle Apple několikanásobně bezpečnější než Touch ID. Vysokou míru zabezpečení, ale mohou zajišťovat i určitá řešení dvojrozměrného snímání. (Alza, 2020)

Otisk prstu

Rozpoznávání otisku prstu je vizuální typ autentizace, který využívá povrchu konečku prstu. Jedná se zároveň o nejrozšířenější biometrickou metodu autentizace. Využívá se zde analýza papilárních linií, jinými slovy jsou zde vyhledávány prohlubně a hřebeny snímaného otisku prstu. Obecný princip fungování je následující – digitální snímek prstu je pořízen pomocí skeneru otisků prstů, systém pak najde unikátní body na konečcích prstů a spáruje obrázek s nalezenými v databázi. (Dasgupta, a další, 2017)

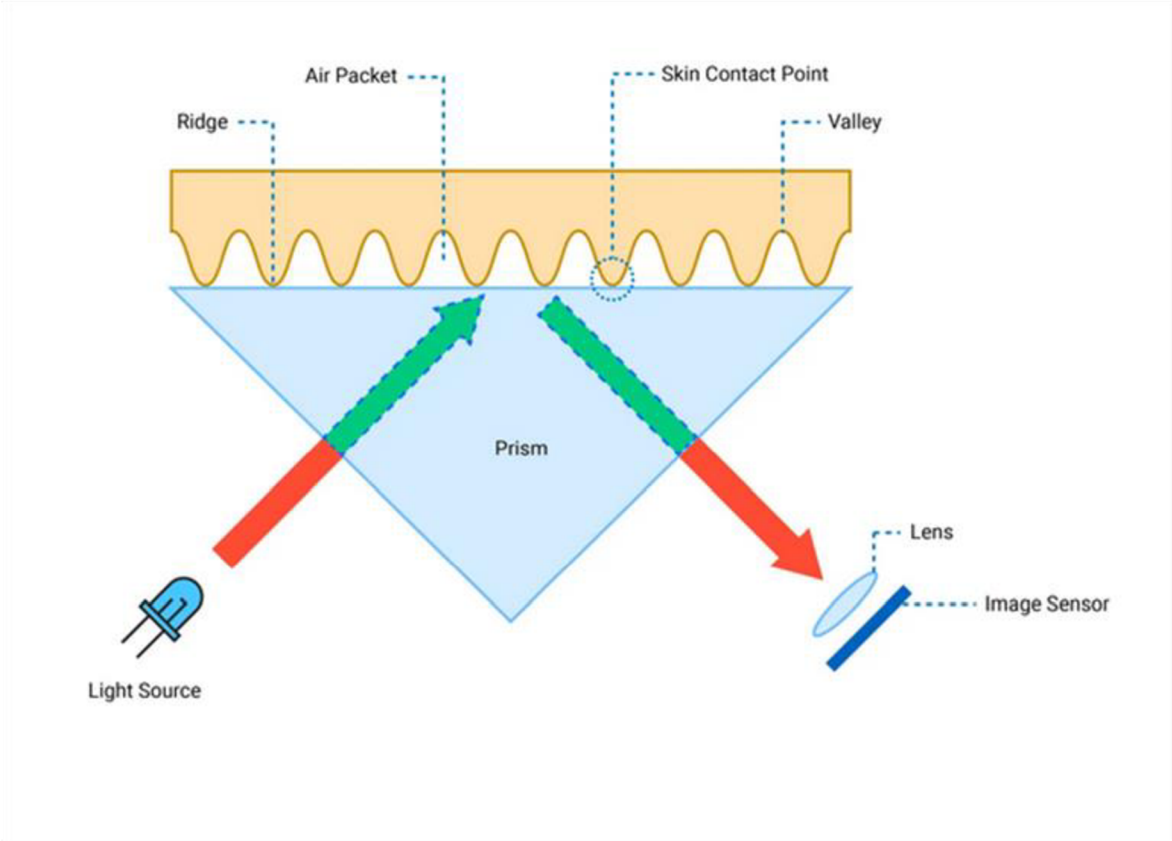
Podle dat z grafu č. 1 stoupá využívanost otisku prstu jako způsobu zabezpečení mobilních telefonů. V roce 2016 používalo otisk prstu jen 5 % uživatelů, v roce 2017 už, ale tento počet vzrostl na 20 %, v roce 2018 na 32 % a v roce 2019 dokonce až na 39 %. Z předešlých dat jasně vyplývá, že obliba odemčení pomocí otisku prstu roste, a to například na úkor odemykání pomocí gesta.



Obrázek č. 7 - charakteristické znaky otisku prstu

Optické skenery

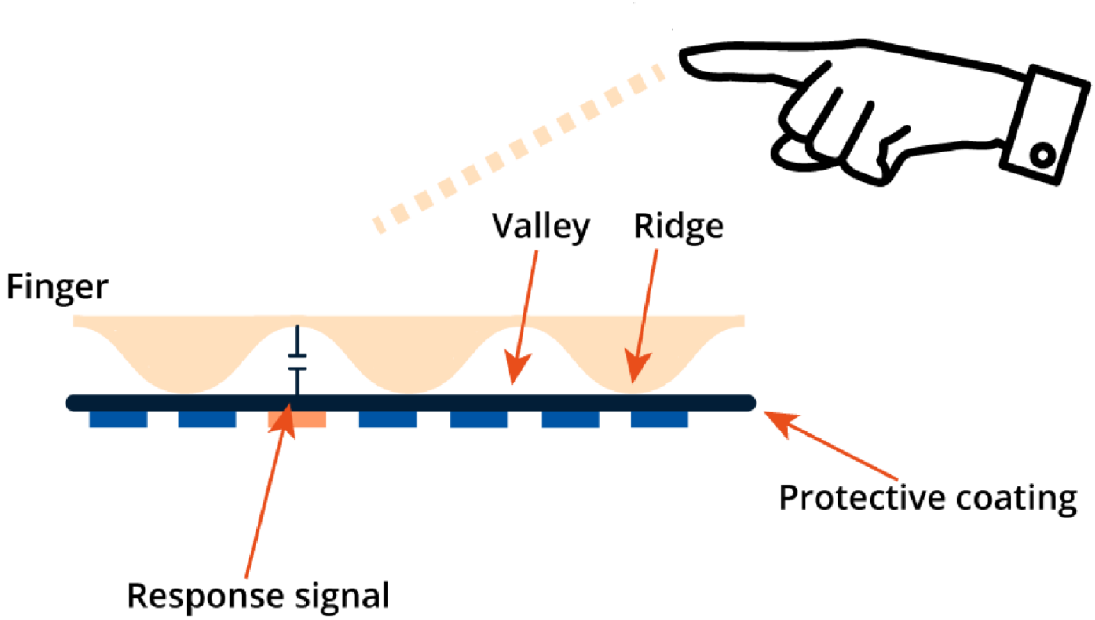
Optické skenery jsou nejstarší používanou metodou pro snímání otisků prstů. Tato technologie nejprve získá obraz daného prstu a následně pomocí algoritmu analyzuje papilární linie. Algoritmus pracuje na principu analýzy světlých a tmavých míst na získané fotografii, čím je tedy fotografie kvalitnější a detailnější s tím větší přesností dokáží algoritmy vypočítat, kde se přesně papilární linie nachází. Nevýhodou optických čteček je že obraz je zachycován pouze ve 2D podobě, je tedy možné s pomocí kvalitně vyfocené kopie otisku prstu systém oklamat. Tyto senzory se většinou vyskytují u levnějších mobilních telefonů. (Moravec, 2016) (e3displays)



Obrázek č. 8 - Princip fungování kapacitních skenerů otisku prstu

Kapacitní skenery

Jedná se o nejčastěji používaný typ skenerů v mobilních telefonech. Není zde vytvářen klasický obraz otisku prstu, ale namísto toho je pomocí kondenzátorů uchováván elektrický náboj. Tento skener má takovou citlivost, že dokáže po přiložení prstu rozpoznat, kde se nachází papilární linie právě díky změně elektrického náboje. Čím více kondenzátorů je na skeneru umístěnu tím přesnější, a tedy i bezpečnější otisk prstu bude. Rozptyl kvality kapacitních skenerů se pohybuje od stovek kondenzátorů u těch nejjednodušších, až po tisíce kondenzátorů u těch nejpřesnějších. Největší výhodou tohoto typu skeneru oproti optickému typu je vyšší bezpečnost. I pokud by si útočník vytiskl 3D mapu povrchu prstu tak ho čtečka stejně nerozpozná, protože různé materiály mění velikost náboje v kondenzátorech různými způsoby a ty v mobilních telefonech jsou uzpůsobeny na lidský prst. Jediným způsobem, jak tento typ čteček prolomit je softwarový útok. Naopak nevýhodou těchto senzorů oproti těm optickým je vyšší cena. (Moravec, 2016)



Obrázek č. 9 - Princip fungování kapacitních skenerů prstu

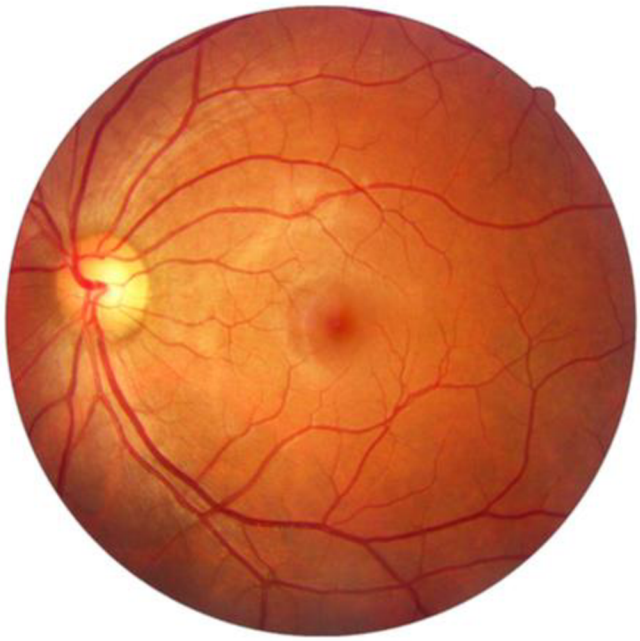
Ultrazvukové skenery

Ultrazvukové skenery jsou novým typem senzorů určených pro čtečky otisků prstů v mobilních telefonech. Princip fungování je následující – senzor je vybaven ultrazvukovým vysílačem a ultrazvukovým přijímačem, ultrazvukový signál je vyslán směrem k prstu, který je ke snímači přiložen, signál je následně od prstu odražen nazpět. Poté přijímač vyhodnotí, za jak dlouho dobu se signál vrátil nazpět a podle toho určí, zda se jedná o správný otisk prstu. Čím delší dobu je prst ke čtečce přiložen tím detailnější otisk prstu se podaří získat. Tento typ skenerů je považován za ještě bezpečnější než kapacitní senzory, prolomení lze rovněž prakticky zajistit pouze softwarově. (Moravec, 2016) (e3displays)

Skenery otisků prstů jsou v mobilních telefonech založeny na některém ze tří výše popsaných principů. To co, ale opravdu rozděluje jednotlivé čtečky od sebe jsou dodatečné komponenty a software. Každý výrobce používá své algoritmy a způsob porovnání skenu otisku prstu. Jedním způsobem je porovnání do detailu celého skenu. Druhým způsobem je vyhledání kde jednotlivé linie splývají v jednu nebo úplně končí. Tato splývající nebo konečná místa jsou pak porovnána s předlohou, která byla zaznamenána stejným způsobem. A tím, že není porovnáván celý otisk je ušetřen výpočetní výkon i čas. (Moravec, 2016)

Sken oční sítnice

Jedná se o počítačový rozpoznávací systém, který září světlo do zadní části oka, a protože krevní cévy absorbují světlo jinak než okolní tkáně, proces umožňuje počítači získat přesnou distribuci krevních cév, která je pro každého člověka jedinečná. Poté, podobně jako při rozpoznávání otisku prstu počítač najde jedinečné body na snímku a měří vzdálenosti mezi nimi. Kromě vzorů krevních cév se také používají vzory žil k nalezení jedinečných vlastností. Sken sítnice vyžaduje značně větší úsilí než sken oční duhovky a je citlivější i na pohyb oka. Tedy i sebemenší pohyb může způsobit odmítnutí uživatele autentizačním systémem. K zachycení sítnice jsou také potřeba mnohem sofistikovanější kamery, než které se dají použít k rozpoznáni obličeje. (Dasgupta, a další, 2017)



Obrázek č. 10 - Oční sítnice

3.3.4 Ověření uživatele na základě toho, kde se nachází

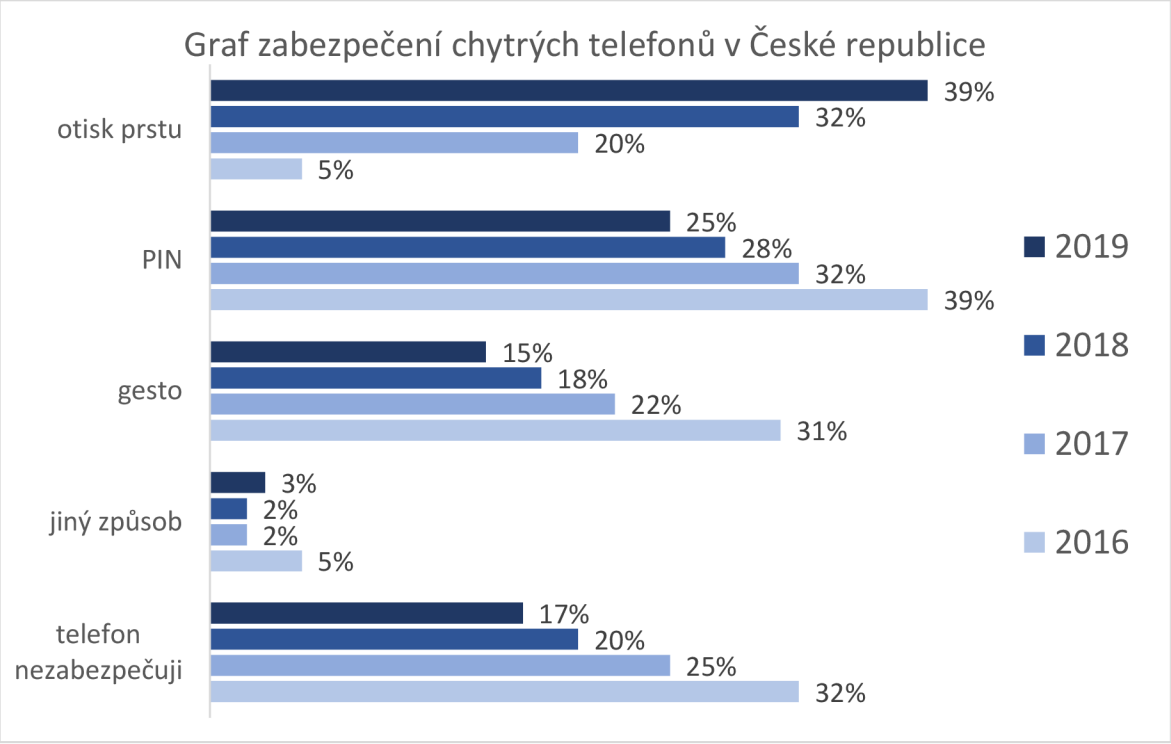
Tento typ autentizace využívá umístění uživatele k ověření jeho identity. Nejčastěji se k tomuto účelu využívá GPS, IP adresa nebo ID vysílače. Obecně se používá ve spojení s jiným typem autentizace. Například pokud má uživatel správné přihlašovací údaje tak systém ověří kde se nachází a na základě toho určí, zda má uživatel oprávnění se z daného místa do systému přihlásit. Také může sledovat kdy a odkud se uživatel přihlásil. Například pokud se uživatel přihlásí z Prahy a za 30 minut znovu z Londýna. Tak v daném čase je takový přesun uživatele

nemožný a jedná se v tom případě o podezřelou aktivitu a účet by měl být zablokován. (Dasgupta, a další, 2017)

3.4 Zabezpečení mobilních zařízení

3.4.1 Graf zabezpečení chytrých telefonů

Podle průzkumu firmy ESET z roku 2019 (ESET, 2019) si uživatelé nejčastěji zabezpečují mobilní telefony těmito způsoby:



Graf č. 1 - Zabezpečení chytrých telefonů. Zdroj: ESET

Dodatečný průzkum (ESET, 2021) ukázal, že v roce 2020 stoupl počet uživatelů požívajících otisk prstu na 41 % a PIN kódu na 28 %. Počet Čechů využívajících gesta naopak klesl na 14 % a navíc přibylo 6 % uživatelů, kteří mají telefon zabezpečený rozpoznáním obličeje.

4 Vlastní práce

Praktická část bakalářské práce se zabývá porovnáním mobilních aplikací určených k vícefaktorové autentizaci. Jednotlivé aplikace budou nejdříve obecně charakterizovány a poté zhodnoceny dle zvolených kritérií. Závěr této části práce následně porovná výsledky zhodnocení aplikací. Všechny aplikace byly hodnoceny za použití mobilního telefonu iPhone 13 s verzí iOS 16.2.

Pro zhodnocení bylo vybráno následujících 8 nejpoužívanějších aplikací:

- Microsoft Authenticator verze. 6.7.5
- Google Authenticator verze 3.4.0
- Twilio Authy verze 25.0.1.
- Duo Mobile verze 4.33.0
- LastPass Authenticator verze 2.7.8
- 2FA Authenticator (2FAS) verze 4.0.3
- Authenticator od SMM service verze 1.1.4
- Authenticator od 2Stable verze 3.18.1

4.1 Metody

Jednotlivé mobilní aplikace budou zhodnoceny a porovnány dle kritérií, které jsou podle autora pro aplikace určené k vícefaktorové autentizaci důležité. Kritéria jsou následující:

- Počet účtů – maximální počet přidaných účtů
- Záloha – zda aplikace obsahuje funkci online zálohy účtů
- Zámek obrazovky – zda aplikace nabízí možnost uzamčení
- Motiv – zda aplikace obsahuje tmavý motiv
- Další funkce – zda aplikace obsahuje dodatečné funkce
- Jazyky – počet podporovaných jazyků
- Velikost – velikost aplikace v MB

Nejdříve jsou pro jednotlivá kritéria stanoveny váhy, a to použitím Saatyho metody párového porovnání.

Stanovení vah kritérií

Saatyho metoda slouží k určení vah kritérií a jedná se o metodu kvantitativního párového porovnání kritérií. Pro ohodnocení párových kritérií se používá devítibodová stupnice a je možné používat i mezistupně (sudé hodnoty 2, 4, 6, 8) (Šubrt, 2011):

- 1 – rovnocenná kritéria i a j
- 3 – slabě preferované kritérium i před j
- 5 – silně preferované kritérium i před j
- 7 – velmi silně preferované kritérium i před j
- 9 – absolutně preferované kritérium i před j

Každou dvojici je tedy nutné porovnat a velikost preference i-tého kritéria vzhledem k j-tému zapsat do Saatyho matice. Pokud je j-té kritérium preferováno před i-tým, zapíší se to Saatyho matice převrácené hodnoty. Na diagonále matice budou vždy 1, protože stejná kritéria si jsou rovnocenná. Po přiřazení hodnot se pro každé kritérium vypočte geometrický průměr řádků Saatyho matice. Váhy jednotlivých kritérií se vypočítají jako podíl geometrického průměru daného kritéria a celkového součtu geometrických průměrů. Výsledně váhy jsou uvedeny v tabulce č. 3.

	Počet účtů	Záloha	Zámek obrazovky	Motiv	Další funkce	Jazyky	Velikost	Geometrický průměr	Váha
Počet účtů	**1**	3	5	8	6	7	9	4,626	0,411
Záloha	1/3	**1**	4	7	5	6	8	3,010	0,267
Zámek obrazovky	1/5	1/4	**1**	5	3	4	6	1,511	0,134
Motiv	1/8	1/7	1/5	**1**	1/4	1/3	3	0,367	0,033
Další funkce	1/6	1/5	1/3	4	**1**	3	5	0,944	0,084
Jazyky	1/7	1/6	1/4	3	1/3	**1**	3	0,563	0,050
Velikost	1/9	1/8	1/6	1/3	1/5	1/3	**1**	0,244	0,022
							Celkem	11,265	1,000

Tabulka č. 3 - stanovení vah kritérií

Po stanovení vah použitím Saatyho metody je nejdůležitějším kritériem maximální počet účtů, které aplikace nabízí s vahou 0,411. Maximální počet účtů by měl být co největší a nejlépe neomezený z důvodu velkého počtu služeb, které buď vyžadují nebo podporují vícefaktorové

ověřování. Druhým nejdůležitějším kritériem je funkce zálohy s vahou 0,267. Online zálohy je důležitá funkce, která zajišťuje obnovu a přístup k přidaným účtům například po ztrátě nebo odcizení zařízení. Třetím nejdůležitějším kritériem s vahou 0,134 je zámek obrazovky, který zvyšuje bezpečnost aplikace. Podpora dalších funkcí aplikace má váhu pouze 0,084 a to z toho důvodu, že dodatečné funkce sice mohou zpříjemnit a zkvalitnit práci s aplikací nebo dokonce nahradit funkce jiných aplikací, ale přímo nesouvisí s procesem autentizace. V pořadí pátým kritériem je podpora jazyků s vahou 0,050. Velké množství podporovaných jazyků je zajisté výhodou, ale u aplikace pro vícefaktorovou autentizaci není tak důležité. Podpora tmavého režimu má váhu pouze 0,033 a to proto, že ovlivňuje pouze vzhled aplikace, a ne její funkčnost. Nejméně důležitým kritériem s vahou 0,022 je velikost aplikace, která v současné době není natolik stěžejní z důvodu dostatečné velikosti paměti v novodobých mobilních zařízeních.

Zhodnocení aplikací

Pro zhodnocení aplikací je použita bodovací metoda s váhami. Nejprve jsou aplikace v příslušných kritériích ohodnoceny v rozmezí 1 až 5 bodů, kde 5 bodů znamená maximum a 1 bod minimum. Přidělené body jsou poté vynásobeny váhou daného kritéria. Po vynásobení všech kritérií jsou body sečteny a výsledek tohoto součtu představuje celkové hodnocení aplikace. Vzorec pro výpočet je zobrazený na obrázku č. 12, kde h_i je výsledné bodové ohodnocení aplikace, v_j váha kritéria, r_{ij} přiřazené bodové hodnocení aplikace u daného kritéria a k počet kritérií.

$$h_i = \sum_{j=1}^{k} v_j r_{ij}$$

Obrázek č. 11 - vzorec pro výpočet hodnocení aplikace

4.2 Microsoft Authenticator

Charakteristika

První porovnávanou aplikací byl zvolen Microsoft Authenticator ve verzi 6.7.5. Aplikace je zdarma, vyvíjí ji Microsoft Corporation a v současné verzi je její velikost 170,2 MB.

Kompatibilita

- iPhone – požadován iOS 14.0 nebo novější
- iPad – požadován iPadOS 14.0 nebo novější
- iPod touch – požadován iOS 14.0 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje spojené s uživatelem – následující údaje, které mohou být shromažďovány a propojeny s identitou uživatele, lze použít k dále uvedeným účelům
    - Analytika
        - Uživatelský obsah (zákaznická podpora, jiný uživatelský obsah)
        - Identifikátory (ID uživatele, ID zařízení)
        - Údaje o použití (interakce s produktem)
        - Diagnostika (další diagnostické údaje)
    - Funkčnost aplikace
        - Poloha (přesná poloha)
        - Kontaktní údaje (emailová adresa)
        - Uživatelský obsah (zákaznická podpora, jiný uživatelský obsah)
        - Identifikátory (ID uživatele, ID zařízení)
        - Údaje o použití (interakce s produktem)
        - Diagnostika (další diagnostické údaje)
- Údaje nespojené s uživatelem – následující údaje, které mohou být shromažďovány, ale ne propojeny s identitou uživatele, lze použít k dále uvedeným účelům:
    - Funkčnost aplikace
        - Diagnostika (údaje o selhání)

Detailní informace o údajích, které mohou aplikace shromažďovat a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat, jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje celkem 42 jazyků:

- čeština, angličtina, arabština, baskičtina, bulharština, chorvatština, dánština, estonština, finština, francouzština, galicijština, hebrejština, hindština, holandština, indonéština, italština, japonština, katalánština, kazaština, korejština, litevština, lotyština, malajština, maďarština, norština, němčina, polština, portugalština, rumunština, ruština, slovenština, slovinština, srbština, thajština, tradiční čínština, turečtina, ukrajinština, vietnamština, zjednodušená čínština, řečtina, španělština, švédština

Microsoft Authenticator funguje s jakýmkoliv účtem, který používá dvoustupňové ověřovaní a podporuje standardy jednorázového hesla (TOTP). K přidání účtu je nutné se k němu v aplikaci přihlásit, naskenovat QR kód nebo opsat speciální číselný kód. Po přidání účtu aplikace generuje ověřovací kódy, tyto kódy jsou číselné, šestimístné a generují se každých 30 sekund. Aplikace dále nabízí možnosti vlastního uspořádání účtů, přejmenování jednotlivých účtů nebo skrytí jednorázových kódů z hlavní obrazovky (kódy se poté zobrazují pouze po rozkliknutí konkrétního účtu). Aplikace ale naopak nenabízí manuální nebo automatickou možnost přepnutí do tmavého režimu.

Školní, osobní nebo pracovní účty od Microsoftu mají navíc v aplikaci zpřístupněny dodatečné funkce – přihlašování telefonem (tento způsob umožňuje přihlášení bez nutnosti hesla a to pomocí uživatelského jména a mobilního zařízení za pomocí otisku prstu, obličeje nebo PIN kódu), povolení schvalovacích oznámení (při povolení této možnosti může uživatel používaným zařízením schvalovat oznámení pro ověření přihlášení a nemusí opisovat jednorázová hesla), změnu hesla, aktualizaci bezpečnostních údajů nebo kontrolu posledních aktivit.

Microsoft Authenticator nabízí kromě samotného generování kódů i další užitečné funkce:

- **Záloha** – aplikace zálohuje přihlašovací údaje k účtu a související nastavení aplikace do cloudu. Pro zálohu je nutný osobní účet Microsoft, který funguje jako účet pro obnovení. Pro zařízení iOS je navíc nutný účet iCloudu pro skutečné umístění uložiště, tato služba je ale dostupná pouze pro zařízení s iOS. Pokud se

tedy uživatel rozhodne přejít na operační systém Android nebude mít možnost se k této záloze dostat.

- **Správce hesel** – Microsoft Authenticator dokáže na webech a aplikacích vyplňovat uložená hesla. Zároveň podporuje import hesel z Google Chrome, Firefox, LastPass, Bitwarden, Roboform nebo ze souboru CSV, také umožňuje export hesel do souboru CSV. Hesla se také automaticky synchronizují s prohlížečem Microsoft Edge.
- **Generátor hesel** – výše zmíněný Správce hesel osahuje i funkci Generátoru hesel. Princip fungování a možnosti přizpůsobení jsou stejné jako u dříve zmíněného generátoru hesel od firmy ESET (viz. Obrázek č. 1).
- **Správce adres** – tato funkce dokáže podobně jako Správce hesel vyplňovat uložené adresy na webech a aplikacích a synchronizovat se s prohlížečem Microsoft Edge
- **Ověřená ID** – tato služba umožňuje bezpečné vystavování a ověřování přihlašovacích údajů na pracovišti, potvrzení o statusu studenta či učitele, certifikace a další jedinečné atributy identity. Více informací o této službě je uvedeno na stránkách Microsoft (Microsoft)
- **Zámek aplikace** – tato funkce umožňuje vyžadovat zámek obrazovky při otevírání aplikace, schválení oznámení nebo automatickém vyplnění na webech a v aplikacích. S použitím otisku prstu nebo skenu obličeje ani výrazně neprodlouží proces ověření.

Zhodnocení

Kritérium	Microsoft Authenticator		Váhy	Vážené body
Počet účtů	bez omezení	5	0,411	2,053
Záloha	ano	5	0,267	1,336
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ne	1	0,033	0,033
Další funkce	správce hesel, správce adres, ověřená ID	5	0,084	0,419
Jazyky	42	5	0,050	0,250
Velikost (MB)	170,2	1	0,022	0,022
	Celkem	**27**	1	**4,783**

Tabulka č. 4 - zhodnocení aplikace Microsoft Authenticator

4.3 Google Authenticator

Charakteristika

Druhou porovnávanou aplikací byla zvolena bezplatná aplikace Google Authenticator ve verzi 3.4.0. Vývojářem aplikace je Google LLC a v současné verzi je její velikost 27 MB.

Kompatibilita

- iPhone – požadován iOS 13.0 nebo novější
- iPad – požadován iPad OS 13.0 nebo novější
- iPod touch – požadován iOS 13.0 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje spojené s uživatelem – následující údaje, které mohou být shromažďovány a propojeny s identitou uživatele, lze použít k dále uvedeným účelům
    - Analytika
        - Identifikátory (ID zařízení)
        - Údaje o použití (interakce s produktem)
        - Diagnostika (další diagnostické údaje)
        - Další údaje (další typy údajů)
    - Funkčnost aplikace
        - Identifikátory (ID zařízení)
        - Diagnostika (další diagnostické údaje)
- Údaje nespojené s uživatelem – následující údaje, které mohou být shromažďovány, ale ne propojeny s identitou uživatele, lze použít k dále uvedeným účelům:
    - Analytika
        - Poloha (přibližná poloha)
        - Uživatelský obsah (zákaznická podpora)
        - Diagnostika (údaje o selhání, údaje o výkonu)
    - Funkčnost aplikace
        - Poloha (přibližná poloha)

- Uživatelský obsah (zákaznická podpora)
- Diagnostika (údaje o selhání, údaje o výkonu)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje celkem 32 jazyků:

- čeština, angličtina, arabština, chorvatština, dánština, finština, francouzština, hebrejština, holandština, indonéština, italština, japonština, katalánština, korejština, malajština, maďarština, norština, němčina, polština, portugalština, rumunština, ruština, slovenština, thajština, tradiční čínština, turečtina, ukrajinština, vietnamština, zjednodušená čínština, řečtina, španělština, švédština

Google Authenticator je jednoduchý a soustředí se pouze na generování jednorázových hesel. Jednotlivé účty se přidávají buď naskenováním QR kódu nebo manuálním zadáním účtu a klíče. Samotná aplikace generuje šestimístné číselné kódy a to každých 30 sekund. Google Authenticator narozdíl od Microsoft Authenticator neobsahuje žádné dodatečné funkce jako správce hesel nebo správce adres. Nenabízí ani žádné speciální možnosti nastavení pro vlastní účty Google nebo možnost zálohy přidaných účtů. Obsahuje ale funkci exportu účtů, která uživateli umožnuje přesunout stávající účty do jiného zařízení. Dále aplikace nabízí možnost vlastního seřazení účtů a jejich přejmenování. Při používání má aplikace takový motiv, jaký je nastaven jako systémový – světlý nebo tmavý. V nastavení lze aktivovat bezpečnostní prvek „Obrazovka ochrany soukromí“, který omezuje přístup do aplikace tím, že vyžaduje Face ID. U této funkce je možné nastavit prodlevu, po níž se zámek při přepínání mezi aplikacemi objeví. K dispozici jsou tyto možnosti – okamžitě, po 10 sekundách, po 1 minutě nebo po 10 minutách.

Zhodnocení

Kritérium	Google Authenticator		Váhy	Vážené body
Počet účtů	bez omezení	5	0,411	2,053
Záloha	ne	1	0,267	0,167
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ano	5	0,033	0,163
Další funkce	žádné	1	0,084	0,084
Jazyky	32	4	0,050	0,200
Velikost (MB)	27	5	0,022	0,108
	Celkem	**26**	1	**3,546**

Tabulka č. 5 - zhodnocení aplikace Google Authenticator

4.4 Twilio Authy

Charakteristika

Třetí porovnávanou aplikací byla vybrána Twilio Authy ve verzi 25.0.1. Aplikace je zdarma, vyvíjí ji Authy Inc. a v současné verzi je její velikost 23,4 MB.

Kompatibilita

- iPhone – požadován iOS 13.0 nebo vyšší
- iPad – požadován iPadOS 13.0 nebo novější
- iPod touch – požadován iOS 13.0 nebo novější
- Mac – požadován macOS 11.0 nebo novější a Mac s čipem Apple M1 nebo novější
- Apple Watch – požadován watchOS 3.0 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje spojené s uživatelem – následující údaje, které mohou být shromažďovány a propojeny s identitou uživatele, lze použít k dále uvedeným účelům
    - Analytika
        - Poloha (přibližná poloha)
        - Identifikátory (ID uživatele, ID zařízení)
        - Údaje o použití (interakce s produktem)
        - Diagnostika (údaje o selhání, údaje o výkonu)

- Funkčnost aplikace
    - Kontaktní údaje (emailová adresa, telefonní číslo)
    - Identifikátory (ID uživatele, ID zařízení)
    - Údaje o použití (interakce s produktem)
    - Diagnostika (údaje o selhání, údaje o výkonu)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje celkem 3 jazyky:

- angličtina, portugalština, španělština

Twilio Authy vyžaduje pro používání zadání telefonního čísla a emailové adresy a následné ověření zadaného telefonního čísla buď pomocí SMS nebo telefonátem. Účty lze přidávat jak QR kódem, tak manuálním opsáním klíče. Číselné ověřovací kódy se generují každých 30 sekund a jsou šestimístné. Generované kódy nejsou všechny viditelné, zobrazen je pouze ten od daného otevřeného účtu. Jednotlivé účty si může uživatel libovolně seřadit a pojmenovat. A stejně jako například Microsoft Authenticator neobsahuje manuální ani automatickou možnost přepnutí do tmavého režimu. Narozdíl od Microsoft Authenticator, ale neobsahuje žádné funkce například pro práci s hesly. Nabízí ale možnost zabezpečení pomocí PIN kódu, po vytvoření kódu může uživatel aktivovat ochranu použitím biometriky. Twilio Authy také podporuje přijímání nebo odmítání požadavků na autentizaci pomocí oznámení. Tato funkce funguje, ale pouze v případě, že uživatel nemá aktivované zabezpečení pomocí PIN kódu. V případě, že uživatel má nastavený PIN kód, tuto funkci využít nemůže. Dále aplikace nabízí možnost synchronizace mezi více zařízeními – například mezi desktopem a mobilním telefonem. Pokud tedy uživatel ztratí přístup ke svému mobilnímu zařízení má možnost obnovy přes desktop. Authy také disponuje funkcí zálohy registrovaných účtů. Pro zálohu účtů si uživatel musí vytvořit heslo s pomocí kterého se k záloze dostane.

Zhodnocení

Kritérium	Twilio Authy		Váhy	Vážené body
Počet účtů	bez omezení	5	0,411	2,053
Záloha	ano	5	0,267	1,336
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ne	1	0,033	0,033
Další funkce	žádné	1	0,084	0,084
Jazyky	3	1	0,050	0,050
Velikost (MB)	23,4	5	0,022	0,108
	Celkem	**23**	1	**4,335**

Tabulka č. 6 - zhodnocení aplikace Twilio Authy

4.5 Duo Mobile

Charakteristika

Čtvrtou aplikací pro porovnání byla zvolena aplikace Duo Mobile ve verzi 4.33.0. Aplikace je zdarma, vyvíjí ji Duo Security LLC a v současné verzi je její velikost 22,2 MB

Kompatibilita

- iPhone – požadován iOS 13.0 nebo novější
- iPad – požadován iPadOS 13.0 nebo novější
- iPod touch – požadován iOS 13.0 nebo novější
- Apple Watch – požadován watchOS 4.0 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje spojené s uživatelem – následující údaje, které mohou být shromažďovány a propojeny s identitou uživatele, lže použít k dále uvedeným účelům
    - Analytika
        - Poloha (přibližná poloha)
        - Identifikátory (ID zařízení)
        - Údaje o použití (interakce s produktem, další údaje o použití)
        - Diagnostika (údaje o selhání, další diagnostické údaje)
    - Funkčnost aplikace

- Údaje o použití (interakce s produktem)
- Diagnostika (údaje o selhání, další diagnostické údaje)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje celkem 23 jazyků:

- čeština, angličtina, dánština, finština, francouzština, hindština, holandština, indonéština, italština, japonština, katalánština, korejština, norština, němčina, polština, portugalština, thajština, tradiční čínština, turečtina, vietnamština, zjednodušená čínština, španělština, švédština

Stejně jako předchozí porovnávané aplikace nabízí i Duo Mobile možnost přidání účtu jak pomocí QR kódu, tak číselného kódu. Jednorázové kódy se také generují každých 30 sekund. Jedná se o šestimístné kódy, které ale nejsou zobrazeny při spuštění aplikace, ale začnou se generovat až po kliknutí na tlačítko zobrazit. Na rozdíl od Twilio Authy nevyžaduje pro fungování registraci, účty je možné tedy přidávat hned po spuštění aplikace podobně jako u Microsoft Authenticator nebo Google Authenticator. Jednotlivé účty jsou řazeny pod sebe a je možné je libovolně přesouvat, zároveň je lze i přejmenovat. Vzhled aplikace je automaticky stejný jako systémový motiv. Duo Mobile obsahuje možnost zálohy účtů třetích stran, a to nastavením hesla pro obnovení. Záloha je ale jediná speciální funkce, kterou aplikace nabízí, postrádá tedy i možnost zamčení aplikace za použití kódu, hesla nebo biometriky.

Zhodnocení

Kritérium	Duo Mobile		Váhy	Vážené body
Počet účtů	bez omezení	5	0,411	2,053
Záloha	ano	5	0,267	1,336
Zámek obrazovky	ne	1	0,134	0,134
Motiv	ano	5	0,033	0,163
Další funkce	žádné	1	0,084	0,084
Jazyky	23	3	0,050	0,150
Velikost (MB)	22,2	5	0,022	0,108
	Celkem	**25**	1	**4,028**

Tabulka č. 7 - zhodnocení aplikace Duo Mobile

4.6 LastPass Authenticator

Pátou porovnávanou aplikací byl zvolen LastPass Authenticator ve verzi 2.7.8. Aplikace je zdarma, vyvíjí ji LogMeIn, Inc. a v současné verzi je velká 25,3 MB.

Kompatibilita

- iPhone – požadován iOS 14.0 nebo novější
- iPad – požadován iPadOS 14.0 nebo novější
- iPod touch – požadován iOS 14.0 nebo novější

Ochrana soukromí aplikace

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje spojené s uživatelem – následující údaje, které mohou být shromažďovány a propojeny s identitou uživatele, lze použít k dále uvedeným účelům
    - Reklama nebo marketing vývojáře
        - Identifikátory (ID uživatele)
    - Analytika
        - Identifikátory (ID uživatele)
        - Údaje o použití (interakce s produktem)
    - Funkčnost aplikace
        - Poloha (přibližná poloha)
        - Identifikátory (ID uživatele, ID zařízení)
- Údaje nespojené s uživatelem – následující údaje, které mohou být shromažďovány, ale ne propojeny s identitou uživatele, lze použít k dále uvedeným účelům:
    - Funkčnost aplikace
        - Diagnostika (údaje o selhání, údaje o výkonu)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje celkem 7 jazyků:

- angličtina, francouzština, holandština, italština, němčina, portugalština, španělština

Účty se do aplikace LastPass Authenticator přidávají buď pomocí QR kódu, speciálního kódu nebo ze zálohy. Pří přidávání pomocí speciálního kódu nabízí aplikace rozšířené nastavení – změna času ve kterém se generují hesla, počet číslic generovaného kódu a použitý algoritmus (SHA1, SHA256, SHA512). Nicméně aplikace varuje před změnami těchto nastavení s odůvodněním, že tyto nastavení potřebují být upraveny jen ve výjimečných případech a jejich změna by mohla znemožnit přístup k účtu. Standartně se kódy generují v třiceti sekundových intervalech a jsou šestimístné. Pro přidání účtů ze zálohy je nutné stáhnutí aplikace LastPass Password Manager. Přidané účty je poté možné libovolně přejmenovat a řadit buď abecedně, od nejnovějšího, nejstaršího nebo podle vlastního seřazení. Účet lze též označit hvězdičkou a tím ho přidat do oblíbených, to vytváří další možnost vlastního řazení. Zámek aplikace je realizovaný pomocí biometriky nebo PIN kódu, i při vybrání možnosti biometriky aplikace vyžaduje vytvoření šestimístného kódu pro případ nefunkčnosti Face ID. Při aktivování zámku obrazovky aplikace upozorní, že při zapnutém zámku není možné využívat chytré hodinky pro verifikaci. Aplikace rovněž obsahuje možnost zálohy účtů, pro aktivaci této funkce je ale nutné stáhnutí již předem zmíněné aplikace LastPass Password Manager. Motiv aplikace se automaticky nastavuje podle toho systémového.

Zhodnocení

Kritérium	LastPass Authenticator		Váhy	Vážené body
Počet účtů	bez omezení	5	0,411	2,053
Záloha	ano, ale pouze s aplikací LastPass Password Manager	4	0,267	1,069
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ano	5	0,033	0,163
Další funkce	žádné	1	0,084	0,084
Jazyky	6	2	0,050	0,100
Velikost (MB)	25,3	5	0,022	0,108
	Celkem	**27**	1	**4,248**

Tabulka č. 8 - zhodnocení aplikace LastPass Authenticator

4.7 2FA Authenticator (2FAS)

Charakteristika

Šestou porovnávanou aplikací byl zvolen 2FA Authenticator (2FAS) ve verzi 4.0.3. Aplikace je zdarma, vyvíjí ji Two Factor Authentication Service, Inc. a v současné verzi je její velikost17,9 MB.

Kompatibilita

- iPhone – požadován iOS 15.4 nebo novější
- iPad – požadován iPadOS 15.4 nebo novější
- iPad touch – požadován iOS 15.4 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje nespojené s uživatelem – nesledující údaje, které mohou být shromažďovány, ale ne propojeny s identitou uživatele, lze použít k dále uvedeným účelům:
    - Analytika
        - Údaje o použití (interakce s produktem)
    - Funkčnost aplikace
        - Diagnostika (údaje o selhání)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje pouze jediný jazyk a tím je angličtina.

Do aplikace 2FA Authenticator je možné účty přidávat několika způsoby. Účty lze přidávat buď naskenováním QR kódu nebo načtením QR kódu z galerie, účet lze také přidat manuálně zadáním kódu. Další možností je importování ze zálohovaného souboru nebo z aplikace Google Authenticator. Přidané účty je poté možné upravovat různými způsoby, u účtů je například možné změnit jejich jméno, přidat je do skupiny, změnit jejich ikonu buď nahrazením z existující databáze nebo vlastním popsáním – u této možnosti lze rovněž změnit barvu pozadí.

Jednotlivé účty jsou zobrazeny na hlavní obrazovce a jsou rozřazeny podle vytvořených skupin ve kterých je možné je dále libovolně seřadit. Aplikace nastavuje světlý a tmavý motiv automaticky, podle nastavení systému. Jednorázové kódy se generují 30 sekundách a jsou šestimístné. V nastavení aplikace se nachází možnosti zálohy. Záloha se provádí buď automaticky na iCloud nebo je zde možnost zálohy vytvořením souboru, tato možnost slouží k offline záloze. Souborová záloha nabízí jak import z existujícího souboru nebo export do nového souboru. Aplikace doporučuje cloudové zálohování pomocí iCloudu. Poslední možnost nabízí vymazání záloh, tato možnost vymaže všechny zálohy i z ostatních zařízení synchronizovaných s účtem. V nastavení je dále možné zapnout zámek obrazovky. Zámek je realizovaný čtyřmístným PIN kódem, po nastavení kódu je možné zapnout biometrickou autentizaci, je zde také možné nastavit maximální počet neúspěšných pokusů na 3, 5, 10 nebo limit vypnout, lze nastavit i jak dlouho bude trvat uzamčení po překročení maximálního poštu pokusů, dostupné možnosti jsou následující: 3 minuty, 5 minut nebo 10 minut. V pokročilých nastaveních aplikace nabízí možnost spárování s webovým rozšířením, zapnutí widgetů nebo funkci zobrazování dalšího kódu. Další kód se poté zobrazuje v posledních 5 vteřinách pod aktuálním kódem. Při povolení widgetů aplikace varuje, že všechny kódy mohou být viditelné i bez odemčení zámku aplikace.

Zhodnocení

Kritérium	2FA Authenticator (2FAS)		Váhy	Vážené body
Počet účtů	bez omezení	5	0,411	2,053
Záloha	ano	5	0,267	1,336
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ano	5	0,033	0,163
Další funkce	žádné	1	0,084	0,084
Jazyky	1	1	0,050	0,050
Velikost (MB)	17,9	5	0,022	0,108
	Celkem	**27**	1	**4,465**

Tabulka č. 9 - zhodnocení aplikace 2FA Authenticator (2FAS)

4.8 Authenticator od SMM service

Charakteristika

Sedmou porovnávanou aplikací byl zvolen Authenticator ve verzi 1.1.4, který vyvíjí SMM service. Aplikace je ke stažení zdarma, ale pro zpřístupnění pokročilejších funkcí je nutné zakoupení předplatného. V současné verzi je velikost aplikace 57,9 MB.

Kompatibilita

- iPhone – požadován iOS 13.0 nebo novější
- iPad – požadován iPadOS 13.0 nebo novější
- iPad touch – požadován iOS 13.0 nebo novější
- Mac – požadován macOS 11.0 nebo novější a Mac s čipem Apple M1 nebo novější
- Apple Watch – požadován watchOS 6.0 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje použité ke sledování uživatele – následující údaje mohou být použity k sledování uživatele napříč aplikacemi a weby vlastněnými jinými společnostmi:
    - Nákupy – historie nákupů
    - Identifikátory – ID zařízení
- Údaje nespojené s uživatelem – následující údaje, které mohou být shromažďovány, ale ne propojeny s identitou uživatele, lze použít k dále uvedeným účelům:
    - Reklama nebo marketing vývojáře
        - Nákupy (historie nákupů)
        - Identifikátory (ID zařízení)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje celkem 10 jazyků:

- čeština, angličtina, arabština, francouzština, italština, japonština, němčina, portugalština, ruština, španělština

Authenticator, který vyvíjí 2MM service podporuje přidávání účtů QR kódem pomocí kamery nebo z galerie, zároveň je účty možné přidat ručně pomocí speciálního kódu. Po přidání se jednorázové kódy generují v intervalu 30 sekund a jsou šesticiferné. V nastavení jednotlivých účtů je možné nastavit jejich název nebo změnit jejich ikonu, také je zde možné nastavit vlastní záložní kódy. V bezplatné verzi je, ale možné přidat pouze 3 účty. Záloha účtů je také dostupná pouze v prémiové verzi. Zámek obrazovky je naopak dostupný i v bezplatné verzi. Pro jeho aktivování je nutné si nejdříve vytvořit heslo, po vytvoření hesla je možné aktivovat přihlášení za použití biometriky. Aplikace také nabízí několik přidaných funkcí, jedná se o soukromý prohlížeč, správce hesel a VPN. Správce hesel zahrnuje i automatickou zálohu na iCloud, služba VPN je dostupná pouze s předplatným. Pokud se uživatel rozhodne zakoupit předplatné, zbaví se i reklam, které aplikace obsahuje.

Možná předplatná a jejich ceny jsou následující:

- roční – 999 Kč
- měsíční – 249 Kč
- roční s VPN – 2150 Kč
- měsíční s VPN – 329 Kč

Zhodnocení

Kritérium	Authenticator od SMM		Váhy	Vážené body
Počet účtů	3 / bez omezení*	3	0,411	1,232
Záloha	ano*	3	0,267	0,802
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ne	1	0,033	0,033
Další funkce	soukromý prohlížeč, správce hesel*, VPN*	3	0,084	0,251
Jazyky	10	2	0,050	0,100
Velikost (MB)	57,9	3	0,022	0,065
	Celkem	**20**	1	**3,153**

* dostupné pouze se zakoupeným předplatným

Tabulka č. 10 - zhodnocení aplikace od SMM service

4.9 Authenticator od 2Stable

Charakteristika

Osmou a zároveň poslední aplikací byl zvolen Authenticator ve verzi 3.18.1, který vyvíjí 2Stable. Podobně jako předchozí Authenticator od SMM service je i tato aplikace zdarma ke stažení ale k zpřístupnění všech funkcí je nutné zakoupení předplatného. V současné verzi je aplikace velká 77 MB.

Kompatibilita

- iPhone – požadován iOS 15.0 nebo novější
- iPad – požadován iPadOS 15.0 nebo novější
- iPad touch – požadován iOS 15.0 nebo novější
- Mac – požadován macOS 12.0 nebo novější
- Apple Watch – požadován watchOS 8.0 nebo novější

Ochrana soukromí v aplikaci

Vývojář uvedl, že součástí opatření na ochranu soukromí v této aplikaci může být zpracování dat následujícími způsoby:

- Údaje nespojené s uživatelem – následující údaje, které mohou být shromažďovány, ale ne propojeny s identitou uživatele, lze použít k dále uvedeným účelům
    - Analytika
        - Nákupy (historie nákupů)
        - Uživatelský obsah (zákaznická podpora)
        - Údaje o použití (interakce s produktem)
        - Diagnostika (další diagnostické údaje)
    - Personalizace produktu
        - Nákupy (historie nákupů)
        - Údaje o použití (interakce s produktem)
        - Diagnostika (další diagnostické údaje)
    - Funkčnost aplikace
        - Nákupy (historie nákupů)
        - Uživatelský obsah (zákaznické podpora)
        - Údaje o použití (interakce s produktem)

- Diagnostika (údaje o selhání, údaje o výkonu, další diagnostické údaje)

Detailní informace o údajích, které mohou aplikace shromažďovat, a o některých způsobech, jak je může vývojář nebo partneři třetích stran používat jsou uvedeny v (Apple).

Jazyky

Aplikace podporuje jediný jazyk a tím je angličtina.

Při přístup do aplikace si uživatel musí jako první vytvořit heslo, v nastavení je poté možné zapnout přihlašovaní za použití biometriky. Účty je možné přidávat několika způsoby a to manuálně, převodem z Google Authenticator, vyfocením QR kódu nebo QR kódem uloženým v galerii, ze souboru nebo pomocí URL adresy. Po přidání aplikace je možné nastavit její název, ikonu, zapsat záložní kódy a povolit pro účet zobrazení ve widgetech nebo Apple Watch. V rozšířených nastaveních je možné nastavit algoritmus (SHA1, SHA256, SHA512), počet cifer (6, 8) a časový interval generování. Podobně jako aplikace LastPass Authenticator i tato aplikace varuje před změnami těchto nastavení. Při ponechání původního nastavení se kódy generují s použitím algoritmu SHA1 každých 30 vteřin a jsou šesticiferné. Účty je možné řadit podle doby přidání nebo podle názvu. Motiv aplikace se automaticky nastavuje podle systémové předvolby. Aplikace rovněž jako ta předchozí obsahuje předplatné, bez kterého nejsou dostupné určité funkce. Konkrétně se jedná o zálohu a synchronizaci mezi zařízeními a neomezený počet účtů. Na rozdíl od aplikace Authenticator od vývojářů 2MM service, ale neobsahuje reklamy. Dostupná předplatná jsou následující – roční (449 Kč) a měsíční (129 Kč)

Zhodnocení

Kritérium	Authenticator od 2Stable		Váhy	Vážené body
Počet účtů	2 / bez omezení*	3	0,411	1,232
Záloha	ano*	3	0,267	0,802
Zámek obrazovky	ano	5	0,134	0,671
Motiv	ano	5	0,033	0,163
Další funkce	žádné	1	0,084	0,084
Jazyky	1	1	0,050	0,050
Velikost (MB)	77	3	0,022	0,065
	Celkem	**21**	1	**3,066**

* dostupné pouze se zakoupeným předplatným

Tabulka č. 11 - zhodnocení aplikace od 2Stable

5 Výsledky a diskuse

V tabulce č. 12 jsou ke kritériím, které zvolil autor, přiřazeny hodnoty. Poté jsou aplikace na základě uvedených hodnot bodově ohodnoceny v jednotlivých kritériích viz. tabulka č. 13.

Kritérium	Microsoft Authenticator	Google Authenticator	Twilio Authy	Duo Mobile
Počet účtů	bez omezení	bez omezení	bez omezení	bez omezení
Záloha	ano	ne	ano	ano
Zámek obrazovky	ano	ano	ano	ne
Motiv	ne	ano	ne	ano
Další funkce	správce hesel, správce adres, ověřená ID	žádné	žádné	žádné
Jazyky	42	32	3	23
Velikost (MB)	170,2	27	23,4	22,2
Kritérium	**LastPass Authenticator**	**2FA Authenticator (2FAS)**	**Authenticator od SMM**	**Authenticator od 2Stable**
Počet účtů	bez omezení	bez omezení	3 / bez omezení*	2 / bez omezení*
Záloha	ano, ale pouze s aplikací LastPass Password Manager	ano	ano*	ano*
Zámek obrazovky	ano	ano	ano	ano
Motiv	ano	ano	ne	ano
Další funkce	žádné	žádné	soukromý prohlížeč, správce hesel*, VPN*	žádné
Jazyky	6	1	10	1
Velikost (MB)	25,3	17,9	57,9	77

* dostupné pouze se zakoupeným předplatným

Tabulka č. 12 -hodnoty parametrů jednotlivých aplikací

Tabulka číslo 13 obsahuje bodové ohodnocení parametrů jednotlivých aplikací. Hodnocení vychází z údajů v tabulce číslo 12. Parametry jsou ohodnoceny body od 1 do 5, a následně vynásobeny vahou daného kritéria. Poté jsou vážené body pro jednotlivé aplikace sečteny, tento součet je uveden v řádku Výsledné hodnocení a představuje konečné bodové ohodnocení aplikace.

Kritérium	Microsoft Authenticator	Google Authenticator	Twilio Authy	Duo Mobile	Váha
Počet účtů	5	5	5	5	0,411
Záloha	5	1	5	5	0,267
Zámek obrazovky	5	5	5	1	0,134
Motiv	1	5	1	5	0,033
Další funkce	5	1	1	1	0,084
Jazyky	5	4	1	3	0,050
Velikost (MB)	1	5	5	5	0,022
Výsledné hodnocení	4,783	3,546	4,335	4,028	
Kritérium	**LastPass Authenticator**	**2FA Authenticator (2FAS)**	**Authenticator od SMM**	**Authenticator od 2Stable**	**Váha**
Počet účtů	5	5	3	3	0,411
Záloha	4	5	3	3	0,267
Zámek obrazovky	5	5	5	5	0,134
Motiv	5	5	1	5	0,033
Další funkce	1	1	3	1	0,084
Jazyky	2	1	2	1	0,050
Velikost (MB)	5	5	3	3	0,022
Výsledné hodnocení	4,248	4,465	3,153	3,066	

Tabulka č. 13 - Ohodnocené parametry jednotlivých aplikací

V prvním kritériu Počet účtů dostaly všechny aplikace nejvyšší bodové ohodnocení, protože nelimitují maximální počet přidaných účtů. Jedinými výjimkami jsou aplikace Authenticator od SMM a Authenticator 2Stable, které dostaly body tři. A to z toho důvodu, že mají omezen maximální počet účtů a pro zrušení tohoto omezení je nutné zakoupení předplatného. V kritériu Záloha dostaly maximální počet bodů za podporu funkce zálohy pouze aplikace Microsoft Authenticator, Twilio Authy, Duo Mobil a 2FA Authenticator (2FAS). LastPass Authenticator dostal o bod méně jelikož vyžaduje pro zapnutí zálohy nainstalování aplikace LastPass Password Manager. Třemi body byly ohodnoceny aplikace Authenticator od

SMM a Authenticator od 2Stable, které sice nabízí možnost zálohy ale pouze se zakoupeným předplatným. Nejmenší možný počet bodů obdržel Google Authenticator, který funkci zálohy neobsahuje vůbec. V kritériu Zámek obrazovky dostaly všechny aplikace plný počet bodů s výjimkou aplikace Duo Mobile, která zámek obrazovky nenabízí. V kritériu Motiv obdržely maximální počet bodů ty aplikace, které obsahují automatické či manuální přepnutí do tmavého režimu. Konkrétně se jedná o aplikace Google Authenticator, Duo Mobile, LastPass Authenticator, 2FA Authenticator (2FAS) a Authenticator od 2Stable. Ostatní aplikace tmavý režim nepodporují a dostaly tedy pouze jeden bod. Jediný Microsoft Authenticator obdržel pět bodů za přidané funkce v aplikaci. Aplikace nabízí funkce jako správce hesel, správce adres nebo službu ověřená ID. Jedinou další aplikací, která nabízí rozšířené funkce je Authenticator od SMM, konkrétně se jedná o soukromý prohlížeč, správce hesel a VPN. Authenticator od SMM byl v tomto kritériu ale kvůli zpoplatnění těchto funkcí ohodnocen pouze třemi body. Největší počet podporovaných jazyků (42) a tedy i největší bodové ohodnocení dostal Microsoft Authenticator. Druhý největší počet jazyků (32) podporuje aplikace Google Authenticator a dostala taky čtyři body. Tři body dostala aplikace Duo Mobile, která podporuje 23 jazyků. Dvěma body byly ohodnoceny aplikace LastPass Authenticator a Authenticator od SMM, které podporují podobný počet jazyků – 6 a 10. Aplikace Twilio Authy, 2FA Authenticator (2FAS) a Authenticator od 2Stable obdržely pouze jeden bod, protože oproti ostatním aplikacím v podpoře jazyků zaostávají. V kritériu Velikost bylo ohodnoceno pěti body celkem pět aplikací. Velikost těchto aplikací se pohybuje v rozmezí 17,9 až 27 MB. Tři body dostaly aplikace Authenticator od SMM a Authenticator od 2Stable, které jsou velké 57,9 MB a 77 MB. Nejmenší možné bodové ohodnocení dostala aplikace Microsoft Authenticator, která je velká 170,2 MB.

V tabulce číslo 14 jsou seřazeny aplikace podle celkového počtu dosažených bodů po použití Saatyho metody ke stanovení vah a následně bodovací metody rozšířené o váhy kritérií k vypočtení konečného počtu bodů.

Pořadí	Aplikace	Hodnocení
1.	Microsoft Authenticator	4,783
2.	2FA Authenticator (2FAS)	4,465
3.	Twilio Authy	4,335
4.	LastPass Authenticator	4,248
5.	Duo Mobile	4,028
6.	Google Authenticator	3,546
7.	Authenticator od SMM	3,153
8	Authenticator od 2Stable	3,066

Tabulka č. 14 - výsledné pořadí aplikací

Největšího bodového ohodnocení dosáhla aplikace Microsoft Authenticator, která získala 4,783 bodů, a to především kvůli svým dodatečným funkcím jako správce hesel nebo správce adres. Na druhém místě se umístila aplikace 2FA Authenticator (2FAS), která dosáhla 4,465 bodů i přesto, že podporuje pouze jeden jazyk. Twilio Authy získala 4,335 bodů a stala se třetí nejlepší aplikací. Čtvrtého nejvyššího bodového ohodnocení dosáhla aplikace LastPass Authenticator s 4,428 body, které uniklo druhé místo kvůli nutnosti stažení další aplikace pro možnost zálohy. Na dalších místech následovaly aplikace Duo Mobile (4,028 bodů) a Google Authenticator (3,546 bodů), která ztratila kvůli absenci funkce zálohy 1,069 bodů. Nejnižší bodové ohodnocení dostaly aplikace Authenticator od SMM (3,153 bodů) a Authenticator od 2Stable (3,066 bodů), a to zejména kvůli omezení maximálního počtu účtů v neplacené verzi aplikace, ale také kvůli zpoplatnění některých funkcí, které ostatní lépe umístěné aplikace poskytují zdarma.

6 Závěr

Hlavním cílem bakalářské práce byla analýza rozdílných způsobů vícefaktorové autentizace a porovnání mobilních aplikací určených k vícefaktorové autentizaci. Pro splnění hlavního cíle byly stanoveny dílčí cíle – vypracování přehledu problematiky vícefaktorové autentizace a vypracování přehledu různých způsobů vícefaktorové autentizace.

V úvodu teoretické části práce byly vysvětleny pojmy autentizace a autorizace, a následně byly představeny 4 typy autentizace – ověření uživatele na základě toho co zná, vlastní, čím je nebo kde se nachází. K jednotlivým typům autentizace byly dále uvedeny příklady, které byly blíže popsány. Konkrétně se jednalo například o hesla, PIN kódy, softwarové tokeny, rozpoznání obličeje nebo otisk prstu.

Praktická část bakalářské práce se zabývala porovnáním osmi nejpoužívanějších aplikací určených k vícefaktorové autentizaci pro systém iOS. Byly vybrány aplikace Microsoft Authenticator, Google Authenticator, Twilio Authy, Duo Mobile, LastPass Authenticator, 2FA Authenticator (2FAS), Authenticator od SMM service a Authenticator od 2Stable.

Všechny výše zmíněné aplikace plní svůj účel, kterým je především generování jednorázových kódů a lze je tedy použít pro vícefaktorovou autentizaci. Aplikace se tedy mohou zdát na první pohled stejné, ale některé z nich poskytují nebo naopak postrádají důležité funkce nebo možnosti. Cílem praktické části bylo tedy nalezení a zhodnocení těchto rozdílů.

Před samotným porovnáním byly aplikace nejdříve obecně charakterizovány. Pro porovnání aplikací byla zvolena bodovací metoda rozšířená o váhy kritérií. Autor nejprve stanovil 7 kritérií, podle kterých budou aplikace porovnávány – maximální počet přidaných účtů, možnost online zálohy, možnost uzamčení aplikace, možnost tmavého režimu, nabídka dodatečných funkcí, podpora jazyků a velikost aplikace. Následně byly Saatyho metodou určeny váhy jednotlivých kritérií. Poté byly aplikace v jednotlivých kritériích ohodnoceny a s použitím dříve stanovených vah kritérií bylo vypočteno konečné hodnocení aplikace podle kterého bylo určeno počadí aplikací.

Nejlepší aplikací pro vícefaktorovou autentizaci z osmi porovnávaných se stala aplikace Microsoft Authenticator, která získala 4,783 bodů. Druhý největší počet bodů (4,465) získala aplikace 2FA Authenticator (2FAS). Na třetím místě s 4,335 body se umístila aplikace Twilio Authy. LastPass Authenticator získal 4,248 bodů a skončil tak na čtvrtém místě. Na pátém místě následovala aplikace Duo Mobile s 4,028 body. V pořadí šestý se umístil Google Authenticator s 3,546 body. Na předposledním místě skončil Authenticator od SMM s 3,153 body. A na posledním místě se s nejmenším počtem bodů (3,066) umístil Authenticator od 2Stable.

7 Seznam použitých zdrojů

Alza. 2020. Odemykání obličejem: jak to funguje a na co si dát pozor. *Alza.* [Online] 8. duben 2020. [Citace: 2. září 2022.] https://www.alza.cz/slovnik/odemykani-oblicejem.

Apple. Ochrana soukromí - definice a příklady. *Apple.* [Online] [Citace: 12. únor 2023.] https://apps.apple.com/cz/story/id1539235847?l=cs.

CZ.NIC. Bezpečná hesla. *Nebojte se internetu.* [Online] [Citace: 25. srpen 2022.] https://www.nebojteseinternetu.cz/page/3448/bezpecna-hesla/.

Dasgupta, Dipankar, Roy, Aranuva a Nag, Abhijit. 2017. *Advances in User Authentication.* místo neznámé : Springer, 2017. ISBN 978-3-319-58808-7.

e3displays. Experts Agree: Face ID Is Not The Answer, In-Display Fingerprint Sensors Are. *e3displays.* [Online] [Citace: 5. září 2022.] https://www.e3displays.com/experts-agree-face-id-is-not-the-answer-in-display-fingerprint/.

ESET. 2019. Jak zvolit bezpečné heslo? *Dvojklik.* [Online] ESET, 1. červenec 2019. [Citace: 26. srpen 2022.] https://www.dvojklik.cz/jak-zvolit-bezpecne-ciselne-heslo/.

ESET. 2021. Návod: jak chránit chytrý telefon s Androidem. *Dvojklik.* [Online] ESET, 26. duben 2021. [Citace: 10. říjen 2022.] https://www.dvojklik.cz/navod-jak-chranit-chytry-telefon-s-androidem/.

IDG. 2014. Zabezpečte si podniková data. *Security World.* listopad, 21. listopad 2014.

Kolouch, Jan a Bašta, Pavel. 2019. *CyberSecurity.* Praha : CZ.NIC, 2019. ISBN 978-80-88168-31-7.

Kos, Adam. 2022. Rozpoznávání obličeje na chytrých telefonech: Je lepší Face ID nebo řešení Androidu? *Jablickar.* [Online] 13. leden 2022. [Citace: 12. září 2022.] https://jablickar.cz/rozpoznavani-obliceje-na-chytrych-telefonech-je-lepsi-face-id-nebo-reseni-androidu/.

Matyáš, Vašek a Krhovják, Jan. 2008. *Autorizace elektronických transakcí a autentizace dat i uživatelů.* Brno : Masarykova univerzita, 2008. 978-80-2104-556-9.

Microsoft. Microsoft. [Online] [Citace: 30. říjen 2022.] https://www.microsoft.com/cs-cz/security/business/identity-access/microsoft-entra-verified-id.

Moravec, Petr. 2016. Čtečky otisku prstů pod drobnohledem – jak fungují? *Mobilizujmeme.* [Online] 20. únor 2016. [Citace: 10. září 2022.] https://mobilizujeme.cz/clanky/ctecky-otisku-prstu-pod-drobnohledem-jak-funguji.

Nordpass. Top 200 most common passwords. *NordPass.* [Online] [Citace: 25. srpen 2022.] https://nordpass.com/most-common-passwords-list/.

Rak, Roman, Matyáš, Vašek a Říha, Zdeněk. 2008. *Biometrie a identina člověka ve forenzních a komerčních aplikacích.* Praha : Profesionál, 2008. ISBN 978-80-247-2365-5.

Sham, Swaroop. 2021. Security Questions: Best Practices, Examples, and Ideas. *okta.* [Online] 4. březen 2021. [Citace: 28. srpen 2022.] https://www.okta.com/blog/2021/03/security-questions/.

Spector, Lincoln. 2016. When to choose a password, when to choose a PIN. *PCWorld.* [Online] 15. červen 2016. [Citace: 26. srpen 2022.] https://www.pcworld.com/article/414922/when-to-choose-a-password-when-to-choose-a-pin.html.

Šubrt, Tomáš. 2011. *Ekonomicko-matematické metody.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2011. ISBN 978-80-7380-345-2.

Tristul. Autentizace a autorizace. *Tristul.* [Online] http://www.trisul.cz/bezpecnost-autentizace-autorizace/.

8 Seznam obrázků, tabulek a grafů

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů