VYSOKÁ ŠKOLA POLYTECHNICKÁ JIHLAVA

Aplikovaná informatika

Synergie vícefaktorového ověřování a Single Sign-On

Bakalářská práce

Autor práce: Adam Polák

Vedoucí práce: Mgr. Antonín Přibyl

Jihlava 2024

Vysoká škola polytechnická Jihlava

Tolstého 16, 586 01 Jihlava

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Autor práce:	**Adam Polák**
Studijní program:	Aplikovaná informatika
Obor:	Aplikovaná informatika
Garant studijního programu:	Ing. Lenka Kuklišová Pavelková, Ph.D.

Název práce:	**Synergie více faktorového ověřování a Single Sign-On**
Vedoucí práce:	Mgr. Antonín Přibyl
Cíl práce:	Bakalářská práce se bude zabývat výzkumem a implementací synergie mezi více faktorovým ověřováním (MFA) a Single Sign-On (SSO) pro zjednodušení a zrychlení přihlašování na sdílených počítačích ve zdravotnickém prostředí a zejména pak zvýšení bezpečnosti přístupu personálu k ICT prostředkům nemocnice. Zjištění ukazují, že kombinace těchto technologií má významný vliv na efektivitu práce zdravotnického personálu, umožňuje jim rychlý a bezpečný přístup k nezbytným IT systémům a aplikacím. Práce se zaměří na analýzu potřeb a požadavků personálu, návrh a implementaci systému MFA a SSO a hodnocení jejich dopadu na pracovní postupy a výkon zdravotnického personálu. Výsledky práce poskytnou cenné poznatky a doporučení pro efektivní využití MFA a SSO v rámci zdravotnických organizací.

Abstrakt

Bakalářská práce se zaměřuje na implementaci systému MFA a SSO a hodnocení dopadu na pracovní postupy zaměstnanců Nemocnice Jihlava. Teoretická část bakalářské práce popisuje, jaké možnosti byly na výběr pro implementaci MFA a SSO systému, popis vybrané platformy pro implementaci. Praktická část dále popisuje analýzu potřeb a požadavků organizace, testování pilotního nasazení v rámci jednoho oddělení, popis samotné implementace v celé organizaci, hodnocení dopadu a výsledků, kterých jsme dosáhli díky MFA a SSO.

Klíčová slova

Vícefaktorového ověřování (MFA), Single Sign-On (SSO), Zdravotnictví

Abstract

The bachelor thesis focuses on the implementation of the MFA and SSO system and the evaluation of the impact on the work practices of the employees of the Jihlava Hospital. The theoretical part of the bachelor thesis describes what options were chosen for the implementation of the MFA and SSO system, description of the selected platform for implementation. The practical part further describes the analysis of the needs and requirements of the organization, testing of the pilot deployment within one department, description of the actual implementation in the whole organization, evaluation of the impact and results achieved through MFA and SSO, the results are evaluated by employees who use the MFA and SSO system at work.

Keywords

Multi-Factor Authentication (MFA), Single Sign-On (SSO), Healthcare

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Podle § 47b zákona o vysokých školách souhlasím se zveřejněním své práce podle směrnice prorektora pro studium č. 2/2020, a to bez ohledu na výsledek obhajoby.

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mě požadovat přiměřený příspěvek na úhradu nákladů vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne 10. dubna 2024

…….

Podpis studenta

Poděkování

Rád bych zde poděkoval svému vedoucímu bakalářské práce Mgr. Antonínu Přibylovi za rady a podporu při psaní této bakalářské práce.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

ID	Identifikace
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MFA	Vícefaktorové ověřování
PC	Osobní počítač
PIN	Personal Identification Number
RFID	Radiofrekvenční identifikace
OU	Organizational Unit
SSL	Secure Sockets Layer
GPO	Group Policy Object
SSO	Single Sign-On

Úvod

Když jsem před několika lety začal pracovat ve zdravotnické organizaci, rychle jsem si uvědomil, jak důležitá je správa zabezpečení a pohodlný přístup k citlivým zdravotnickým informacím. Každý den jsme se potýkali s výzvami, jak zaručit bezpečný a rychlý přístup personálu k pacientským datům. Zákon o kybernetické bezpečnosti totiž stanovuje, jak heslo uživatele má být komplexní, jaká je jeho doba platnosti, zakazuje použití stejného hesla a zakazuje používání hesel, která jsou snadno uhodnutelná. Tato opatření jsou v souladu s moderními standardy kybernetické bezpečnosti a představují odpověď na neustálé se vyvíjející hrozby v digitálním světě.

Práce ve zdravotnictví je často hektická a stresující. Efektivní přihlašovací postupy mohou udělat zásadní rozdíl ve výkonu a péči poskytované pacientům. Personál v nemocnici by si tak nemusel pamatovat veškerá hesla pro přihlašování do různých systémů používané v rámci organizace. Místo zdlouhavého zadávání hesla o různých znacích by se zaměstnanci mohli přihlašovat a autentizovat například pomocí ID karty a zadání číselného pinu nebo biometriky.

Nemocnice Jihlava je největší nemocnicí na Vysočině. Je jednou z pěti nemocnic zřizovanou Krajem Vysočina. Ročně zde zdravotníci provedou více než 500 tisíc ambulantních ošetření (Výroční zpráva, 2022).

Počet těchto ošetření rok od roku stoupá, například ještě v roce 2017 bylo číslo o více než 100 tisíc nižší (Výroční zpráva, 2017). S počtem pacientů stoupá také počet přihlášení zdravotníků do systému, zvyšuje se počet IT techniky, obsluhujícího personálu.

V jihlavské nemocnici se ročně provede zhruba 7,5 tisíce operací (Výroční zpráva, 2017), z toho asi 5,5 tisíce je plánovaných a zbytek akutních operací. Tato čísla se měnila za poslední roky v souvislosti s onemocněním Covid 19, který pro zdravotnická zařízení, Nemocnici Jihlava nevyjímaje, znamenal omezení plánované péče. Omezena byla tedy plánovaná operativa velkých výkonů, jako jsou ortopedické operace, například totální endoprotézy. Výjimku měli onkologičtí pacienti a neodkladné stavy. Od roku 2018 je tedy počet operací kvůli tomu zkreslený.

Nemocnice Jihlava zaměstnává více než 1500 lidí na hlavní pracovní poměr, dalších zhruba 300 lidí zde pracuje na vedlejší pracovní poměr nebo dohody o provedení práce. Počty zaměstnanců se rok od roku zvyšují, jejich počet stoupl za posledních deset let téměř o třetinu (Výroční zpráva, 2022, 2017)

Průměrný přepočtený počet zaměstnanců		
Kategorie zaměstnanců	**Rok 2021**	**Rok 2022**
Lékaři	245,71	250,37
Farmaceuti	12,57	12,68
Všeobecné sestry a porodní asistentky	683,83	698,07
Ost. zdrav. prac. nelékaři s odb. způsobilostí	96,88	95,66
Zdrav prac. nelékaři s odb. způsobilostí	38,57	40,16
Zdrav. prac. nelék. pod odb. dohledem	208,15	222,54
Jiní odb. prac. nelékaři s odb. způsobilostí	3,57	3,13
THP	94,85	102,11
Dělníci a provozní pracovníci	114,55	114,9
Celkem	**1498,78**	**1539,62**

Tabulka 1: Průměrný počet zaměstnanců

zdroj: (nemji.cz)

Průměrný přepočtený počet zaměstnanců			
Kategorie zaměstnanců	rok 2010 1	rok 2011 2	Rozdíl ,+ -, 3=2-1
Lékaři	158,73	164,11	5,38
Farmaceuti	7,00	7,00	0,00
Všeobecné sestry a porodní asistentky	558,64	561,76	3,12
Ost. zdrav. prac nelékaři s odb. způsobilostí.	84,60	84,12	-0,48
Zdrav prac. nelékaři s odb. způsobilostí	17,29	23,03	5,74
Zdrav. prac. nelék. pod odb. dohledem	151,37	152,96	1,59
Jiní odb. prac. nelékaři s odb. způsobilostí	1,00	1,0	0,00
THP	72,46	74,04	1,58
Dělníci a provozní pracovníci	118,16	116,85	-1,31
Celkem	1169,25	1184,87	15,62

Tabulka 2: Průměrný počet zaměstnanců 2010/2011

zdroj: (nemji.cz)

Je jasné, že se stoupajícím počtem zaměstnanců a pacientů bylo potřeba změnit a ulehčit přístupy, které potřebují nejenom zdravotníci ke své práci, a minimalizovat časové ztráty při přihlašování. Navíc v období, kdy nám do životů zasáhlo onemocnění Covid 19, bylo potřeba řešit jednodušší přihlašování zdravotníků do systému. Ti byli mnohdy i hodiny v ochranných oblecích, ve kterých byl každý pohyb navíc obtížný, a vítali každé zjednodušení a ulehčení práce, jako právě přihlášení do systému.

Motivace

Hlavním hnacím impulsem mé bakalářské práce je představit systém MFA a SSO širšímu publiku v České republice. Tyto pokročilé technologie dosud možná nezaznamenaly širokou známost, a proto se mé úsilí zaměřuje na rozšíření povědomí o jejich potenciálu a výhodách.

Cílem mé práce není pouze přiblížit tato inovativní řešení pro zdravotnická zařízení, ale rovněž je prezentovat jako užitečný nástroj pro různé organizace, které manipulují s osobními či jinými kritickými údaji. Věřím, že MFA a SSO nejsou jen prostředky ke zvýšení bezpečnosti přístupu, ale také klíčovým prvkem v optimalizaci pracovních procesů a zvyšování efektivity práce v digitálním prostředí. Rozšířením povědomí o těchto technologiích chci přispět k vytvoření informovanějšího prostředí, ve kterém organizace mohou lépe chápat a využívat moderního zabezpečení přístupu. Tato práce se tak stává krokem směrem k technologické osvětě a zdůrazňuje možnosti, které MFA a SSO mohou nabídnout organizacím v širším spektru odvětví v České republice.

Cíl práce

Hlavním cílem mé bakalářské práce je detailní popis procesu implementace systému MFA a SSO. Bude provedena důkladná analýza tohoto systému s důrazem na jeho výkonnost a dopady na pracovní postupy zdravotnického personálu.

Tímto komplexním přístupem budeme schopni poskytnout podrobný a vyvážený obraz o implementaci a účinnosti systému MFA a SSO ve specifickém prostředí Nemocnice Jihlava.

1 Teoretická část

Teoretická část vysvětluje, na jakých principech funguje MFA a SSO. K tomu nastiňuje současný stav v Nemocnici Jihlava a ukazuje, jaká jsou možná řešení.

1.1 Vícefaktorového ověřování MFA

Vícefaktorové ověřování (MFA) představuje sofistikovaný bezpečnostní přístup, který vychází z konceptu vyžadování více než jednoho ověřovacího prostředku či faktoru při snaze získat přístup k systému, účtu nebo citlivým informacím. Jeho základním účelem je posílit celkové bezpečnostní opatření tím, že nutil uživatele poskytnout kombinaci unikátních prvků, čímž výrazně redukuje riziko neoprávněného přístupu a zneužití.

MFA spojuje různé kategorie faktorů, jako jsou znalosti (hesla, PINy), majetek (fyzické nebo digitální objekty), charakteristiky (biometrie), poloha, čas a akce. Uživatel tak musí prezentovat alespoň dva nebo více těchto odlišných prvků, aby úspěšně prošel ověřovacím procesem. Tato kombinace poskytuje robustní vrstvu bezpečnosti, která se stává klíčovým prvkem v prevenci kybernetických hrozeb a chrání důvěrná data před neoprávněným přístupem.

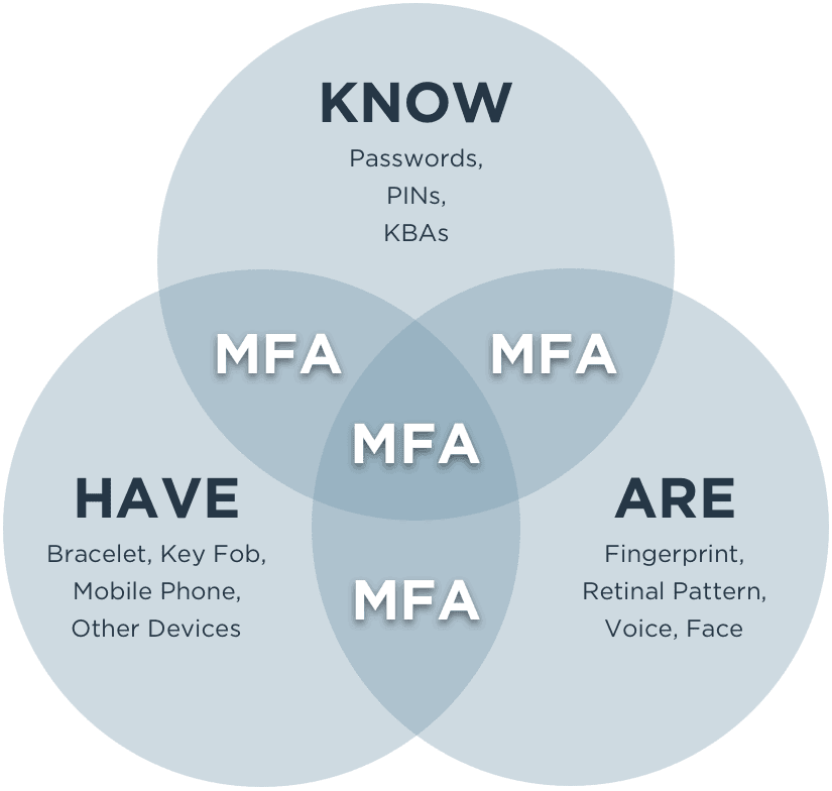
Implementace MFA reaguje na dynamiku moderního kybernetického prostředí a zdůrazňuje důležitost komplexního přístupu k zabezpečení, kde jednoúrovňové metody jsou stále více náchylné k překonání. MFA tedy výrazně přispívá k posílení celkové bezpečnostní architektury, a přináší tak uživatelům a organizacím větší klid a důvěru ve správu citlivých informací a digitálních prostředků.

1.1.1 Typy vícefaktorového ověřování

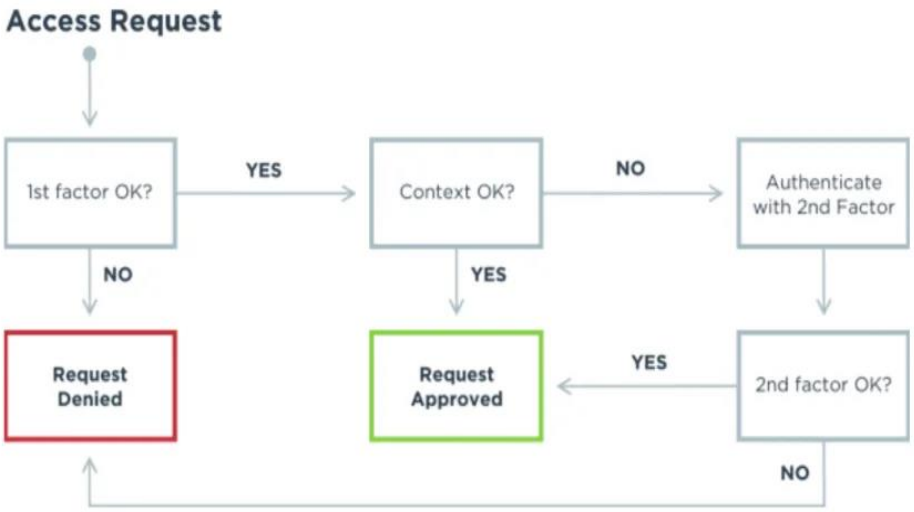
Kombinací těchto faktorů MFA poskytuje vyvážený a sofistikovaný přístup k zabezpečení, snižuje riziko neoprávněného přístupu a přispívá k celkové bezpečnosti informačních systémů.

1. **Znalosti (Something You Know):**
    - Nejčastějším příkladem je heslo nebo PIN. Uživatel musí poskytnout něco, co zná.
2. **Majetek (Something You Have):**
    - Zahrnuje fyzické objekty nebo digitální zařízení, které uživatel vlastní. Patří sem RFID karty, mobilní zařízení s generátorem jednorázových kódů (OTP), USB tokeny apod.
3. **Charakteristiky (Something You Are):**
    - Využívá biometrické charakteristiky samotného uživatele, například otisky prstů, rozpoznání obličeje, hlasu nebo duhovky.
4. **Poloha (Somewhere You Are):**
    - Založeno na geografické poloze uživatele nebo jeho zařízení. Tento faktor může být využíván při ověřování prostřednictvím GPS nebo jiných lokalizačních technologií.

5. **Čas (Sometime You Are):**
    - Ověřování na základě časových parametrů, například ověření uživatele v určitém časovém okně.
6. **Akce (Something You Do):**
    - Zahrnuje ověřování na základě konkrétních akcí uživatele, například gesta na dotykovém zařízení, způsoby interakce s klávesnicí nebo pohyby myší.



Obrázek 1: Faktory ověřování
zdroj: (pingidentity.com)



Obrázek 2: Princip fungování MFA
Zdroj: (pingidentity.com)

Zvyky se těžko odbourávají. Většina organizací nemá čas ani prostředky na úplné odstranění uživatelských jmen a hesel pro ověřování uživatelů, takže jsou nutné další způsoby ověření identity uživatele. Vícefaktorové ověřování udržuje data a systémy v bezpečí tím, že přidává překážky, které zastaví špatné hráče v jejich počínání. I když je heslo nebo jiná metoda ověřování kompromitována, je velmi vzácné, aby měl hacker k dispozici také druhý nebo třetí faktor ověřování. Funkce MFA zabraňuje uživatelům bez potřebného počtu ověřovacích faktorů v přístupu k vašim zdrojům. (Eight Benefits of Multi-Factor Authentication (MFA), 2021)

Jediné kompromitované heslo umožnilo hackerům narušit provoz společnosti Colonial Pipeline, protože k přístupu do její sítě VPN nebyly vyžadovány jiné formy ověření. Ransomware a další kybernetické útoky se staly hlavní prioritou v agendě kybernetické bezpečnosti USA. Přestože organizace mohou poskytovat školení o kybernetické bezpečnosti, zaměstnanci stále podléhají taktice phishingu nebo z pohodlnosti sdílejí hesla. Zákazníci se také mohou stát obětí podvodů nebo jim mohou být odcizena jejich data. Systém MFA zabraňuje zlým subjektům používat kompromitované přihlašovací údaje ke vstupu do vašich systémů, protože nemohou poskytnout druhý nebo třetí faktor ověření. (Eight Benefits of Multi-Factor Authentication (MFA), 2021)

1.2 Jednotné přihlašování SSO

Jednotné přihlašování, často označované jako Single Sign-On (SSO), reprezentuje inovativní koncept v oblasti informačních technologií přinášející uživatelům revoluční pohodlí při interakci s různými systémy a aplikacemi. Tato moderní technologická filozofie vychází z jednoduchého, avšak mocného principu: umožnit uživateli přihlásit se jednou a následně nabídnout bezproblémový přístup k širokému spektru digitálních služeb a aplikací, aniž by bylo nutné opakovaně zadávat přihlašovací údaje. Tím, že uživateli poskytuje virtuální klíč k digitálnímu světu po jediném úspěšném přihlášení, eliminuje SSO frustrující proces opakované autentizace. Tento koncept nabízí jednotné brány do digitálního prostoru, kde uživatel může plynule

přecházet mezi různými systémy a aplikacemi, aniž by byl obtěžován množstvím přihlašovacích údajů.

SSO nejen zvyšuje uživatelskou pohodu, ale také přináší potenciál pro zvýšení bezpečnosti, zabraňující slabým heslům nebo neoprávněnému používání účtů. Tento koncept nese s sebou vize jednoduchosti a efektivity ve světě digitálního přihlašování, vytvářející jednotný a bezproblémový zážitek pro uživatele v kybernetickém prostoru.

1.2.1 Možnosti jednotného přihlašováni

Výběr metody jednotného přihlašování závisí na konfiguraci ověřování dané aplikace. Pro cloudové aplikace jsou často využívány federativní možnosti, včetně protokolů jako OpenID Connect, OAuth a SAML. Některé aplikace mohou preferovat jednotné přihlašování založené na heslech, kdežto jiné mohou podporovat propojené nebo zakázané jednotné přihlašování. (Co je jednotné přihlašování ve službě Microsoft Entra ID?, 2023)

Tato variabilita v metodách jednotného přihlašování umožňuje organizacím flexibilně přizpůsobit své přístupy zabezpečení dle specifických požadavků, což v konečném důsledku posiluje bezpečnostní opatření a zvyšuje uživatelskou pohodu.

1. **Webové SSO (Web SSO):**
    - Tento typ SSO je zaměřen především na webové aplikace. Uživatel se přihlásí jednou a poté má automatický přístup ke všem webovým aplikacím, které jsou integrovány do SSO systému. Příkladem může být přihlášení pomocí účtu Google nebo Facebooku na různých webových stránkách.
2. **Enterprise SSO:**
    - Enterprise SSO je navrženo pro podnikové prostředí a umožňuje uživatelům jedno přihlášení pro přístup k různým podnikovým systémům a aplikacím. To zahrnuje interní software, e-mailové systémy a další firemní nástroje.
3. **Federované SSO:**
    - Tento typ SSO umožňuje uživatelům přihlásit se na jedné federaci a poté získat přístup k zdrojům v jiných federovaných organizacích. Je často využíván v rámci spolupráce mezi organizacemi nebo napříč různými sektory.
4. **Desktop SSO:**
    - Desktop SSO umožňuje uživatelům přihlášení na svém počítači nebo pracovní stanici a automatický přístup ke všem aplikacím a zdrojům, ke kterým mají oprávnění.
5. **Mobile SSO:**
    - Tento typ SSO je optimalizován pro mobilní zařízení a umožňuje uživatelům jednoduché a bezpečné přihlášení na svých telefonech či tabletech.

Obrázek 3: Princip fungování AWS SSO

zdroj: (aws.amazon.com)

S přechodem na cloud používají zaměstnanci na pracovišti stále více aplikací. Vyžadování samostatných uživatelských jmen a hesel pro každou aplikaci je pro zaměstnance velkou zátěží a upřímně řečeno je nereálné. Jednotné přihlašování tuto kognitivní zátěž snižuje.

Jednorázové přihlášení také šetří čas, a tím zvyšuje produktivitu zaměstnanců. Vzhledem k tomu, že 68 % zaměstnanců každou hodinu přepíná mezi deseti aplikacemi, může eliminace vícenásobného přihlašování ušetřit firmě značný čas i peníze.

Řešení SSO, která jsou součástí systému správy identit a přístupu, obvykle obsahují portál aplikací. Pokud chtějí zaměstnanci aplikaci používat, vyberou si ji na portálu. Pokud uživatel aplikaci nemá, může o ni požádat prostřednictvím portálu a ta je přidána se zapnutým SSO. Vše probíhá rychle, takže uživatelé, kteří by mohli být odrazováni od žádosti o aplikace nebo jejich používání, je budou s větší pravděpodobností používat. (Proč je SSO důležité?, 2023)

1.3 Současný stav problematiky

S rychlým rozvojem digitálních technologií ve zdravotnictví vstupujeme do nové éry, kde jsou zdravotníci nevyhnutelně konfrontováni s potřebou práce v několika informačních systémech a aplikacích, které obsahují citlivá pacientská data. Tento trend přináší výzvy spojené s administrativní zátěží, kdy zdravotníci musí spravovat a pamatovat si více hesel pro přístup do různých systémů. V důsledku toho je čas, který by mohl být věnován přímé péči o pacienty, ztracen ve zdánlivě nekonečných cyklech přihlašování.

V této situaci vzniká naléhavá potřeba inovativních řešení, která nejen zajišťují bezpečnost citlivých dat, ale také optimalizují pracovní postupy zdravotníků. Ztracený čas při opakovaném zadávání hesel může být efektivněji využit pro poskytování péče pacientům a prohlubování odborných dovedností zdravotníků. V tomto kontextu se implementace moderních technologií, jako je jednotné přihlašování (SSO) a vícefaktorové ověřování (MFA), stává klíčovým krokem

směrem k efektivnějšímu a bezpečnějšímu zdravotnickému prostředí. Tyto technologie nejen zvyšují bezpečnostní standardy, ale také přinášejí efektivitu a pohodlí zdravotníkům, čímž posilují celkový výkon zdravotnických organizací.

1.4 Seznámení se s problematikou

V prostředí nemocnice se běžně využívá rozsáhlé škály aplikací a informačních systémů zabezpečených prostřednictvím uživatelských jmen a hesel. Bohužel, některé z těchto aplikací neumožňují ověření v rámci domény, což vede k tomu, že zdravotníci jsou nuceni si pamatovat více přihlašovacích údajů. Tato situace se dále komplikuje používáním tzv. obecných účtů na koncových stanicích v ambulancích a sestrách. V současné konfiguraci každé oddělení disponuje svým vlastním obecným účtem, což sice usnadňuje rychlejší přihlašování do počítačů, ale zároveň zvyšuje počet přihlašovacích údajů, které musí zdravotníci spravovat. V kancelářích a inspekčních pokojích se naopak uživatelé přihlašují k individuálním profilům, což dále komplikuje a zpomaluje celkový proces práce na počítačích. Implementace systému vícefaktorového ověřování (MFA) a jednotného přihlašování (SSO) se tak jeví jako klíčový krok směrem k efektivnější a bezpečnější práci s počítači. Tato technologická inovace by nejen zrychlila celý proces přihlašování, ale také by snížila administrativní břemeno spojené s pamatováním a správou více uživatelských účtů. Díky tomu by se zdravotníci mohli plněji soustředit na poskytování péče pacientům, což je v jádru jejich profesionálního poslání.

1.5 Rešerše možných řešení

Na trhu se nyní nachází rozsáhlý výběr řešení schopných implementovat nástroje pro jednotné přihlašování (SSO) a vícefaktorové ověřování (MFA) pro organizace. Pro naši nemocnici je kritické vybrat takové řešení, které efektivně využije RFID ID karet pro autentizaci, zároveň poskytne centrální správu uživatelů a koncových stanic. Po vypsání veřejné zakázky byly dvěma předními firmami, které předložily nabídku na svá řešení, firma Autocont a firma KeyShield SSO. Firma Autocont, prémiový partner společnosti Imprivata, představila svůj produkt Imprivata OneSign, který se těší vysoké reputaci v oblasti implementací jednotného přihlašování a vícefaktorového ověřování. Tato firma má bohaté zkušenosti s implementací a prodejem produktů Imprivata OneSign v České republice. Druhou firmou, která se účastnila výběrového řízení, byla firma KeyShield SSO, přicházející s vlastním produktem KeyShield SSO. Jejich nabídka zdůrazňuje možnosti využití v různých prostředích a slibuje efektivní řešení pro implementaci SSO a MFA. Obě firmy prezentují silné stránky svých produktů a mají zkušenosti s nasazením ve zdravotnických organizacích. Rozhodování bude záviset na specifických požadavcích nemocnice, finančních aspektech a konkrétních výhodách, které každé řešení nabízí. Analyzování nabídek a konzultace s oběma firmami mohou poskytnout podrobnější pohled na to, které řešení bude nejlépe odpovídat potřebám a cílům naší nemocnice.

1.5.1 Imprivata OneSign

Imprivata OneSign, i když v České republice možná není tak široce známá jako v zahraničí, představuje významné a efektivní řešení pro organizace, zejména ty velké, které se zaměřují na využívání ID karet pro přihlašování do koncových stanic. Tato platforma je v souladu

s předpisy v oblasti kybernetické bezpečnosti, konkrétně se Zákonem o kybernetické bezpečnosti, což ji činí vhodnou volbou pro zdravotnická prostředí.

Imprivata OneSign umožňuje přihlášení pomocí ID karet prostřednictvím kombinace přiložení karty ke čtečce u počítače a zadání PINu. Tímto způsobem se nejen splňují právní předpisy, ale zároveň poskytuje jednoduchý a bezpečný způsob přístupu k systémům. Výhodou je možnost rozdělit přihlašování na sdílené a personifikované, což umožňuje flexibilitu podle konkrétních potřeb organizace.

Jednotné přihlašování, implementované pomocí Imprivata OneSign, může být aplikováno na širokou škálu aplikací, včetně webových a android čteček, což usnadňuje a zrychluje přístup k důležitým informacím. Zvláště je významné, že tato platforma podporuje i snadnější přihlášení do android čteček, což je výhledově důležité pro proces výdeje léků pacientům na lůžkách. S Imprivata OneSign tak organizace získává komplexní a inovativní nástroj, který nejen posiluje bezpečnost, ale také zvyšuje efektivitu práce ve zdravotnickém prostředí.

Obrázek 4: Imprivata OneSign logo
zdroj: (allvectorlogo.com)

Pro získání přístupu k aplikacím, sítím a online zdrojům jsou uživatelé stále častěji povinni poskytovat uživatelská jména a hesla obsahující složité kombinace písmen, číslic a speciálních znaků. Tyto požadavky na silné heslo poskytují uživatelům lepší ochranu proti narušení bezpečnosti a umožňují organizacím vyhovět rostoucím regulačním požadavkům. Se zvyšující se složitostí hesla však roste i frustrace uživatelů a nespokojenost. Složitá hesla obsahující písmena, číslice a speciální znaky jsou pro lidi těžko zapamatovatelná, zvláště když je hesla třeba často měnit. Čím více aplikací člověk používá, tím více hesel si musí pamatovat. Tehdy nastává „únava heslem“ a uživatelé se uchylují ke sdílení svých hesel s ostatními, píšou je na papírky schované pod klávesnicemi, nebo je dávají do zásuvky u stolu. Tyto zkratky a řešení usnadňují neoprávněné osobě získat legitimní přihlašovací údaje uživatele. To samozřejmě může vést ke krádeži informací, zneužití nebo sabotáži a porušení vládních a průmyslových předpisů, které nařizují ochranu a soukromí zákaznických a důvěrných údajů. Složitost hesel také vytváří problémy pro IT týmy. Uživatelé, kteří zapomenou svá hesla, jsou často uzamčeni ze svých systémů a nemohou vykonávat svou práci. Poté zavolají IT helpdesk pro resetování hesla. Nejenže jsou tyto hovory časově náročné a nákladné, ale také mají tendenci

odvádět technický personál od strategičtějších IT iniciativ. (Imprivata OneSign Single Sign-On, 2015)

Problémy s přístupem ke sdíleným pracovním stanicím mohou být pro uživatele frustrující. S aplikací Imprivata OneSign však stačí pouhé přejetí identifikačním průkazem nebo dotyk prstu na čtečce otisků prstů, abyste okamžitě odemkli nebo zamkli jakoukoli pracovní stanici. Tento přístup bez kliknutí umožňuje rychlé přepínání uživatelů mezi více souběžnými pracovními stanicemi se systémem Windows i bezpečné a rychlé přepínání uživatelů na obecných kioskových pracovních stanicích. (Imprivata OneSign Single Sign-On, 2015)

1.5.2 KeyShield SSO

KeyShield SSO je produktem české společnosti KeyShield SSO. Má obdobné funkčnosti jako Imprivata OneSign a je zaměřená nejen na zdravotnictví.

KeyShield SSO je skutečné řešení SSO, které zjišťuje a poskytuje identitu uživatelů sítě na základě jejich ověření v eDirectory, Active Directory nebo LDAP (prostřednictvím klienta KeyShield SSO). Jakmile je uživatel ověřen, KeyShield SSO ověří jeho identitu a uchovává informace o IP adrese a plném jménu uživatele. Pokud se pak uživatel pokusí připojit k nějakému informačnímu systému, je jeho identita ověřena dotazem na KeyShield SSO na základě IP adresy. Pokud je uživatel známý, není nutné žádné další ověřování. Tento přístup je efektivnější a bezpečnější než způsob, který funguje například u internetového prohlížeče, který uchovává jména a hesla, jež byla použita pro ověření. (KeyShield SSO, 2023)

Obrázek 5: KeyShield SSO logo
zdroj: (keyshieldsso.com)

Nemocnice a další zdravotnická zařízení mají velkou část uživatelů – lékařů a sester – kteří nepracují na „svém“ počítači ve „své“ kanceláři. Pohybují se podle potřeby a využívají sdílené počítače na sesternách, vyšetřovnách, operačních sálech apod. Jejich hlavní pracovní náplní je péče o pacienty a tradiční koncept „ukončit“ – „odhlásit“ – „přihlásit“ – „spustit“ – „přihlásit“ je velmi zdržuje. Proto se často setkáváme s tím, že všichni pracují na toho, kdo se na začátku směny přihlásil jako první, že uživatelé omezí použití informačního systému, aby nemuseli podstoupit výše uvedený postup, že požádají někoho jiného, aby akci provedl za ně, nebo tedy že postupem s klením projdou a přijdou pokaždé o cenné minuty, které by mohli věnovat své práci. (Nemocniční přihlašovací systém, 2023)

Osobní karty, čipy, tokeny, které nyní uživatelé používají pro otevírání dveří a vjezdů, docházkový systém, objednání a vyzvednutí oběda nebo placení v kantýně jsou využitelné a ve skutečnosti ideální i pro systém přihlašováni a rychlého střídání – všichni je znají, mají je pořád s sebou, a chrání si je. Přiložením karty ke čtečce uživatel oznamuje, kdo je, a nemusí tedy psát své jméno.

Zadáním hesla potvrdí svou identitu a je přihlášen tzv. dvoufaktorově – i kdyby někdo jiný znal jméno a heslo, bez karty se přihlásit nemůže. (Nemocniční přihlašovací systém, 2023)

1.6 Zhodnocení dostupných řešení

Po pečlivém posouzení obou řešení, KeyShield SSO a Imprivata OneSign, jsme došli k závěru, že obě nabízejí vysokou úroveň použitelnosti pro naši nemocnici. Přestože obě technologie poskytují efektivní jednotné přihlašování (SSO) a vícefaktorové ověřování (MFA), zdůraznili jsme několik klíčových faktorů, které nás vedly k preferenci Imprivata OneSign.

Jedním z klíčových faktorů rozhodujících ve prospěch Imprivata OneSign byla bezproblémová integrace s naší stávající infrastrukturou. Imprivata OneSign se ukázala být flexibilní a snadno přizpůsobitelná specifickým potřebám naší nemocnice, což znamená minimální rušení provozu a plynulou implementaci. Dále jsme zvážili praktičnost a uživatelskou přívětivost. Zatímco KeyShield SSO vyžaduje fyzickou interakci s čtečkou karty pro přihlášení a odhlášení, Imprivata OneSign umožňuje bezkontaktní přístup s použitím ID karty. Tato vlastnost je klíčová zejména v hektickém prostředí nemocnice, kde se každý okamžik počítá.

Celkově lze říct, že Imprivata OneSign poskytuje komplexní a uživatelsky příjemné řešení, které splňuje naše požadavky na bezpečnost, efektivitu a jednoduchost používání. Tímto jsme se rozhodli implementovat systém Imprivata OneSign jako optimální volbu pro naši zdravotnickou organizaci, věříme, že přinese značné výhody pro naše pracovní postupy a zabezpečení citlivých informací.

1.7 Použitá technologie

Pečlivě vybraná technologie hraje klíčovou roli ve zjednodušení práce zaměstnanců a správců. Její výběr není pouhým momentálním rozhodnutím, ale strategickým krokem směrem k dlouhodobému zefektivnění pracovních procesů a připravenosti na budoucí rozšíření. Včetně bezpečnostních opatření, oprav a nasazování nových funkcionalit, které budou postupně integrovány do pracovního prostředí. Touto perspektivou zajišťujeme, že zvolená technologie nejen že odpovídá současným potřebám, ale je připravena i na budoucí výzvy a inovace v oblasti zabezpečení a IT infrastruktury.

1.7.1 Imprivata OneSign

Imprivata OneSign představuje jedinečný produkt z portfolia společnosti Imprivata, který vyniká schopností spravovat přihlašování a autentizaci, s cílem zjednodušit a zabezpečit přístup k IT systémům a aplikacím. Jeho konfigurace je intuitivní a usnadněná díky webovému rozhraní, což umožňuje správcům snadno přizpůsobit nastavení podle specifických potřeb.

Obrázek 6: Platformní integrace
zdroj: (imprivata.com)

Jedním z klíčových prvků Imprivata OneSign je poskytování jednotného přihlašování, což výrazně snižuje nutnost opakovaného zadávání hesel. Tato funkce nejen zvyšuje pohodlí uživatelů, ale také přispívá k celkové bezpečnosti přístupu.

Flexibilita systému se projevuje v podpoře různých forem vícefaktorového ověřování. Uživatelé mohou využívat RFID karty, biometrické údaje nebo mobilní zařízení, což umožňuje implementaci bezpečnostních opatření dle konkrétních potřeb organizace.

Důležitým prvkem je také schopnost synchronizace s doménou, což centralizovaně usnadňuje správu uživatelských účtů a jejich přihlašovacích údajů. Tímto způsobem lze efektivně sledovat a auditovat přístupy uživatelů, toto vede k další vrstvě zabezpečení.

Intuitivní rozhraní Imprivata OneSign navíc zjednodušuje ovládání a tvorbu aplikačních profilů. Celkově představuje komplexní a inovativní nástroj, který nejen posiluje bezpečnost, ale i efektivitu práce v digitálním prostředí.

2 Praktická část

Před samotnou implementací Imprivata OneSign do organizace bylo potřeba vybrat oddělení, kde bude spuštěno pilotní testování softwaru. Museli jsme provést analýzu jejich požadavků a procesů. V analýze jsem se zabýval možnostmi rozšíření do budoucna a vytváření dalších přihlašování SSO pro ulehčení práce.

2.1 Analýza požadavků

U oddělení, kde se plánovalo zahájení testovací fáze, bylo hlavním požadavkem zdravotníků rychlé a bezpečnější přihlašování do nemocničního informačního systému. Dále požadovali zjednodušení procesu přihlašování do firemního intranetu a aplikace určené pro zobrazování rentgenových snímků. Splnění těchto kritérií by po úspěšném testování umožnilo rozšíření implementace do ambulantních prostor a lůžkových oddělení nemocnice, což by zefektivnilo práci zdravotníků a zvýšilo celkovou bezpečnost přístupu k citlivým datům. Při splnění těchto požadavků se po testování mohlo implementovat dále do ambulancí či lůžkových oddělení nemocnice. Laboratoře nebo lékárna dále požadovaly i vstup pro jiný typ aplikací, které využívají na svém oddělení.

2.2 Implementace

Partnerská společnost Autocont hrála klíčovou roli při implementaci systému Imprivata OneSign, poskytující cennou podporu jak během samotné instalace, tak v průběhu testovací fáze na plicním oddělení. Díky této spolupráci se podařilo odladit detaily přihlašovacího procesu a zajistit, že systém bude plně odpovídat specifickým potřebám a požadavkům uživatelů. Autocont, jako zkušený technologický partner, přispěl nejen svými odbornými znalostmi, ale také praktickými zkušenostmi s podobnými projekty, což umožnilo efektivně identifikovat a vyřešit potenciální problémy.

Imprivata OneSign byla implementována jak v místním virtuálním prostředí založeném na VMware, tak v cloudovém prostředí Azure využívajíc řešení tří virtuálních appliancí pro svůj provoz. Dvě z těchto appliancí, fungující jako databáze, využívají pro replikaci dat mezi sebou nástroj Oracle GoldenGate, čímž je zajištěna konzistence a dostupnost dat. Zatímco první databázová appliance je umístěna v místním virtuálním prostředí, druhá se nachází v cloudovém prostředí Azure. Třetí appliance, umístěná v místním prostředí, plní funkci servisního zařízení.

Imprivata dodává předinstalované virtuální appliace, což značně usnadňuje proces instalace a konfigurace. Během průvodce instalací si administrátoři nastavují klíčové parametry, jako jsou IP adresy, názvy hostitelů (hostname) a další potřebné konfigurace, což zajišťuje hladkou integraci systému do stávající IT infrastruktury. Tento přístup nejen zjednodušuje první kroky nasazení, ale také umožňuje flexibilní a bezproblémovou konfiguraci systému podle specifických potřeb organizace, ať už v místním VMware prostředí nebo v cloudové platformě Azure.

Celý systém je spravován prostřednictvím přehledného webového rozhraní, rozděleného do administrátorské konzole a konzole zařízení, které umožňují efektivní správu uživatelů, politik, a monitorování stavu jednotlivých appliancí.

Díky této komplexní implementaci a spolupráci s Autocontem se podařilo vytvořit robustní a bezpečný systém pro jednotné přihlašování, který zjednodušuje přístup k aplikacím a systémům, zlepšuje bezpečnost citlivých dat a zároveň zvyšuje efektivitu pracovních postupů zdravotníků, umožňujíc jim věnovat více času péči o pacienty.

2.3 Administrátorská konzole

Do administrátorské konzole mají přístup pouze autorizovaní uživatelé, kterými jsou správci IT Nemocnice Jihlava.

2.3.1 Uživatelská karta

Uživatelská karta slouží jako centrální místo pro správu uživatelských účtů, a to jak pro import účtů z domény, tak pro vytváření lokálních účtů přímo v rámci systému. V rámci uživatelské karty lze nastavovat různé politiky a pravidla, které dále zvyšují bezpečnost a kontrolu nad přihlašovacím procesem. Mezi tyto možnosti patří například nastavení délky PINu nebo limit na počet přiřazených karet.

2.3.2 Počítačová karta

Počítačová karta v rámci systému Imprivata OneSign poskytuje ucelený přehled o všech počítačích, na kterých je nainstalován Imprivata agent. Můžeme zde najít název počítače, jeho mac adresu, IP adresu, verzi nainstalovaného agenta, typ agenta, posledního přihlášeného uživatele, čas a datum přihlášení.

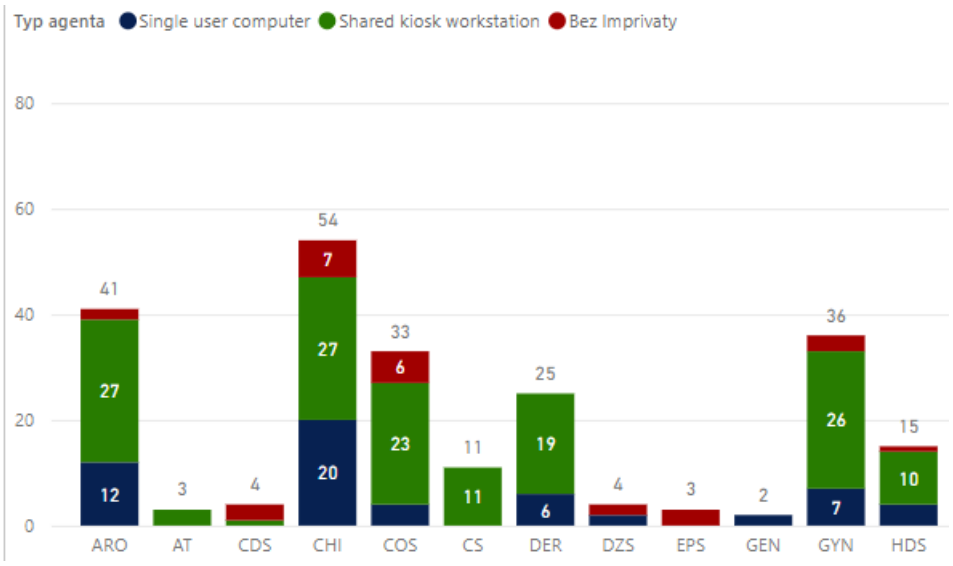
2.3.3 Karta aplikace

V Kartě aplikace se vytváří a nasazují nové profily pro jednotné přihlašování (SSO). Tento nástroj umožňuje administrátorům snadno definovat, jak bude přihlašovací proces pro různé aplikace zautomatizován.

2.3.4 Karta reportů

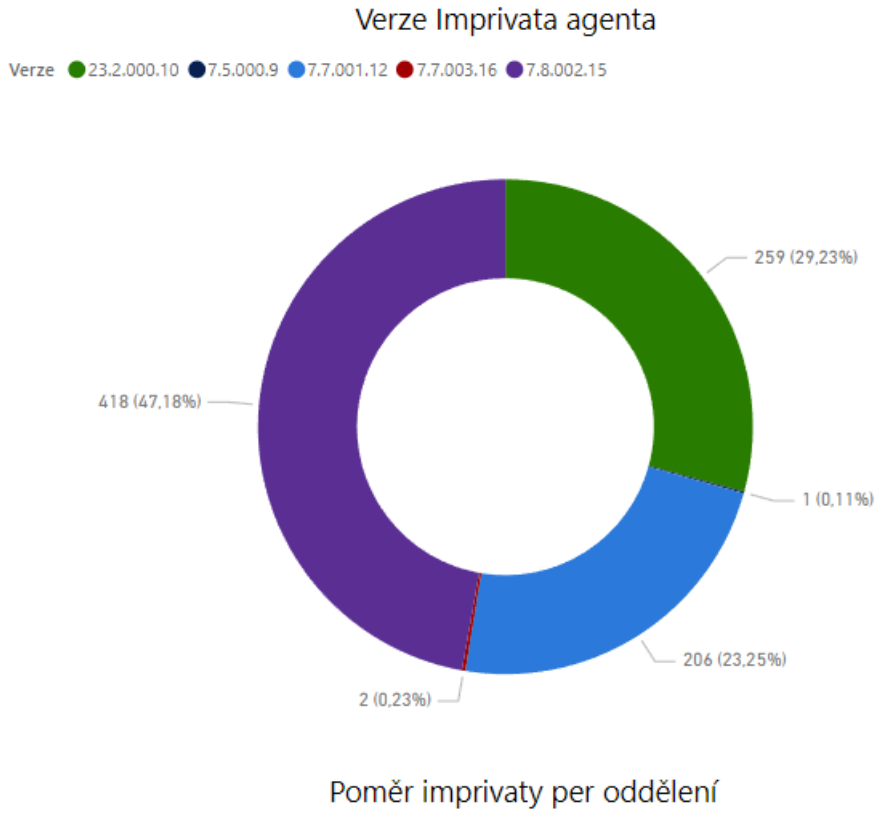
V kartě reportů můžeme najít různé logy a reporty, které zachycují širokou škálu aktivit a statistik. Tyto záznamy poskytují informace pro monitorování, audit a analýzu efektivity. Může se jednat například o aktivity uživatelů, kolik uživatelů má enrollovanou kartu, jaký typ agenta má nebo jakou verzi agenta počítač má.

Pro zlepšení přístupnosti a analýzy těchto dat využíváme Power Bi od Microsoftu. Tento nástroj slouží k vizualizaci dat, který umožňuje transformovat surová data do přehledných a interaktivních dashboardů.



Obrázek 7: Typy agentů a oddělení

zdroj: (vlastní práce)



Obrázek 8: Verze agentů na počítačích

zdroj: (vlastní práce)

2.4 Appliance konzole

2.4.1 Home

Na domovské obrazovce appliance konzole je přehled systémových stavů. Tento dashboard poskytuje uživatelům klíčové informace o aktuálním provozu a zdraví systému a umožňuje rychlou orientaci v jeho stavu a včasnou identifikaci potenciálních problémů nebo potřeb údržby.

2.4.2 Network

Na kartě network se nastavuje IP adresa jednotlivých appliance. Můžeme zde přenastavit host name appliance. Dá se zde nastavit i NTP server a SMTP server.

2.4.3 Systém

V systémové kartě je detailnější přehled o appliancích. Zde můžeme vidět, jak dlouho appliance běží, jestli zálohy proběhly v pořádku a jestli replikace mezi databázovými appliance probíhá správně.

2.4.4 Enterprise

V Enterprise můžeme přidávat nebo odebírat appliancce. Je zde i přehled o tom, jaká verze Imprivata je na appliance serverech.

2.4.5 Security

Zde se může vygenerovat nový SSL certifikát nebo prodloužit jeho působení.

2.4.6 Packages

Přes Packages probíha upgrade verzí Imprivata, je zde možnost jednoduché distribuce aktualizačního balíku na ostatní appliance.

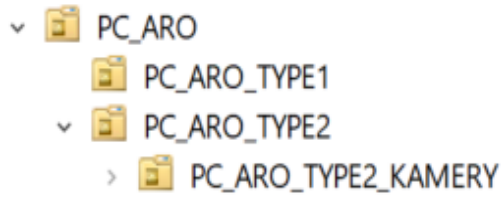
2.5 Deploy a instalace Agentů

Pro zajištění komunikace mezi koncovými stanicemi a aplikačním serverem Imprivata OneSign, je potřeba na těchto stanicích nainstalovat Imprivata agenta. Tento agent je dostupný ke stažení přímo ze serveru Imprivata, přičemž je možnost vybrat si mezi verzemi pro 32bitové a 64bitové operační systémy. V prostředí s více než tisícovkou počítačů, jako je tomu ve naší organizaci, by ruční instalace tohoto softwaru byla extrémně časově náročná.

Aby se tento proces zjednodušil a zrychlil, naše organizace využívá Microsoft System Center Configuration Manager (SCCM), což je nástroj pro hromadnou distribuci softwaru. SCCM umožňuje automatizovat proces instalace a správy softwaru na velkém počtu zařízení, což značně snižuje čas a úsilí potřebné pro tyto operace.

Před spuštěním distribuce agenta Imprivata je klíčové určit, který typ agenta bude na každé koncové stanici použit. Imprivata rozlišuje mezi dvěma typy přihlašování – typ 1 a typ 2, kde každý slouží pro specifické přihlašovací a bezpečnostní potřeby. Pro usnadnění správy a konfigurace skupinových politik (GPO) bylo pro každé oddělení vytvořeno Organizační Jednotky (OU) ve struktuře Active Directory, které obsahují název oddělení a typ použitého agenta.

Takový přístup nejenže zjednodušuje správu a nasazení Imprivata agentů, ale také umožňuje přizpůsobit nastavení politiky bezpečnosti podle specifických potřeb jednotlivých oddělení, což je zásadní pro zajištění bezpečného a efektivního přístupu k systémům a aplikacím ve velkých organizacích.



Obrázek 9: Ukázka OU
zdroj: (vlastní práce)

Pro Android zařízení se aplikace spojená s Imprivata OneSign instaluje přímo z Google Play Store, což zjednodušuje a zrychluje proces zavedení aplikace do praxe. Po instalaci aplikace na Android zařízení je nutné zadat IP adresu jednoho z appliance systému Imprivata OneSign, aby bylo možné zařízení správně konfigurovat a připojit.

Důležitým aspektem správy těchto Android zařízení je využití Microsoft Intune, což je služba pro správu mobilních zařízení (MDM) a mobilních aplikací (MAM), která poskytuje zabezpečené správcovské schopnosti pro zařízení ve firmě. Integrace s Microsoft Intune umožňuje organizacím centralizovaně spravovat instalaci, konfiguraci a bezpečnostní politiky aplikací na všech Android zařízeních. To zahrnuje možnost distribuce aplikací, nastavení bezpečnostních pravidel, monitorování stavu zařízení a vynucování dodržování firemních politik a standardů.

Využití Microsoft Intune společně s Imprivata OneSign přináší výhody v podobě vylepšené bezpečnosti, efektivity a správy mobilních zařízení, které mají přístup k citlivým firemním a zdravotnickým informačním systémům.

2.5.1 Přihlašovací typ 1

Typ 1 agenta v systému Imprivata OneSign je navržen tak, aby po přiložení ID karty k čtečce a zadání PINu došlo k přihlášení uživatele pod jeho doménový účet. Tento agent je ideální pro použití na personalizovaných počítačích, jako jsou ty, které využívají primáři, lékaři v inspekčních pokojích, dokumentační sestry a další. Počítače s tímto typem agenta jsou nastaveny tak, aby uživatele po uzamčení počítače neodhlásily po dobu dvanácti hodin. Pokud se uživatel znovu přihlásí v tomto časovém rozmezí, časovač se resetuje a opět začne počítat dvanáct hodin.

Na jednom počítači můžou být současně uzamčeny až dva uživatelské účty. V případě, že by se pokusil přihlásit třetí uživatel, systém automaticky odhlásí uživatele, který byl na systému aktivní (v uzamčeném stavu) nejdéle, a to po uplynutí patnácti minut od přihlášení třetího uživatele.

Toto opatření je zavedeno z důvodu uvolnění systémových zdrojů a optimalizace výkonu počítače.

Tato konfigurace poskytuje optimální rovnováhu mezi pohodlím uživatelů, kteří potřebují k počítačům přistupovat opakovaně během své směny, a bezpečnostními opatřeními, která zajistí, že systém zůstane chráněný a výkonný i při sdíleném využití.

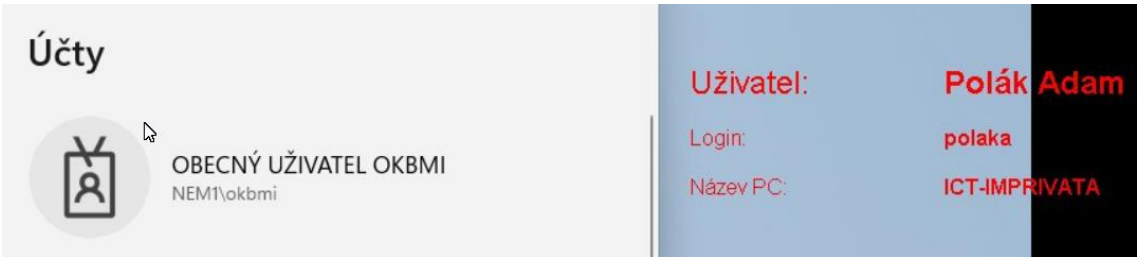
Obrázek 10: Ukázka časomíry na uzamčeném počítači
zdroj: (vlastní práce)

2.5.2 Přihlašovací typ 2

Typ 2 neboli kioskový mód využívá přihlašování tzv. obecného uživatele. Obecný uživatel se do počítače přihlašuje pomocí autologonu, každé oddělení má své vlastní obecné uživatele. Poté co se obecný uživatel přihlásí, Imprivata agent zamkne počítač a odtud se uživatel musí přihlásit pomocí ID karty a jeho pinu. Uživatel tedy pracuje na sdílené ploše, kde využívá například nemocničního informačního systému či dalších programů. U tohoto typu dochází k rychlému přehlašování uživatelů, předchozímu uživateli odhlásí a ukončí programy ve kterých pracoval, a tudíž se nemůže stát, aby se po přihlášení nový uživatel nedostal k práci předchozího uživatele. Kioskového módu se využívá hlavně na sesternách, vyšetřovnách a ambulancích, kde se sestry nebo lékaři často střídají.

U kioskového typu je možné využít i transparentní uzamčené obrazovky, která je obzvláště užitečná v situacích, kde je nutné, aby určité aplikace zůstaly viditelné a aktivní i při uzamčení počítače. Tato funkce se často využívá na JIP oddělení, kde na počítačích mají kamerový systém, který monitoruje pacienty. Díky transparentní uzamčené obrazovce může zdravotnický personál udržovat nepřetržitý dohled nad pacienty, zatímco zabezpečení systému zůstává zachováno.

Při aktivaci této funkce je možné specifikovat, která aplikace se má po uzamčení systému automaticky přesunout do popředí obrazovky. To znamená, že aplikace zůstane viditelná a funkční, zatímco ostatní části systému jsou uzamčeny a nedostupné, což přispívá k ochraně citlivých dat a informací uložených na počítači.



Obrázek 11: Ukázka obecného uživatele a přihlášeného uživatele
zdroj: (vlastní práce)

2.6 Vytvoření SSO profilů pro Windows aplikace

Imprivata OneSign umí vytvářet SSO profily, které umí zjednodušovat proces přihlašování pro koncové uživatele. Proces vytváření SSO profilu v Imprivata OneSign zahrnuje tyto kroky:

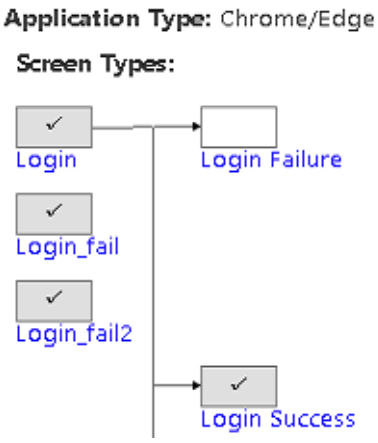
2.6.1 Identifikace aplikace

Nejprve je třeba identifikovat aplikaci, pro kterou chceme vytvořit SSO profil. To zahrnuje určení přihlašovacího mechanismu, který aplikace používá. Pro naši ukázku jsem vybral webovou aplikaci FONS FE.

Obrázek 12: Přihlašovací obrazovka FONS
zdroj: (vlastní práce)

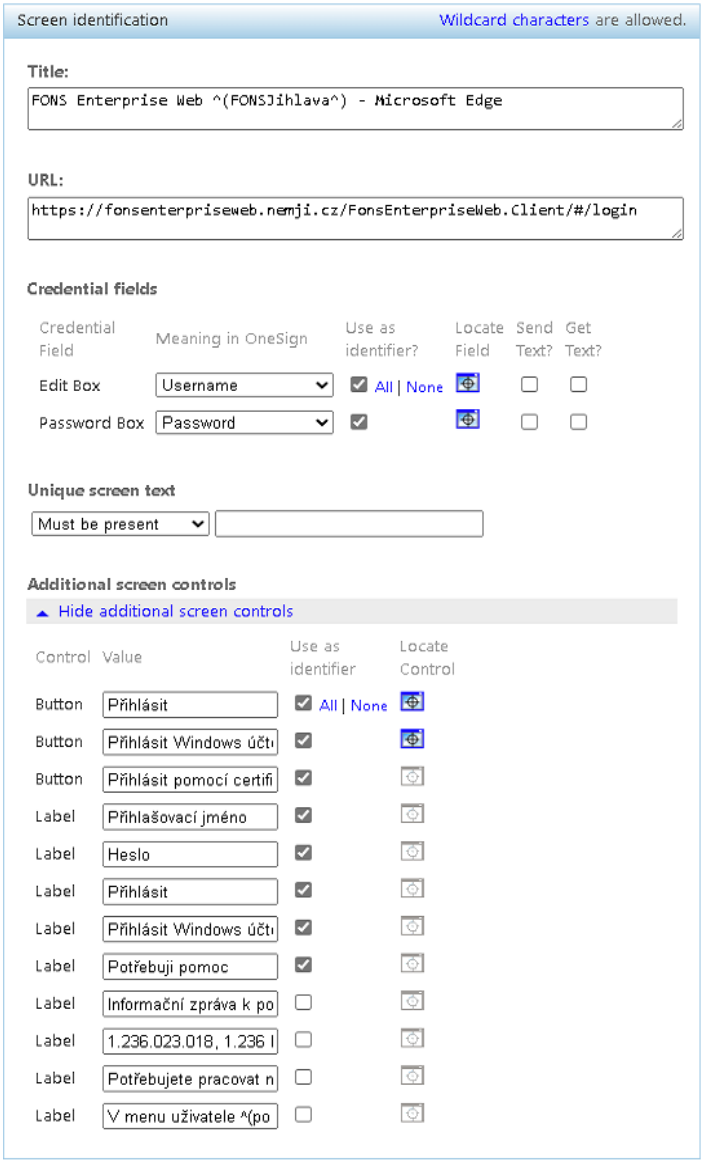
2.6.2 Zachycení přihlašovacího procesu

Pro efektivní fungování Single Sign-On (SSO) v systému Imprivata OneSign je klíčové využití speciálních sond, které jsou součástí každého Imprivata agenta. Tyto sondy jsou zásadní pro automatizaci procesů přihlašování a odhlašování, neboť umožňují systému rozpoznat specifické stavy a obrazovky různých aplikací. Sondou se nejprve musí identifikovat přihlašovací obrazovka aplikace, toto je základní krok, který umožňuje systému rozpoznat, kdy je potřeba zahájit proces SSO. Dále je potřeba identifikovat obrazovku, která se objeví po úspěšném přihlášení uživatele. Identifikace obrazovky, která se zobrazí po odhlášení, pomáhá systému detekovat, kdy byl uživatel úspěšně odhlášen z aplikace. Systém také potřebuje rozpoznat obrazovku, která se zobrazí v případě, že byly přihlašovací údaje zadány nesprávně, nebo pokud uživatelský účet vyexpiroval. Toto je důležité pro zajištění, že v případě problémů s přihlašováním bude možné situaci řádně identifikovat a řešit.



Obrázek 13: Typy obrazovek při vytváření profilu SSO

zdroj: (vlastní práce)

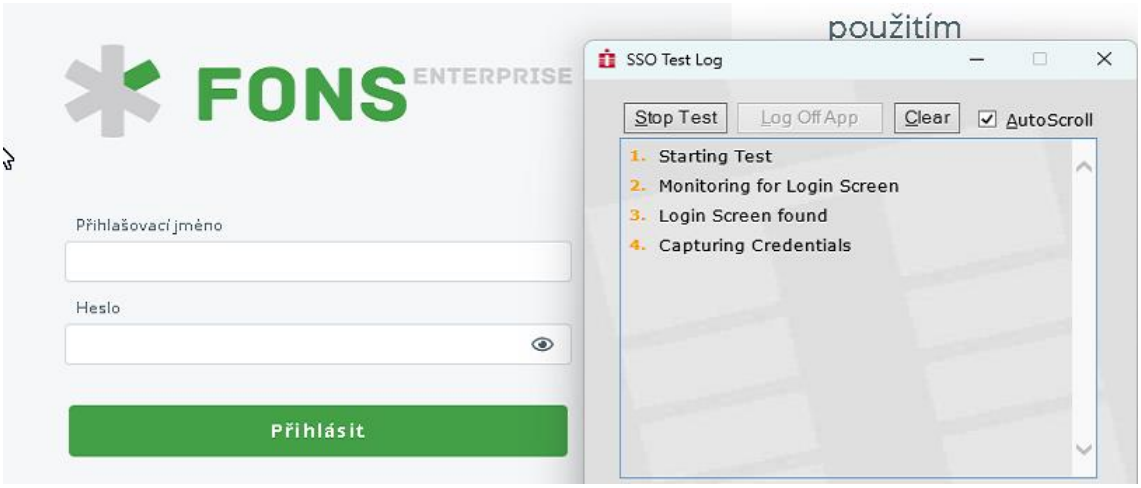


Obrázek 14: Strukturovaný přehled přihlašovací obrazovky FONS

zdroj: (vlastní práce)

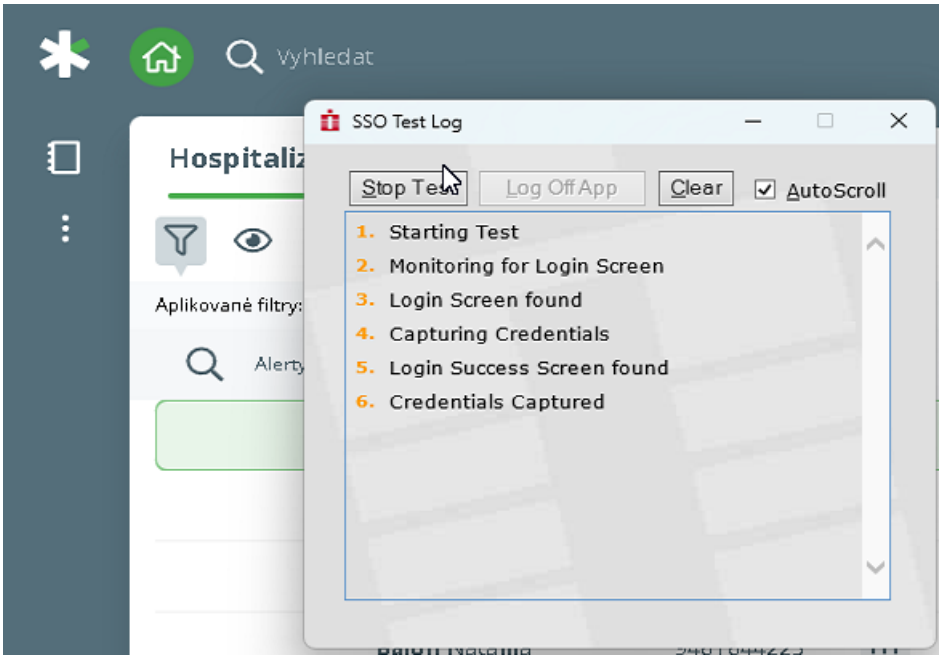
2.6.3 Testování

Při testování procesu přihlašování se používá speciální logovací software, který sleduje a zaznamenává každý krok přihlašovacího procesu. Tento nástroj umožňuje rychlou diagnostiku případných problémů. Jakmile uživatel spustí danou aplikaci, která se testuje, logovací software začne zaznamenávat každý dílčí krok. Pokud dojde k chybě nebo logovací software nerozpozná testovací aplikaci, tuto chybu zaznamená a poskytne detailnější informace.



Obrázek 15: Testování přihlašovací obrazovky

zdroj: (vlastní práce)



Obrázek 16: Úspěšné testování přihlášení

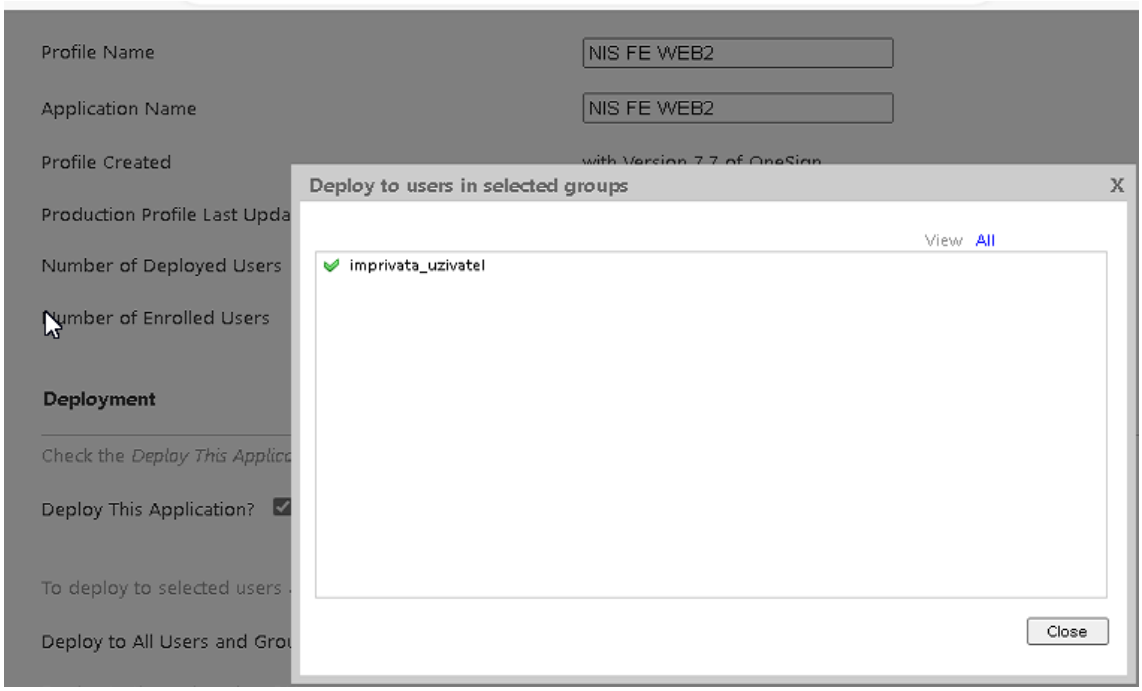
zdroj: (vlastní práce)

Z prvního obrázku je patrné, že při testování nedošlo k žádnému problému a Imprivata OneSign dokázala bez potíží rozeznat přihlašovací stránku webové aplikace a po vyplnění přihlašovacích údajů automaticky přihlásila uživatele.

Poté co Imprivata OneSign přihlásila uživatele, její logovací software rozeznal obrazovku, která se objeví po přihlášení uživatele, a tím pádem je potvrzené, že SSO je správně nakonfigurováno.

2.6.4 Nasazení profilu SSO do ostrého provozu

Pokud testování SSO profilu proběhlo úspěšně bez jakýchkoliv problémů, je možné tento profil přesunout do ostrého provozu. To znamená, že se profil stane aktivním a použitelným pro reálné přihlašovací operace v rámci organizace. V této fázi je důležité rozhodnout, jak široce bude profil nasazen. Můžeme nasadit profil pro všechny uživatele, pokud všichni mají přístup k dané aplikaci nebo použití profilu můžeme omezit na určité skupiny uživatelů.



Obrázek 17: Ukázka skupiny uživatelů

zdroj: (vlastní práce)

2.6.5 Využití funkce ISX RunAs

Funkce ISXrunAs v systému Imprivata OneSign přináší řešení pro specifickou situaci, kdy desktopová aplikace nepoužívá tradiční přihlašovací obrazovku pro zadání uživatelského jména a hesla, ale místo toho se spoléhá na ověření identity prostřednictvím Windows přihlašovacích údajů. Tato funkce je obzvláště užitečná v prostředích, kde se počítač sdílí mezi více uživateli, například u kiosků nebo sdílených pracovních stanic, kde může být počítač přihlášen pod obecným uživatelským účtem (Typ 2).

Využití ISXrunAs umožňuje, aby se aplikace spustila pod účtem uživatele, který se ověřil pomocí své ID karty nebo RFID pásku, a to i v situacích, kdy je počítač přihlášen pod obecným účtem. To eliminuje potřebu pro uživatele spouštět aplikaci jako jiný uživatel a manuálně zadávat svoje přihlašovací údaje, což by jinak vedlo k zpomalení pracovního procesu.

Pro použití této funkce je nutné upravit zástupce aplikace tím, že do pole cíl zástupce se před cestu ke spouštěné aplikaci vloží cesta k ISXRunAs.exe nástroji, který je součástí instalace Imprivata OneSign Agenta.

```
"C:\Program Files (x86)\Imprivata\OneSign Agent\ISXRunAs.exe" /profile "C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe"" https://fonsenterpriseweb.nemji.cz/FonsEnterpriseWeb.Client/#/login
```

Obrázek 18: Ukázka funkce ISXrunAS

zdroj: (vlastní práce)

Tato úprava zajistí, že při spuštění aplikace pomocí zástupce bude aplikace spuštěna pod identitou uživatele, který se ověřil na začátku pracovního sezení.

2.7 Vytvoření SSO v android zařízení

Proces vytváření SSO profilů pro Android zařízení v rámci systému Imprivata OneSign se liší od procesu pro aplikace na Windows. Imprivata OneSign nabízí podporu pro jednotné přihlašování nejen k nativním android aplikacím, ale také k webovým aplikacím. K dispozici jsou předem vytvořené SSO profily pro řadu aplikací od Microsoftu, jako jsou Microsoft Teams, Microsoft Outlook a různé aplikace z balíku Office, což usnadňuje integraci a nasazení v organizacích. Kromě toho Imprivata poskytuje před konfigurované SSO profily pro některé webové aplikace běžně využívané v americkém zdravotnictví.

2.7.1 Vytvoření SSO pro aplikace instalované do android zařízení

Pro specifické aplikace instalované do android zařízení, které vyžadují individualizované nastavení SSO profilu, je postup následující:

- **Získání APK Souboru**: Nejprve je potřeba získat APK soubor od dodavatele aplikace, kterou chcete integrovat do systému SSO.
- **Analýza v Android Studio**: APK soubor je následně otevřen v integrovaném vývojovém prostředí (IDE) Android Studio pomocí funkce "Profile or Debug APK". Tento krok umožňuje zobrazit zdrojový kód aplikace.
- **Identifikace Přihlašovací Obrazovky**: Hlavním úkolem je v zdrojovém kódu aplikace najít přihlašovací obrazovku a identifikovat názvy políček, do kterých se vyplňují přihlašovací jméno a heslo.
- **Vytvoření SSO Profilu**: S informacemi o přihlašovacích políčkách je možné vytvořit SSO profil, který automaticky vyplní přihlašovací údaje a umožní uživatelům rychle a bezpečně se přihlásit k aplikaci.

```
<app appType="0" desc="Fons" logoutMethod="1" nm="CZ.STAPRO.FONSSMART.ENTERPRISE" profileType="2">
  <env nm="Android" type="100">
    <scn auto="1" dgs="1" nm="">
      <ctl nm="username" var="USR"/>
      <ctl nm="password" var="PWD"/>
      <ctl nm="" var="PIN"/>
      <ctl nm="nem1.nemji.cz" var="DOM"/>
    </scn>
  </env>
</app>
```

Obrázek 19: Ukázka kódu při vytváření SSO pro android aplikaci

zdroj: (vlastní práce)

Tento kód představuje příklad konfiguračního souboru pro SSO profil aplikace v systému Imprivata OneSign pro Android zařízení. Z kódu je patrné, jak je SSO profil strukturován a jaké klíčové prvky obsahuje pro automatizaci přihlašovacího procesu.

- **<app appType="0" desc="Fons" logoutMethod="1" nm="CZ.STAPRO.FONSSMART.ENTERPRISE" profileType="2">:** Tento řádek definuje základní atributy aplikace, včetně typu aplikace (**appType**), popisu (**desc**), metody odhlášení (**logoutMethod**), unikátního názvu balíčku aplikace (**nm**) a typu profilu (**profileType**).
- **<env nm="Android" type="100">**: Specifikuje prostředí, pro které je profil určen, tomto případě pro Android zařízení.
- **<scn auto="1" dgs="1" nm="">**: Definuje scénář přihlašovací obrazovky, kde **auto** značí automatické vyplnění přihlašovacích údajů a **dgs** digitální signaturu obrazovky.
- **<ctl nm="username" var="USR"/>**: Určuje kontrolní prvek pro uživatelské jméno, kde **nm** je název políčka a **var** proměnná použitá pro uložení hodnoty uživatelského jména.
- **<ctl nm="password" var="PWD"/>**: Definuje kontrolní prvek pro heslo s podobnou strukturou jako uživatelské jméno.
- **<ctl nm="" var="PIN"/>**: Může reprezentovat další pole pro zadání PINu, pokud je to vyžadováno aplikací.
- **<ctl nm="nem1.nemji.cz" var="DOM"/>**: Specifikuje další kontrolní prvek, možná pro doménu nebo jiný identifikační údaj, v závislosti na specifikách aplikace.

2.7.1 Vytvoření SSO pro webové aplikace používané v android zařízení

Pro vytvoření SSO profilu pro webovou aplikaci určenou pro použití na Android zařízeních s využitím Imprivata OneSign je proces podobný, ale zaměřený na webové technologie.

- **Otevření Webové Aplikace**: Na Android zařízení otevřete webový prohlížeč a přejděte na přihlašovací stránku webové aplikace, pro kterou chcete vytvořit SSO profil.
- **Zobrazení Zdrojového Kódu**: Většina webových prohlížečů umožňuje zobrazit zdrojový kód stránky, což může být obvykle nalezeno v menu pro vývojáře nebo kliknutím pravým tlačítkem myši na stránku a výběrem možnosti "Zobrazit zdrojový kód" či podobného příkazu.
- **Identifikace Políček pro Přihlašování**: V zdrojovém kódu hledejte políčka určená pro zadávání uživatelského jména a hesla. Typicky jsou tyto prvky identifikovány pomocí atributů jako **name** nebo **id**.

- **Vytvoření SSO Profilu v Imprivata OneSign**: Při vytváření nebo úpravě SSO profilu pro danou webovou aplikaci v administrátorské konzoli Imprivata OneSign se zadá URL adresa webu a identifikované názvy nebo identifikátory políček pro uživatelské jméno a heslo. Tím se zajistí, že při přístupu k webové aplikaci bude Imprivata OneSign automaticky vyplňovat přihlašovací údaje.

```
<app appType="1" desc="FONS WEB" logoutMethod="0" nm="https://fonsenterpriseweb.nemji.cz/FonsEnterpriseWeb.MobileClient" profileType="2">
  <env nm="Android" type="100">
    <scn auto="1" dgs="1" nm="">
      <ctl nm="user-name" var="USR"/>
      <ctl nm="password" var="PWD"/>
    </scn>
  </env>
</app>
```

Obrázek 20: Ukázka kódu při vytvoření SSO pro webové aplikace používané v Android zařízení

zdroj: (vlastní práce)

Nasazení (deploy) SSO profilů pro Android zařízení v rámci systému Imprivata OneSign probíhá obdobným způsobem jako u aplikací pro Windows. Administrátoři mají možnost určit, jak široce bude profil dostupný a kdo bude moci daný SSO profil využívat.

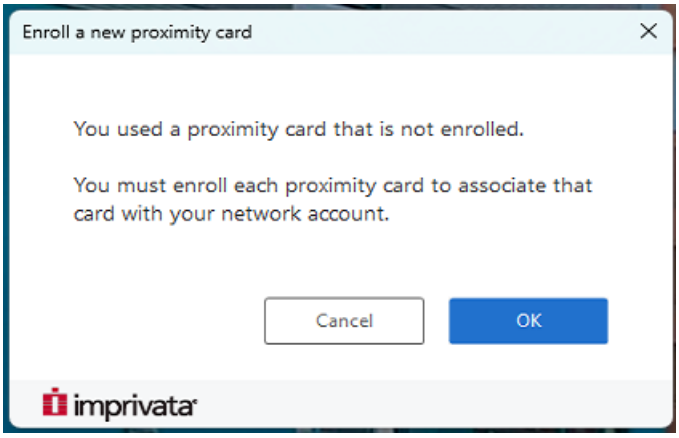
2.8 Enrollment ID karet a RFID pásků

Proces registrace uživatele neboli propojení uživatelského účtu s identifikační kartou nebo RFID páskem, v systému Imprivata probíhá v několika jednoduchých krocích, které zajišťují bezpečné a efektivní ověření identity uživatele.

Nově nastupující pracovníci prochází vstupním školením, kde si každý nastaví nové heslo pro svůj doménový účet. Poté si zaenrolují kartu ke svému účtu.

2.8.1 Přiložení identifikační karty nebo RFID pásku

Uživatel nejprve přiloží svou identifikační kartu nebo RFID pásek k čtečce. Tato čtečka musí být připojena k počítači, na kterém je instalován software Imprivata.

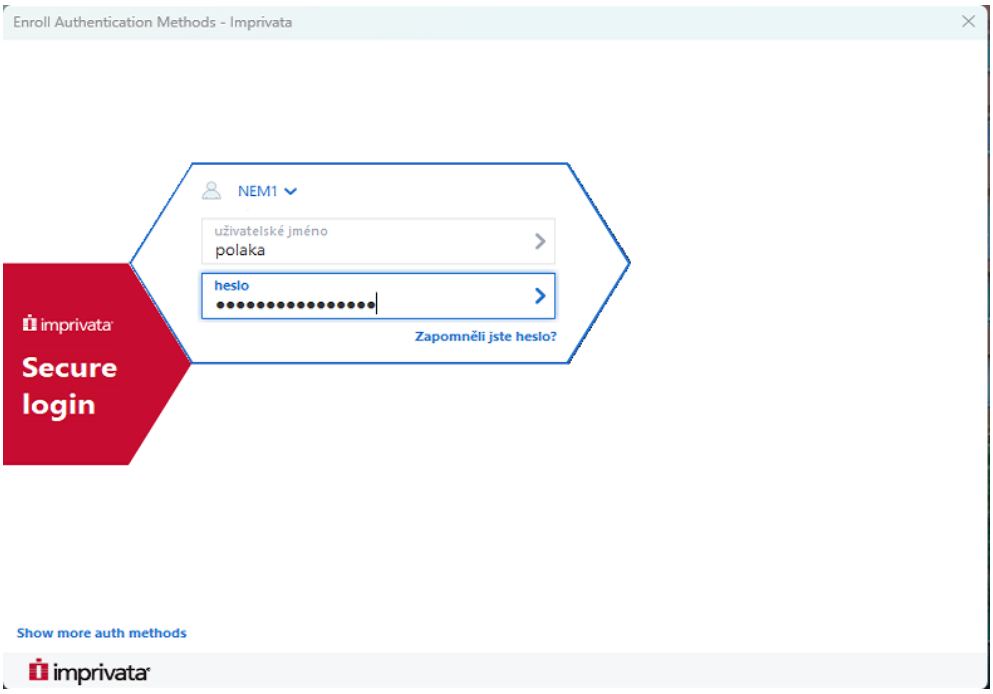


Obrázek 21: Vyskakovací okno po přiložení nenastavené karty

zdroj: (vlastní práce)

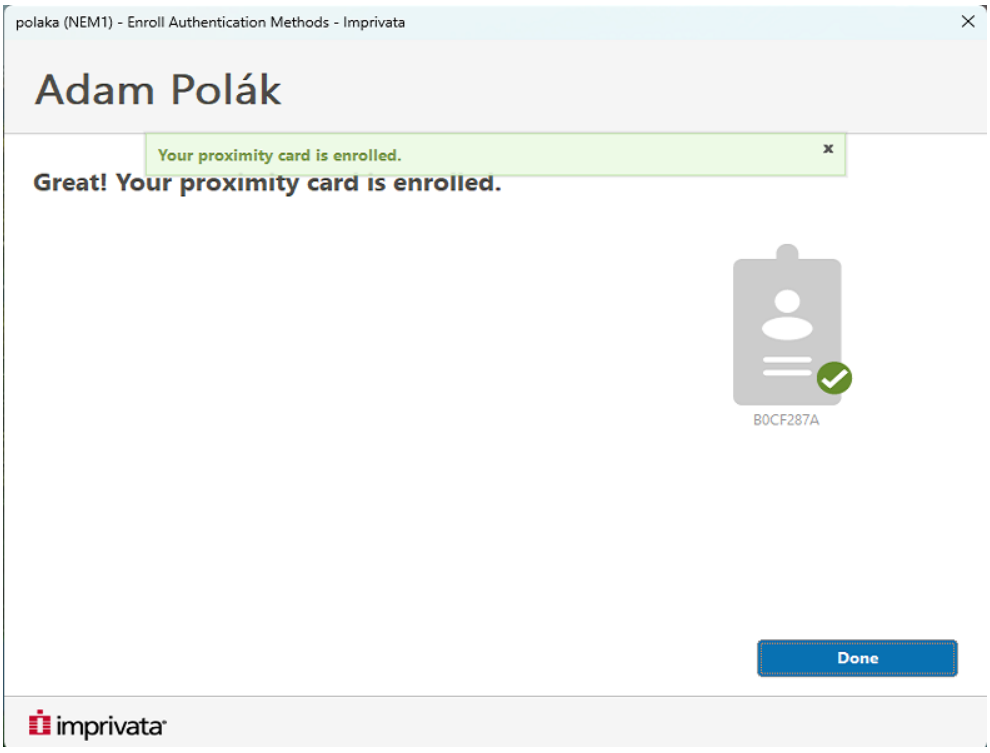
2.8.2 Zadání přihlašovacích údajů

Následně je uživatel vyzván, aby zadal své přihlašovací údaje do domény. Tento krok zabezpečuje, že propojení identifikačního prostředku s uživatelským účtem probíhá autorizovaně.



Obrázek 22: Přihlašovací okno pro nastavení karty

zdroj: (vlastní práce)

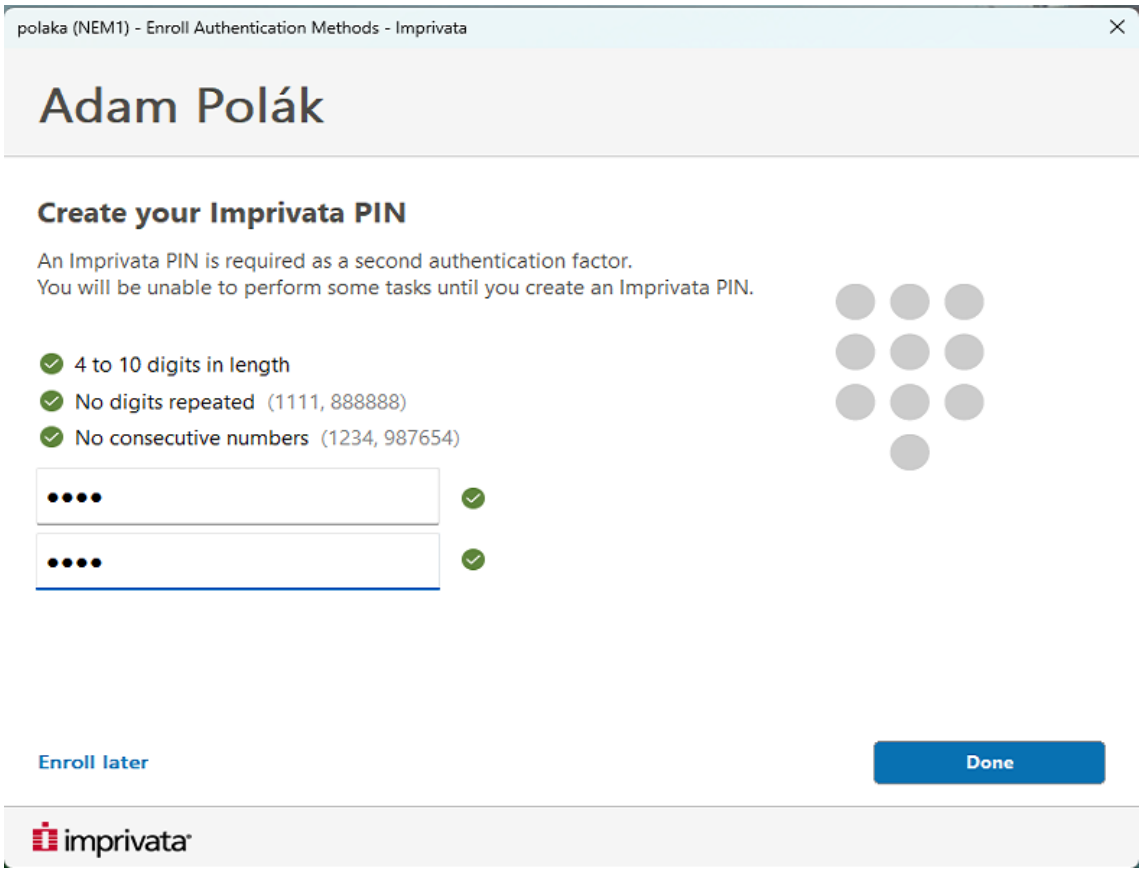


Obrázek 23: Úspěšné přiřazení karty k uživateli

zdroj: (vlastní práce)

2.8.3 Vytvoření PINu

Po úspěšném zadání přihlašovacích údajů je uživatel požádán o vytvoření číselného PINu. Tento PIN bude následně vyžadován při každém přihlášení prostřednictvím identifikační karty nebo RFID pásku.



Obrázek 24: Nastavení PINu pro ověření kartou

zdroj: (vlastní práce)

Tento postup umožňuje rychlé a bezpečné přihlášení do systémů a aplikací bez nutnosti opakovaného zadávání složitých přihlašovacích údajů. Použití identifikační karty nebo RFID pásku spolu s PINem poskytuje dvojí ověření identity, což zvyšuje bezpečnost přístupu k citlivým informacím a systémům.

Závěr

Cílem této bakalářské práce byl popis implementace a popis systému Imprivata OneSign v Nemocnici Jihlava.

Cíle se podařilo splnit a nasadit řešení do prostředí o 1 100 počítačů a 1 750 zaměstnancích.

Implementace Imprivata OneSign v zdravotnickém prostředí přináší řadu významných výhod, které se dotýkají nejen zabezpečení citlivých dat, ale i celkové efektivity a plynulosti pracovních postupů zdravotníků. Tato technologie jednotného přihlašování (SSO) a vícefaktorového ověřování (MFA) posiluje ochranu pacientských informací před neoprávněným přístupem, zároveň však zjednodušuje a zrychluje proces přihlašování pro zdravotnický personál.

Díky Imprivata OneSign se zdravotníci nemusí zabývat zdlouhavým a opakovaným přihlašováním do různých systémů a aplikací. Tím se výrazně snižuje čas strávený administrativou, což zdravotníkům umožňuje věnovat více pozornosti a času péči o pacienty. Zjednodušení pracovních postupů díky rychlému a bezpečnému přihlašování představuje klíčový krok k zefektivnění každodenní práce v nemocnicích a jiných zdravotnických zařízeních.

Imprivata OneSign je navíc flexibilní řešení, které efektivně pracuje i s aplikacemi, jež využívají lokální uživatelské účty, což dále rozšiřuje jeho použitelnost a přínosy v rámci zdravotnického prostředí. Integrace s různými typy aplikací a systémů znamená, že zdravotníci mohou s menším úsilím a bezpečně přistupovat k širokému spektru nástrojů potřebných pro svou práci.

Implementace a správa systému Imprivata OneSign je navíc navržena tak, aby byla co nejjednodušší a nejintuitivnější. To umožňuje IT oddělením rychle a efektivně zavádět a spravovat tento systém, minimalizuje potřebu technické podpory a zvyšuje celkovou spokojenost uživatelů s IT infrastrukturou. Tím se zjednodušuje nejen samotné přihlašování, ale i správa přihlašovacích a bezpečnostních politik v rámci organizace.

Ve výsledku implementace Imprivata OneSign v nemocnicích, jako je Nemocnice Jihlava, představuje zásadní posun směrem k modernímu a pacientem-centrovanému zdravotnickému prostředí, kde zvýšení bezpečnosti a efektivita pracovních postupů jdou ruku v ruce s poskytováním kvalitní péče.

Seznam použité literatury

Co je jednotné přihlašování ve službě Microsoft Entra ID? *Microsoft Learn* [online]. 2023 [cit. 2023-12-28]. Dostupné z: https://learn.microsoft.com/cs-cz/entra/identity/enterprise-apps/what-is-single-sign-on

Co je SSO (Single-Sign-On)? *AWS Amazon* [online]. 2023 [cit. 2023-12-28]. Dostupné z: https://aws.amazon.com/what-is/sso/

Co je: Vícefaktorové ověřování. *Microsoft* [online]. 2021 [cit. 2023-12-28]. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-v%C3%ADcefaktorov%C3%A9-ov%C4%9B%C5%99ov%C3%A1n%C3%AD-e5e39437-121c-be60-d123-eda06bddf661

Imprivata OneSign Single Sign-On [online]. 2017, 1-4 [cit. 2023-12-27]. Dostupné z: https://www.imprivata.com/sites/default/files/resource-files/OS-DS-SSO-GCS-0916.pdf

KEYSHIELD SSO. *Co je to KeyShield SSO?* [online]. [cit. 2023-11-18]. Dostupné z: https://www.keyshieldsso.com/about/

MALIK, Zain. Eight Benefits of Multi-Factor Authentication (MFA). *Ping Identity* [online]. 2021 [cit. 2023-12-28]. Dostupné z: https://www.pingidentity.com/en/resources/blog/post/eight-benefits-mfa.html

Nemocniční přihlašovací systém. *TDP* [online]. 2023 [cit. 2023-12-28]. Dostupné z: http://www.tdp.cz/keyshield-let%C3%A1k-9

Proč je SSO důležité? *One login* [online]. 2023 [cit. 2023-12-28]. Dostupné z: https://www.onelogin.com/learn/why-sso-important

SSO (jednotné přihlášení). *Ciberseguridad Comillas* [online]. 2023 [cit. 2023-12-28]. Dostupné z: https://ciberseguridad.comillas.edu/sso-single-sign-on/

Výroční zpráva 2017 [online]. 2017, 1-70 [cit. 2023-12-27]. Dostupné z: https://www.nemji.cz/assets/File.ashx?id_org=427000&id_dokumenty=8854

Výroční zpráva 2022 [online]. 2022, 1-84 [cit. 2023-12-27]. Dostupné z: https://www.nemji.cz/assets/File.ashx?id_org=427000&id_dokumenty=11504