FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání diplomové práce

Název:	Integrace digitálních dokladů totožnosti do procesu ověření identity zákazníků.
Student:	Bc. Viktoriia Havrylenko
Vedoucí:	Ing. Pavel Náplava, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Manažerská informatika
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	do konce letního semestru 2024/2025

Pokyny pro vypracování

Analyzujte a vyhodnoťte možnosti implementace zpracování digitálních dokladů totožnosti podle standardu Doc 9303 ICAO do vybraných procesů konkrétního dodavatele (bude definován vedoucím práce):
1) Popište proces ověření identity v kontextu onsite a remote onboardingu zákazníků. Analyzujte předpisy, existující v rámci EU a České republiky, související s tímto procesem.
2) Seznamte se s nástroji pro podporu onboardingového procesu od vybraného externího dodavatele. V rámci možností proveďte analýzu konkurence v této oblasti.
3) Analyzujte standard Doc 9303 společnosti ICAO a související technické prostředky. Zhodnoťte možnosti integrace zpracování digitálních dokladů totožnosti do v současné době dodávaného řešení (viz bod 2).
4) Na základě provedené analýzy vytvořte business case, který poslouží jako podklad pro rozhodování vedení společnosti o přínosech rozšíření aplikace.
5) Připravte prototyp a sadu testovacích scénářů, navazujících na návrh změn v bodu 3, jako doplněk vypracovaného business casu.

Elektronicky schválil/a Ing. David Buchtela, Ph.D. dne 7. února 2024 v Praze.

Diplomová práce

INTEGRACE DIGITÁLNÍCH DOKLADŮ TOTOŽNOSTI DO PROCESU OVĚŘENÍ IDENTITY ZÁKAZNÍKŮ

Bc. Viktoriia Havrylenko

Fakulta informačních technologií
Katedra teoretické informatiky
Vedoucí: Ing. Pavel Náplava, Ph.D.
7. května 2024

Obsah

Seznam obrázků

Seznam tabulek

Chtěla bych vyjádřit své hluboké poděkování vedoucímu práce, Ing. Pavlu Náplavovi, Ph.D., za jeho odborné vedení, cenné rady a neustálou podporu během rozvoje této diplomové práci. Dále bych ráda poděkovala týmu Trask ZenID a společnosti Trask Solutions a.s. za možnost pracovat na tomto zajímavém projektu. Jejich ochota sdílet odborné znalosti a poskytnout praktické rady byla neocenitelná a významně přispěla k úspěšnému dokončení mé práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 7. května 2024

Abstrakt

Tato diplomová práce se věnuje rozšíření systému Trask ZenID, produktu společnosti Trask Solutions a.s pro automatizované ověřování identity zákazníků na dálku, o zpracování digitálních dokladů totožnosti. Cílem bylo ověřit vhodnost této integrace prostřednictvím analýzy splnění požadavků Evropského orgánu pro bankovnictví (EBA) a technických specifikací ICAO 9303. Práce zahrnuje vytvoření business case s finanční analýzou, která potvrdila finanční proveditelnost projektu. Dále byl vyvinut a otestován prototyp DEMO aplikace, což podpořilo další implementaci. Výsledky ukázaly, že integrace digitálních dokladů může významně přispět k efektivitě a bezpečnosti ověřovacích procesů v Trask ZenID. Práce představuje důležitý příspěvek k rozvoji bezpečnostních a identifikačních procesů na dálku.

Klíčová slova Trask ZenID, automatizované ověřování totožnosti, vzdálená identifikace, digitální doklady totožnosti, NFC technologie, bezkontaktní čipy, ICAO 9303, bezpečnostní prvky na dokladech, business case, mapování procesů, BPMN, tvorba prototypu.

Abstract

This thesis explores the extension of the Trask ZenID system, a product created by Trask Solutions a.s for automated remote customer identity verification, to include the processing of digital identity documents. The goal was to verify the appropriateness of this integration through an analysis of compliance with European Banking Authority (EBA) requirements and ICAO 9303 technical specifications. The work includes the creation of a business case with financial analysis, confirming the financial viability of the project. Furthermore, a DEMO application prototype was developed and tested, supporting further implementation. Results indicated that the integration of digital documents can significantly enhance the efficiency and security of verification processes in Trask ZenID. This thesis represents an important contribution to the development of secure and remote identification processes.

Keywords Trask ZenID, automated identity proofing, remote identification, digital identity documents, NFC technology, contactless chips, ICAO 9303, document security features, business case, process mapping, BPMN, prototype development.

Seznam zkratek

Zkratka	Význam (CZ)	Význam (EN)
AA	Aktivní ověření	Active Authentication
AD	Aktivní adresář	Active Directory
ADD	Karta adres	Address Card
AID	Identifikátor aplikace	Application Identifier
API	Programovací rozhraní aplikace	Application Programming Interface
ATR	Odpověď na reset	Answer To Reset
BAC	Základní kontrola přístupu	Basic Access Control
BIRTH	Rodný list	Birth Certificate
BPMN	Notace pro modelování a mapování procesů	Business Process Model and Notation
CAN	Číslo pro přístup k čipu	Card Access Number
CFT	Boj proti financování terorismu	Combating the Financing of Terrorism
CSCA	Certifikační autorita pro podepisování zemí	Country Signing Certification Authority
CSC	Státní podepisovací certifikát	Country Signing Certificate
CZK	Česká koruna	Czech Crown
ČNB	Česká národní banka	Czech National Bank
DG	Skupina dat	Data Group
DL	Řidičský průkaz	Driving Licence
DPI	Tečky na palec	Dots Per Inch
DSC	Certifikát podepisujícího dokumentu	Document Signer Certificate
EAC	Rozšířená kontrola přístupu	Extended Access Control
E2E	Od konce ke konci	End-to-End
EBA	Evropský orgán pro bankovnictví	European Banking Authority
eIDAS	Elektronická identifikace, autentizace a důvěryhodné služby	Electronic Identification, Authentication and trust Services
eMRTD	Elektronický strojově čitelný cestovní doklad	Electronic Machine Readable Travel Document
eMROTD	Elektronický strojově čitelný oficiální cestovní doklad	Electronic Machine Readable Official Travel Document
eMRP	Elektronický strojově čitelný pas	Electronic Machine Readable Passport
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost	European Union Agency for Cybersecurity
EU	Evropská unie	European Union

Pokračuje na další straně

– pokračování z předchozí stránky		
Zkratka	**Význam (CZ)**	**Význam (EN)**
FAÚ	Finanční analytický úřad	Financial Analytical Office
GDPR	Obecné nařízení o ochraně osobních údajů	General Data Protection Regulation
GUN	Zbrojní průkaz	Gun Permit
GUI	Grafické uživatelské rozhraní	Graphical User Interface
IC	Integrovaný obvod	Integrated Circuit
ICAO	Mezinárodní organizace pro civilní letectví	International Civil Aviation Organization
ID	Doklad totožnosti	Identity document
IČ	Identifikační číslo	Identification Number
ISO	Mezinárodní organizace pro normalizaci	International Standards Organization
KYC	Poznej svého zákazníka	Know Your Customer
LDS	Logická datová struktura	Logical Data Structure
LoA	Úroveň záruky	Level of Assurance
ML	Strojové učení	Machine Learning
MRZ	Strojově čitelná zóna	Machine Readable Zone
NFC	Bezkontaktní komunikace blízkého pole	Near Field Communication
NPV	Čistá současná hodnota	Net Present Value
OCR	Optické rozpoznávání znaků	Optical Character Recognition
ONPREM	Na místě	On-Premises
PACE	Navázání připojení ověřené heslem	Password Authenticated Connection Establishment
PA	Pasivní ověřování	Passive Authentication
PAS	Pas	Passport
PDF	Přenosný formát dokumentů	Portable Document Format
PKD	Veřejný klíčový adresář	Public Key Directory
PRADO	Veřejný rejstřík pravých dokladů totožnosti a cestovních dokladů online	Public Register of Authentic identity and travel Documents Online
RES	Povolení k pobytu	Residence Permit
RFID	Identifikace pomocí rádiové frekvence	Radio Frequency Identification
RQx	Požadavek	Requirement
SaaS	Software jako služba	Software as a Service
SDK	Vývojářský balíček softwaru	Software Development Kit
SLA	Dohoda o úrovni služeb	Service Level Agreement
SOD	Data bezpečnostních objektů	Security Object Data
TC	Testovací scénář	Test Case
TD	Cestovní doklad	Travel Document
TSP	Důvěryhodný poskytovatel služeb	Trusted Service Provider
UV	Ultrafialové	Ultraviolet
UX/UI	Uživatelská zkušenost / Uživatelské rozhraní	User Experience / User Interface
VISA	Vízum	Visa
Pokračuje na další straně		

		– pokračování z předchozí stránky
Zkratka	**Význam (CZ)**	**Význam (EN)**
WBS	Struktura rozkladu práce	Work Breakdown Structure

Kapitola 1
Úvod

V dnešní digitálně propojené společnosti, kde se bezpečnost identifikace stává stále významnějším tématem, je nezbytné věnovat zvýšenou pozornost regulacím, procesům a potenciálním rizikům. Trask ZenID, řešení pro automatizaci identifikace zákazníků, čelí tímto problémům po dobu šesti let. Tento projekt, vedený společností Trask Solutions a.s, představuje komplexní řešení pro identifikaci, které se zaměřuje na zlepšení bezpečnosti a efektivity identifikačních procesů. Toto řešení integruje pokročilé technologie a nabízí uživatelům snadný a rychlý způsob, jak ověřovat svou identitu v digitálním prostředí. Díky své flexibilitě a škálovatelnosti je Trask ZenID ideální pro použití v nejrůznějších odvětvích, od finančních služeb po telekomunikace a veřejnou správu.

V rámci stávajícího rozvoje vedení Trask ZenID plánuje rozšíření služeb produktu. Konkrétně se uvažuje o integraci zpracování a validace elektronických záznamů uložených na čipech digitálních dokladů totožnosti. Tento krok je motivován především potřebou adaptace na rostoucí rozvoj umělé inteligence, která přinesla nové výzvy v oblasti bezpečnosti podobných systémů. Tato integrace by měla nejenom zlepšit uživatelský zážitek, ale prioritně zvýšit bezpečnost a udržet konkurenceschopnost na trhu. S cílem ověřit a potvrdit vhodnost této strategie byla zadána tato diplomová práce. Jejím úkolem je nejen analyzovat správnost zvoleného směru, zvážit potenciální přínosy a rizika spojená s integrací digitálních dokladů, ale také připravit podklady pro budoucí implementaci.

Pro zajištění úspěšné realizace této iniciativy byly definovány následující kroky:

- **Analýza procesu ověřovaní identity:** vysvětlení základních principů procesu identifikace. Seznámení s právními předpisy a regulacemi pro online identifikaci ve vybraných jurisdikcích (EU a ČR). Analýza toho, jak Trask ZenID plní stanovené požadavky na proces identifikace za účelem posouzení vhodnosti integrace digitálních dokladů do stávajících procesů.
- **Seznámení s Trask ZenID:** detailní představení řešení Trask ZenID, jeho komponent a přístupů k realizaci identifikačních procesů. Hodnocení funkcí a bezpečnostních metod ve srovnání s konkurenčními řešeními na trhu. Ověření integrace bezpečnostních prvků na dokladech totožnosti v systému Trask ZenID.
- **Příprava business case:** vypracování projektového plánu pro zvolenou integraci, který specifikuje cíle, časový rámec a etapy implementace. Součástí je také posouzení proveditelnosti a finanční analýza celého projektu. Hlavním cílem je spočítat návratnost investic pro získání podpory od vedení společnosti.
- **Funkční specifikace:** analýza standardů spojených s procesem extrakce a validace dat z digitálních dokladů totožnosti. Budou definovány požadavky na systém a připraveny podklady pro jeho následné rozšíření.

Kapitola 2

Analýza procesu ověřování identity

Tato kapitola se zaměřuje na důkladnou analýzu procesu ověřování identity, který se zkoumá v různých kontextech a případech užití. Zvláštní pozornost je věnována roli klíčových účastníků procesu, jako jsou uživatelé, jejichž identita se ověřuje, ověřovatelé, a regulační orgány, které stanovují pravidla ověřování. Kapitola dále popisuje význam identity a jejích atributů, včetně biometrických dat a oficiálních dokumentů, a analyzuje klíčové fáze procesu. Tato kapitola nejen popisuje teoretické základy procesu, ale také poskytuje náhled do praktické implementace a výzev spojených s digitálním ověřováním identity v souladu s aktuálními technologickými a legislativními standardy.

2.1 Definice procesu ověřování identity

Ověřování identity představuje klíčový prvek v digitálním světě, kde se osobní a finanční transakce stále častěji přesouvají do online prostoru. Jeho význam dramaticky narůstá v kontextu rostoucí kybernetické kriminality, kde identifikační údaje jednotlivců a organizací jsou častým cílem útoků. Správné ověřování identity pomáhá chránit nejen finanční aktiva, ale také osobní údaje. S přísnějšími regulacemi v Evropské unii se stává důkladné a spolehlivé ověřování identity nejen dobrým bezpečnostním opatřením, ale i právní nezbytností. Tyto regulace zdůrazňují potřebu ochrany osobních údajů a dávají jednotlivcům větší kontrolu nad tím, jak jsou jejich údaje používány a sdíleny. Ověřování identity (nebo také identifikace) je obecně proces, při kterém subjekt ověřování, ať už fyzická osoba nebo právnická entita, musí prokázat poskytnutím jednoznačných důkazů, že se skutečně jedná o jeho osobu a nesnaží se napodobit někoho jiného a ukrást jeho identitu [1]. Procesem ověřování identity jsou obvykle chráněny produkty, které mohou obsahovat citlivá data a/nebo služby, které mohou být přístupné pouze těm uživatelům, kteří jsou jednoznačně identifikováni v rámci systému. Tento proces může existovat v rámci systému jako samostatná komponenta, nebo být podpořen dalšími procesy, aby poskytl souvislý a plnohodnotný zážitek uživatelům, odpovídající požadavkům společnosti.

2.1.1 Účastníci procesu ověřování identity

Proces ověřování totožnosti zahrnuje několik klíčových účastníků, jejichž role a úkoly se liší v závislosti na kontextu a konkrétních požadavcích na ověření. Obecně lze rozlišit tři hlavní aktéry:

- **Uživatelé a subjekty, jejichž identita se ověřuje**: tyto subjekty poskytují potřebné

osobní a případně biometrické údaje, které jsou využité pro ověřování jejich totožnosti [2]. V procesu ověřování identity může být subjektem jak fyzická, tak právnická osoba. Fyzické osoby jsou konkrétní osoby, jejichž zapojení do transakcí vyžaduje potvrzení jejich totožnosti. Právnická osoba se od fyzické liší tím, že je vytvořená právními předpisy a může jednat na trhu samostatně, například ve formě společností nebo organizací. Právnické osoby musí být také schopny ověřit svou identitu, obzvlášť při uzavírání smluv, finančních operacích nebo při právních jednáních.

- **Ověřovatel nebo poskytovatel ověřovacích služeb**: ověřovatel je zodpovědný za průběh procesu ověřování identity. Tento aktér shromažďuje poskytnuté důkazy, provádí ověření jejich platnosti, příslušnosti k subjektu identifikace. Na základě těchto kontrol ověřovatel pak buď potvrdí identitu subjektu, nebo ji zamítne. V kontextu vzdáleného ověřování identity přímo existují organizace (poskytovatele ověřovacích služeb), které implementují a spravují technologická řešení pro ověřování identity.
- **Regulační a dozorčí orgány**: tyto instituce stanovují pravidla a normy, které definují, jaké údaje je nutné ověřovat, jakým způsobem a v jakých situacích [3].

2.1.2 Význam identity a její atributů

Identitou se v tomto kontextu rozumí kolekce atributů a důkazů, které jednoznačně identifikují osobu a jsou s ní vázané. Příkladem takových atributů jsou biometrická data, doklady potvrzující totožnost, ověřené certifikáty, data extrahovaná z veřejných rejstříků, úřadů nebo státních databází [4].

Doklady totožnosti jsou oficiální dokumenty vydávané státem nebo jinými oprávněnými institucemi, které slouží k potvrzení identity jednotlivce. Tyto dokumenty obvykle obsahují identifikační údaje, jako jsou jméno, fotografie, datum narození a další biometrické informace. Mezi běžné příklady dokladů totožnosti patří občanský průkaz, cestovní pas, řidičský průkaz, a v některých případech i další vládní nebo mezinárodně uznávané identifikační karty. Právní vlastnosti a formáty dokladů totožnosti se v jednotlivých zemích liší. Konkrétní požadavky je třeba ověřovat na internetových stránkách příslušných regulačních orgánů [5].

Součástí identifikace běžně je ověření biometrických důkazů. Jsou to údaje týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují nebo potvrzují její jedinečnou identifikaci. Příklady biometrických údajů jsou otisky prstu, fotka obličeje, snímek zornic [6].

PRADO a jeho význam pro identifikační procesy

PRADO (z anglického "Public Register of Authentic Identity and Travel Documents Online") je veřejná databáze pravých identifikačních a cestovních dokladů, kterou založila Evropská unie. Jeho primárním úkolem je poskytovat ověřené informace o bezpečnostních prvcích a ochranných metodách, které jsou aplikovány na doklady vydávané členskými státy EU, některými dalšími evropskými státy a mezinárodními organizacemi. PRADO je klíčový nástroj v prevenci proti padělání a zneužívání identifikačních a cestovních dokladů [7].

PRADO poskytuje rozsáhlou databázi, která obsahuje detailní informace o různých typech dokladů, jejich bezpečnostních prvcích a ukázky autentických dokladů pro účely ověřování. Tato platforma je přístupná veřejnosti a je široce využívána nejen orgány veřejné správy, jako jsou policie, celní úřady a imigrační služby, ale také subjekty soukromého sektoru, například bankami, leteckými společnostmi a taky společnostmi, které nabízejí řešení pro vzdálenou identifikaci (včetně Trask ZenID).

V praxi může být PRADO využíván pro:

- **Ověření pravosti dokumentů:** umožňuje rychlou a efektivní kontrolu, zda se bezpečnostní prvky dokumentu shodují s oficiálními záznamy.

- **Školení a vzdělávání:** poskytuje materiály pro školení pracovníků, kteří se podílejí na procesu ověřování dokumentů.
- **Podpora v obráně proti podvodům:** slouží jako nástroj pro rozpoznávání padělaných a zneužitých dokumentů, což napomáhá v prevenci a odhalování trestné činnosti.

V této práci bude PRADO využit pro analýzu existujících bezpečnostních prvků integrovaných do dokladů totožnosti (viz sekce č. 3.8). Klíčovým aspektem této analýzy je posouzení, do jaké míry jsou tyto prvky zpracované systémem Trask ZenID a jak efektivně toto řešení dokáže detekovat a validovat tyto prvky v rámci procesů vzdálené identifikace. Zjištění poskytnutá touto analýzou jsou zásadní pro hodnocení, zda je integrace zpracování digitálních dokladů totožnosti a ověřování jejich bezpečnostních prvků vhodnou strategií pro rozšíření Trask ZenID.

2.1.3 Hlavní případy užití procesu identifikace

Proces ověřování identity hraje klíčovou roli v celé řadě situací, sahajících od digitálních aplikací až po osobní interakce, například na úřadech. Identifikace se uplatňuje v různých oblastech, včetně zdravotnictví, státní správy, sociálních sítí, hotelového průmyslu, při náboru zaměstnanců, na letištích, v bankách, v jiných finančních institucích a dalších.

V závislosti na prostředí, v němž se identifikace provádí, a na subjektu, který je za výsledek identifikace odpovědný, se rozlišuje mezi ověřováním totožnosti na dálku (z anglického ”remote identity proofing”) a na místě (z anglického ”onsight identity proofing”), což platí pro každý kontext, v němž se proces identifikace používá.

Ověřování totožnosti na místě

Při ověřování totožnosti na místě je vyžadována fyzická přítomnost obou účastníků procesu: subjektu ověřování a ověřovatele. Subjekt osobně předá ověřovateli požadované důkazy pro prokázaní své identity. Ověřovatel je posoudí a poskytne výsledek, a to i na základě viditelných příznaků. Součástí identifikace v tomto případě mohou být podpůrné softwarové nástroje, které zastřeší nějakou z identifikačních kontrol. Tento přístup přispívá ke zvětšení efektivity, spolehlivosti a prevence výskytu lidských chyb. Stále se však jedná o identifikaci na místě a odpovědnost za celkový výsledek procesu je plně v rukou ověřovatele [4].

Identifikace na dálku

Při ověřování identity na dálku je proces celkově podpořen softwarovým řešením pro elektronickou identifikaci (poskytovatelem ověřovacích služeb) a zásah fyzické osoby ověřovatele do procesu je minimalizován. Subjekt ověřování interaguje výhradně s digitální komponentou podporující proces ověřování identity, během něhož subjekt poskytne důkazy v digitálním formátu a projde automatickými kontrolami pro ověřování identity. Výsledky těchto kontrol jsou následně strojově interpretovány. Zodpovědnost za správnost výsledku je přenesená na poskytovatele ověřovacích služeb.

Obecně se definují tři hlavní případy užití, u kterých ověřování identity na dálku je legislativně podporováno [4]:

- **Vydávání kvalifikovaných certifikátů**, při kterém důvěryhodné certifikační autority vydávají digitální certifikáty, jež potvrzují identitu držitele a umožňují bezpečné elektronické transakce.
- **Prostředky elektronické identifikace**, představují digitální nástroje a služby, které podle evropské regulace eIDAS umožňují jednotlivcům a organizacím prokázat svou identitu v elektronickém prostředí.

- **Ověřování identity klientů**, ve kterém finanční instituce a jiné povinné subjekty prověřují identitu svých klientů, aby splnily požadavky proti praní špinavých peněz, zahrnující ověřování osobních údajů a dokladů totožnosti.

Hybridní proces

Pokud v průběhu ověřování identity na dálku dojde k problémům nebo nejistotám, může být vyžadován zásah fyzické osoby ověřovatele, nebo také operátora, který provede manuální kontrolu a poskytne další vstup pro možnost dokončení procesu. Konkrétním příkladem může být videokonference mezi subjektem a operátorem, který subjekt požádá o provedení úkonu k ověření jeho živosti nebo o předložení průkazu totožnosti do kamery k potvrzení, že žadatel kartu skutečně vlastní [4].

Hybridní metoda, kdy je proces podporován digitální technologií, ale konečné rozhodnutí je v rukou lidské obsluhy, přináší výhody větší flexibility a schopnosti překonat omezení čistě automatizovaných systémů a zároveň snižuje složitost a zátěž fyzických ověřovatelů.

Tato práce se zabývá především ověřováním identity klientů, kde subjektem je fyzická osoba, a to prostřednictvím vzdáleného plně automatizovaného procesu. Další oblasti byly zmíněny pro dokreslení kontextu, ale nebudou dále rozebírány.

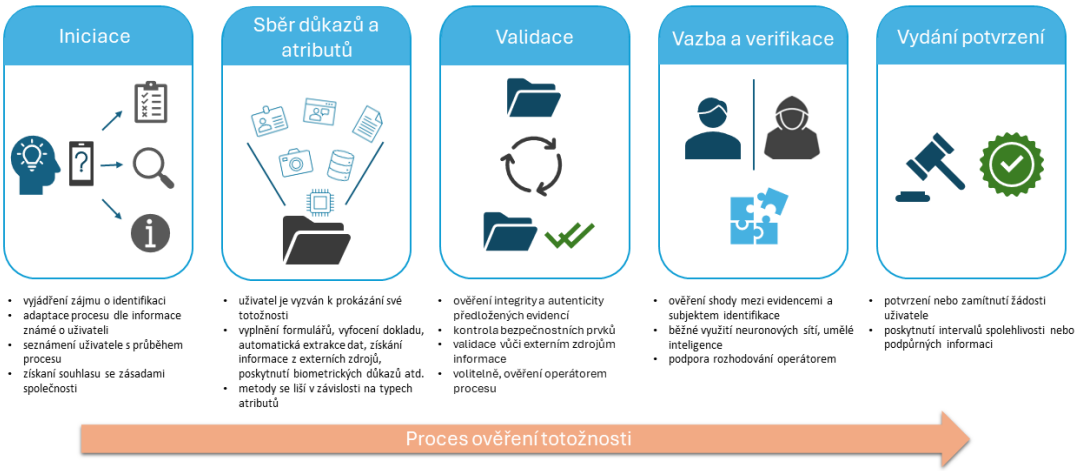
2.2 Průběh identifikace na dálku

Bez ohledu na použité prostředky a typ identifikace se každý proces ověřování identity skládá z několika klíčových fází, které jsou dobře rozlišitelné. Mezi tyto fáze patří iniciace, shromažďování důkazů a atributů, validace, vazba a ověření a vydání potvrzení identifikace.

Organizace, které chtějí implementovat ověřování identity na dálku, mohou všechny tyto fáze implementovat vlastními prostředky nebo se spolehnout na řešení třetích stran - buď pro celý proces ověřování identity, nebo pro konkrétní fáze.

V sekci č. 2.2.1 následuje podrobnější vysvětlení jednotlivých podprocesů vzdálené identifikace včetně krátkého přehledu nejběžnějších metod, které se používají k provádění jednotlivých procesů ověřování totožnosti subjektů. Celkový přehled ověřování identity na dálku a její základních podprocesů je také znázorněn na obrázku č. 2.1.[1] Popis jednotlivých částí byl vytvořen na základě reportu zveřejněného Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) na téma "Ověřování totožnosti na dálku".

[1] Obrázek byl vytvořen autorem na základě definice procesu ověřování totožnosti ve zprávě agentury ENISA [4].



Obrázek 2.1 Znázornění průběhu ověřování totožnosti uživatele

2.2.1 Iniciace

Iniciace představuje začátek procesu, kdy subjekt projeví zájem o ověření své identity. V reakci na tuto žádost si komponenta iniciace v případě potřeby vyžádá další informace o žadateli, aby mohla určit typ potřebné identifikace. Tato fáze je klíčová, protože metody ověřování se mohou lišit v závislosti na identitě žadatele. Rozdíly mohou existovat mezi občany země, kde se identifikace provádí, a cizinci. Ověřování identity cizinců vyžaduje pečlivější prověření. Naopak pro občany státu může být proces usnadněn, zejména pokud již disponují elektronickou identitou od ověřeného poskytovatele.

Na základě informací získaných o klientovi iniciační komponenta poskytne potřebné podklady pro nadcházející proces, aby žadatele řádně informovala a zajistila, že bude mít k dispozici všechny prostředky. V opačném případě může být použit alternativní proces nebo může být žádost zamítnuta. V této fázi musí uživatel rovněž souhlasit s procesem a potvrdit poskytnutí svých osobních údajů a atributů pro ověřování totožnosti, přičemž si musí být vědom podmínek jejich uchovávání.

Mezi nejčastější metody zajištění správného zahájení patří poskytování informací o procesu v digitální podobě, prezentace návodů, průvodců krok za krokem, poskytování odkazů na příslušné dokumenty týkající se podmínek služby a ochrany údajů, usnadnění souhlasu prostřednictvím formulářů, umožnění přístupu k hardwarovým prvkům zařízení (kamera, mikrofon, přístup k souborovým systémům), které jsou nezbytné pro identifikaci, stažení podpůrného softwaru, přesměrování na příslušného poskytovatele identity, generování ověřeného podpisu a další [4].

2.2.2 Sběr důkazů a atributů

Na základě dohodnutého postupu je subjekt dále vyzván k prokázání své totožnosti. Metody sběru evidencí se liší podle typu atributů, které jsou v daném kontextu povinné. Subjekty identifikace mohou být požádány o ruční vyplnění dotazníku nebo formuláře, naskenování nebo vyfocení dokladu totožnosti, který je následně podroben extrakci dat pomocí optického rozpoznávání znaků (viz více v části 3.2.2). Údaje mohou být rovněž extrahovány z elektronických

nosičů informace obsažených v dokladu (například, z kontaktních nebo bezkontaktních čipů) nebo vyžádány z příslušných databází či úřadů (externí zdroje informace). Pro zvýšení spolehlivosti ověřování mohou být dokumenty nebo jiné důkazy natočeny nebo ukázány přímo operátorovi během videokonference. V případě, že identifikace probíhá prostřednictvím jiného poskytovatele identifikačních údajů, bude uživatel požádán o přihlášení a poskytnutí souhlasu se sdílením svých osobních údajů s externí službou [4].

2.2.3 Validace

Stejně jako v případě předchozího procesu, specifika procesu validace se liší v závislosti na legislativě jednotlivých států a požadavcích kladených na typy shromažďovaných informací. Obecně je cílem této části zjistit, zda jsou předložené základní informace autentické, platné, důvěryhodné a zda nebyly padělány nebo jakýmkoli způsobem změněné útočníkem. Mezi nejčastěji používané metody ověřování patří ověřování bezpečnostních strojově ověřitelných prvků na dokladech, provádění křížových kontrol předložených dokladů, ověřování informací v externích nebo interních databázích či registrech, ověřování viditelných evidencí živosti subjektů identifikace, ověřování, zda poskytnuté doklady nejsou zneplatněné nebo zrušené, ověřování subjektů z obchodního hlediska (kontrola věku, pohlaví, státní příslušnosti). V některých případech může být přítomnost provozovatele povinná, aby byly zajištěny spolehlivé výsledky [4].

2.2.4 Vazba a verifikace

Účelem tohoto kroku je zjistit, zda shromážděné důkazy skutečně patří subjektu identifikace, a ověřit, zda se subjekt nesnaží zpochybnit něčí totožnost a zda je skutečně osobou, za kterou se vydává. Tento účel je často podporován vycvičenými neuronovými sítěmi, umělou inteligencí, které například provádějí ověření živosti uživatele pomocí pasivních nebo aktivních metod (viz vice v sekci č. 3.2.2), nebo kontrolují shodu mezi biometrickými charakteristikami obsaženými přímo na dokladu totožnosti a obrázkem získaným během identifikace. Zásah fyzického operátora v dané části je nejběžnějším postupem [4].

2.2.5 Vydání potvrzení

Na konci procesu řešení pro vzdálené ověřování totožnosti zhodnotí shromážděné důkazy a výsledky kontrol. Následně vydá buď jasnou odpověď potvrzující či zamítající žádost uživatele o identifikaci, nebo poskytne rozmezí spolehlivosti a dodatečné informace, které pomohou při rozhodování v navazujících procesech [4].

Podrobnosti procesu ověřování totožnosti a jeho dílčích částí se v jednotlivých státech a oblastech liší z důvodu nedostatečné standardizace a jednotnosti procesu. Různé metody se často kombinují a překrývají, aby poskytovaly spolehlivější a lepší výsledky. Na základě průzkumu provedeného agenturou ENISA je nejoblíbenější metodou sběru údajů od subjektu identifikace použití elektronických nosičů informace (resp. digitálních dokladů totožnosti) a ověřování pomocí biometrických údajů. Tyto metody umožňují spolehlivější odhalení útočníka (viz sekce č. 2.5.1).

2.3 Záruka

Dalším klíčovým aspektem procesu ověřování identity, je skutečnost, že každé řešení nabízející nástroje pro realizaci tohoto procesu by mělo spadat do jasně definované kategorie z hlediska spolehlivosti a důvěryhodnosti poskytované služby. Ne všechna řešení jsou vhodná pro všechny

kontexty. Některé instituce a organizace požadují vyšší úroveň záruky, zejména pokud se jedná o přístup k citlivým informacím, jako je přístup k veřejným službám státních orgánů. Pro jiné může být prioritou spíše maximalizace konverze klientů, což vyžaduje kladení důrazu na uživatelský zážitek nad bezpečností. Dodatečné kontroly mohou být prováděny až po poskytnutí přístupu klientovi k požadovaným informacím nebo službám.

V roce 2014 Evropská Unie představila nové řešení pro elektronickou identifikaci a autentizaci (známé jako eIDAS), jehož cílem bylo zavést do praxe nové identifikační metody. Tyto metody nejenže umožnily potvrzení identity uživatelů na dálku, ale také stanovily unifikovaná pravidla, která měla pomoci zmírnit rozdíly ve způsobech a přístupech k identifikaci mezi členskými státy EU. Tím byla zajištěna vysoká kvalita a záruka procesu identifikace. Navíc byla definována pravidla pro jednotlivé Úrovně záruky (z anglického "Level of Assurance (LoA)"), kterými se jednoznačně kvalifikují poskytovatelé řešení pro ověřování identity. Úrovně jsou definovány následovně [8]:

- **Nízká**: tato úroveň znamená, že identita byla ověřena na základě dokumentů, které jsou považovány za pravé a které byly vydané důvěryhodným zdrojem. Přestože dokumenty byly shledány odpovídajícími, nedostatek dalších důkazů nebo menší kvalita dostupných důkazů neumožňuje plně potvrdit identitu osoby s vysokou mírou spolehlivosti. Příkladem může být ověření totožnosti na dálku, kde se ověřují základní údaje bez hlubších biometrických nebo jiných pokročilých ověřovacích procesů.

- **Podstatná**: na této úrovni byl důkaz totožnosti důkladně ověřen a riziko, že by důkaz nebyl platný, je minimalizováno. To obvykle zahrnuje prezentaci fyzického dokladu totožnosti, který byl rozpoznán jako pravý, nebo potvrzení identity pomocí postupů, které jsou ve státě považovány za rovnocenné s vysokou mírou jistoty. Toto může zahrnovat například použití biometrických údajů (viz sekce č. 2.1.2).

- **Vysoká**: nejvyšší úroveň záruky vyžaduje osobní nebo dozorované vzdálené ověřování identity, povinný sběr biometrických údajů a ověření adresy. Identita je ověřována pomocí více metod, včetně biometrie a dalších pokročilých technologií, což poskytuje vysokou míru jistoty o její pravosti. V případě, že biometrické údaje nejsou k dispozici, je nutné je získat podle standardních postupů daného státu. Tato úroveň je typická pro situace s vysokými bezpečnostními požadavky, jako jsou bankovní transakce nebo přístup k citlivým informacím.

Tyto úrovně jistoty pomáhají institucím a organizacím určit, které řešení pro ověřování identity je nejvhodnější pro jejich specifické potřeby a požadavky.

2.4 Identifikace v kontextu bankovnictví

Jak již bylo zmíněno v sekci č. 2.1, tato práce se zaměřuje primárně na ověřování identity fyzických osob na dálku. Konkretně - v oboru finančních a úvěrových institucí. V tomto kontextu je klíčové uvést další pojem - onboarding, jehož nedílnou součástí je ověřování identity.

Onboarding obecně je proces začlenění jednotlivců do organizace nebo instituce. Onboardingový proces může být jednoduchý, nebo zahrnovat řadu dílčích procesů, jejichž cílem je ověřit důvěryhodnost a spolehlivost jednotlivce a v případě úspěšného ověření zprostředkovat nezbytné informace pro jeho zařazení do dané instituce. Součástí onboardingu může být často i školení týkající se požadovaných služeb nebo obecných zásad společnosti. V kontextu finančních a úvěrových institucí tento proces pomáhá organizacím minimalizovat rizika, jako je podvod, praní špinavých peněz, financování terorismu a další nelegální aktivity [9]. Potvrzení identity je nejrozsáhlejší části přijetí a navázaní spolupráce s novým zákazníkem. Nicméně, tento proces nachází uplatnění i ve řadě dalších operací: provádění určitých typů transakcí, změna údajů, přístup k online bankovnictví, vyžádání úvěru nebo hypotéky, průběžné kontroly a aktualizace informací.

Onboarding nemá univerzálně definovaný proces skrze jediný oficiální zdroj. Existují však různé regulace, směrnice a doporučení, které nastiňují kritéria a nejlepší praxe pro onboarding klientů.

2.4.1 Definice a principy KYC a AML

Před zahájením jakéhokoli obchodního vztahu s klienty, jsou finanční nebo úvěrové instituce povinny provést náležité ověření důvěryhodnosti daného klienta. V této souvislosti je proces onboardingu obvykle součástí aplikovaných kontrolních opatření. Tento proces bývá standardně rozšířen dalšími kontrolami, které dohromady tvoří proces "Know Your Customer (KYC)", z anglického "Poznej svého zákazníka". Tento proces se používá pro posouzení profilu rizika zákazníka a monitorování jeho transakcí. Jedná se o preventivní zásadu, která chrání finanční a úvěrové instituce před nelegálními aktivitami a zajistí, že instituce jsou v souladu s předpisy proti praní špinavých peněz a financování terorismu (AML/CFT) [10].

Klíčovými komponenty KYC procesu jsou:

- Identifikace zákazníka (viz definice v sekci č. 2.2) a úvodní onboarding.
- Důkladné ověření zákazníka (CDD, z anglického "Customer Due Diligence"): proces, jehož cílem je shromažďování a vyhodnocování relevantních informací o zákazníkovi nebo potenciálním zákazníkovi pro odhalení případných rizik, která by finanční instituci mohla hrozit při obchodování s konkrétní organizací nebo jednotlivcem, a to na základě analýzy informací získaných z různch zdrojů [11].
- Rozsáhlá hloubková kontrola (ECDD, z anlického "Enhanced Customer Due Diligence"): zaměřuje se na rizikovější činnosti a osoby, jako jsou politicky exponované osoby ve vysoce rizikových odvětvích podnikání [12].

KYC proces se obvykle skládá z prvotního onboardingu nového klienta, který pokračuje průběžným monitorováním aktivity klientů a reportováním v případě, že dojde k podezřelé aktivitě.

V rámci EU jsou finanční a úvěrové instituce regulovány řadou směrnic a nařízení, které jsou zaměřeny na boj proti praní špinavých peněz a financování terorismu. Klíčovým legislativním rámcem jsou směrnice proti praní špinavých peněz (AMLD) pravidelně aktualizované Evropskou Unií. Tyto směrnice mají za cíl zabránit zneužívání finančního systému pro praní peněz nebo financování terorismu a také mají zásadní význam pro stanovení požadavků na online onboarding a ověřování identity. [2] [3]

2.4.2 Požadavky na proces onboardingu a ověření identity dle EBA

Směrnice AML přímo nespecifikují nástroje nebo kroky, které musí povinné subjekty splnit, aby byly v souladu se zveřejněnými požadavky v kontextu onboardingu a hloubkového ověření klientů na dálku. Vzhledem k tomu v roce 2022 Evropský orgán pro bankovnictví (EBA) zveřejnil obecné pokyny, které tyto nejasnosti doplňují. Cílem je zabránit významným rozdílům mezi realizacemi AML požadavků v různých státech a institucích, což by snížilo bezpečnostní riziko [6].

Konkrétně manuál stanoví postupy a kroky, které musí finanční a úvěrové instituce zavést, aby byly v souladu se směrnicí AMLD4 (oficiálně známá jako Směrnice (EU) 2015/849). Tyto postupy se týkají především tří oblastí:

1. Situace, kdy úvěrové a finanční instituce provádějí onboarding svých klientů na dálku.

[2] AMLD4 - Směrnice (EU) 2015/849
[3] AMLD5 - Směrnice (EU) 2018/843

2. Jak posuzovat kvalitu a dodržení pravidel směrnice, kdy finanční a úvěrové instituce spoléhají na řešení třetích stran, které nabízejí plný nebo částečný onboarding klientů na dálku.

3. Postupy při provedení CDD na dálku.

Hlavními subjekty těchto standardů jsou finanční a úvěrové instituce. Ale tyto pokyny mají být zváženy i dodavateli, kteří poskytují plné nebo částečné onboardingové řešení výše zmíněným institucím, aby byli připravení ke kontrole a přehodnocení svého řešení ze strany odběratelů a také k průběžnému monitorování a dohledu. Pro účely této práce je klíčový právě pohled ze strany dodavatelů služeb a komponent, které mají za účel podporovat onboarding nových zákazníků na dálku. Nerelevantní části budou v dalším popisu úmyslně vynechány.

Povinnosti odběratelů

Před integrací řešení pro onboarding do svých systémů musí zodpovědné orgány a finanční instituce provést posouzení vhodnosti daného řešení, jeho kvality, bezpečnosti, spolehlivosti a rizik.

Zvážit mohou dvě možnosti:

1. Provedení hodnocení samostatně a v případě potřeby poskytnout všechny relevantní podklady potvrzující jejich závěry. Hodnocení podléhají požadavky definované v tabulkách č. 2.1, 2.2, 2.3.

2. Implementovat řešení, které již splňuje podmínky popsané v doporučeních EBA, což může zahrnovat:

   - Řešení splňující úroveň záruky "Podstatná"nebo "Vysoká"(viz kapitola 2.3).
   - Nebo je kvalifikovanou službou, respektive komponentou. Což znamená, že tato služba nebo komponenta prošla procesem certifikace nebo akreditace od oprávněného orgánu, který potvrzuje její schopnost bezpečně a spolehlivě poskytovat služby pro identifikaci klientů [13].

Seznam požadavků pro onboardingové řešení dle EBA

Onboardingové řešení, ať už se jedná o interní řešení nebo službu poskytovanou externím dodavatelem, musí splňovat požadavky zajišťující, že služba je spolehlivá a v souladu s předpisy EU. Příslušná instituce, která řešení implementuje, by měla být schopna splnění těchto požadavků prokázat poskytnutím příslušné dokumentace a výsledků hodnocení, jak již bylo zmíněno výše v sekci č. 2.4.2.

Požadavky jsou kladeny na jednotlivé subprocesy, které probíhají během onboardingu nových klientů. Vzhledem k zaměření Trask ZenID (víe v kapitole č. 3), budou v rámci této práce analyzované především požadavky spojené s procesy "Sběr důkazů a atributů", "Validace shromážděných dat", "Vazba a verifikace"(dle kapitoly č. 2.2). Z analýzy jsou navíc vynechány požadavky kladené na právnické osoby nebo požadavky spojené s kontrolami, které navazují na proces identifikace: mikroplatby, zaslání jednorázového přístupového kódu atd.

Seznam odvozených požadavků je znázorněn v tabulkách č. 2.1, 2.2, 2.3.[4]

[4]Tabulky byly vytvořeny autorem na základě interpretace obecných pokynů EBA. [6].

Sběr důkazů a atributů	
RQ1	**Aktuálnost dat:** zajištění, že data získaná od klienta jsou aktuální, což znamená, že odrážejí nejnovější dostupné informace o klientovi v čase ověřování.
RQ2	**Dostatečnost dat:** data získaná od klienta musí být dostatečná pro účely ověření identity, což zahrnuje množství a typ dokladů a informací potřebných k úspěšnému procesu ověření.
RQ3	**Čitelnost dat:** data musí být čitelná pro možnost následného ověření, což zahrnuje jasnost a srozumitelnost informací poskytnutých klientem, jejich uchování ve zpracovatelné podobě.
RQ4	**Bezpečnost uchovávání dat:** zajištění bezpečnosti uchovávání dat získaných od klientů, včetně ochrany před neoprávněným přístupem a zneužitím.
RQ5	**Okolní podmínky během sběru dat:** data jsou pořizována za vhodných podmínek během sběru důkazů pro zajištění jejich kvality a jednoznačnosti.
RQ6	**Časování pořízení dat:** zajištění, že data byla pořízena v době provedení ověření, aby byla relevantní a aktuální.
RQ7	**Doba uchování dat:** data mají jasně definovanou dobu uchování, po kterou musí být zachována pro případnou revizi nebo audit. Po termínu mají být ze systému smazána.

Tabulka 2.1 Požadavky kladené na proces sběru důkazů a atributů

Validace dat	
RQ8	**Bezpečnostní prvky na dokladu:** ověření, že předložená kopie dokladu totožnosti obsahuje bezpečnostní prvky vložené do původního dokladu.
RQ9	**Dodržení specifikací modelu dokladu:** ověření, že předložená kopie dokladu dodržuje specifikace (typ, velikost znaků, struktura) kladené na původní doklad.
RQ10	**Absence zásahu:** předložená kopie dokladu nesmí obsahovat viditelných příznaků zásahu a manipulace s osobními údaji a fotografií držitele.
RQ11	**Integrita algoritmu pro generování ID:** zajištění integrity algoritmu použitého pro generování jedinečného identifikačního čísla.
RQ12	**Kvalita a rozlišení:** ověření dostatečné kvality a rozlišení předložené kopie dokladu totožnosti.
RQ13	**Původ dokladu:** zkoumání, zda se jedná o doklad poskytnutý vyfocením obrazovky, tištěné kopie, nebo skenu.
RQ14	**Přesnost a konzistence automatizovaného čtení:** zajištění přesnosti a konzistence funkcí pro automatické čtení informací z dokladu, pokud je použito.
RQ15	**Ověření informací z čipu:** ověření souladu informací získaných z vestavěných čipů, s daty z jiných zdrojů, pokud je to technicky možné.
RQ16	**Ověření pravosti bezpečnostních prvků na dokladu:** ověření pravosti bezpečnostních prvků použitých na dokladu včetně jejich známých a ověřitelných charakteristikám.

Tabulka 2.2 Požadavky kladené na proces validaci poskytnutých evidencí

Vazba a verifikace	
RQ17	**Shoda s fyzickou osobou:** zajištění ověření shody mezi viditelnými informacemi o fyzické osobě a poskytnutou dokumentací.
RQ18	**Spolehlivost při ověření shody:** použití odolné a spolehlivé algoritmy k ověření shody mezi biometrickými údaji v dokladu a klientem.
RQ19	**Doplňkové kontroly při nedostatečné důvěře:** pokud není zajištěna požadovaná úroveň důvěry, mějí být uplatněny další kontroly.
RQ20	**Detekce živosti:** provádět ověření detekce živosti pro ověření, že klient je přítomen v komunikační relaci, a to pomocí vyžádání k provedení akcí od klienta (aktivní ověření) nebo pomocí analýzy přijatých dat, které nevyžadují konkrétní akci (pasivní ověření).
RQ21	**Náhodnost v posloupnosti úkonů:** zajištění náhodnosti v posloupnosti úkonů během detekce živosti, pokud je to možné.

Tabulka 2.3 Požadavky kladené na proces vazby a verifikace

2.4.3 Regulace v České Republice

V České republice a v kontextu evropského regulačního prostředí se na dohled nad dodržováním pravidel proti praní peněz a financování terorismu, včetně procesů KYC a online onboardingu, podílí několik orgánů: Česká národní banka (ČNB), Finanční analytický úřad (FAÚ), Ministerstvo financí ČR.

Primární dohled a regulaci finančního sektoru České republiky zajišťuje Česká národní banka (ČNB). Jejím úkolem je dohled nad širokým spektrem finančních subjektů, včetně bank, pojišťoven, důchodových fondů a obchodníků s cennými papíry. Je požadováno, aby tyto instituce důsledně implementovaly a vynucovaly politiku spojené s KYC procesy, což zahrnuje nejen počáteční ověření identity a účelu obchodních vztahů s klienty, ale také kontinuální sledování jejich transakcí a aktivity. V situacích, kdy dojde k detekci podezřelých činností ze strany klientů, jsou finanční instituce právně zavázány k nahlášení takových případů Finančnímu analytickému úřadu pro další analýzu a potenciální právní kroky [3].

Specifika procesů dle státních předpisů

Identifikace je povinná v případě provedení velkých transakcí, podezřelého obchodu nebo vzniku obchodního vztahu [14].

Legislativní předpisy v ČR stanovují minimální rozsah informací, které instituce provádějící onboarding a identifikaci jsou povinné zjistit od svých klientů před uzavřením obchodních vztahů. Instituce musí dodržet tyto povinnosti, avšak nejsou na to omezeny. Vzhledem k odlišnosti obchodních vztahů a vnitřních procesů mají instituce právo rozhodnout, jaké další informace od svých klientů požadovat v závislosti třeba na stupni jejich rizikovosti.

Pro osobní identifikaci fyzických osob je postačující jeden doklad totožnosti, nejčastěji se jedná o občanský průkaz. Tento doklad slouží pro potvrzení pravdivosti následujících informací získaných od klienta: jména, příjmení, rodného čísla (nebo data narození pro cizince), místa narození, pohlaví, údajů o pobytu (název, sídlo, IČ). Pak jsou také zaznamenány informace o dokladu: typ, číslo dokladu, stát nebo orgán, který doklad vydal, doba platnosti, shodu mezi držitelem a osobou identifikace [14].

Legislativa také umožňuje provádění identifikace na dálku. V tomto případě je nezbytné doložit dva doklady potvrzující totožnost. Další povinností je prokázání existence účtu u jiné finanční nebo úvěrové instituce a následný převod peněžních prostředků z tohoto účtu. Alternativou k tomuto způsobu je zaslání osobních informací, která byla opatřena kvalifikovaným elektronickým podpisem [15].

V obou případech instituce musí uchovávat kopie předložených dokladů totožnosti po dobu deseti let. Tyto informace jsou chráněné bankovním tajemstvím (povinností mlčenlivosti). Instituce mají ve svých vnitřních předpisech zohlednit pokyny dané Evropskou unií v příslušném sektoru trhu, zvážit a zohlednit osvědčené principy a postupy v oblasti identifikace a kontroly klienta a mají sami posoudit, která cesta je pro ně vyhovující. Omezení nejsou kladena, takže instituce mohou rozšířit tyto minimální požadavky o další kontroly. Hlavní podmínkou je, aby tyto kontroly nebyly v rozporu s právními předpisy EU a ČR [16].

2.5 Prevence útoků

Dalším důležitým aspektem pro porozumění, jak by měl vypadat spolehlivý proces ověřování identity, jsou hrozby ze strany útočníků na taková řešení. V době rychlé digitalizace a vývoje technologií založených na principu neuronových sítí a umělé inteligence, získávají útočníci neomezený potenciál a sadu nástrojů, které mohou s jednoduchostí využít pro napadení systémů pro onboarding klientů a vzdálenou identifikaci. Tyto systémy se stále častěji potýkají s různorodými útoky a někteří dodavatelé nestíhají s rostoucím tempem technologií včas reagovat na nové typy útoků.

2.5.1 Klasifikace útoků

Útoky lze rozdělit podle zaměření na prostředky identifikace. Mezi ně patří [17]:

- **Pravý doklad totožnosti s pozměněnými částmi:** tento typ útoku zahrnuje použití autentického dokladu, jako je odcizený nebo ztracený doklad, jehož určité informace (např. fotografie nebo datum narození) byly modifikovány tak, aby odpovídaly útočníkovi.
- **Úplná reprodukce pravého dokladu:** zde útočník vytvoří kopii existujícího dokladu totožnosti skutečné osoby, včetně všech oficiálních znaků, což může vést ke zfalšování identity.
- **Výroba dokladu pro fiktivní identitu:** tento útok spočívá ve vytvoření zcela nového dokladu totožnosti, který není registrován v žádné databázi a odpovídá neexistující osobě.
- **Reprodukce dokladu s částečně pravou, částečně fiktivní totožností:** v tomto případě útočník kombinuje pravé a fiktivní informace, například změní datum narození na reálném dokladu, což může být použito pro obejití věkových omezení nebo pro získání přístupu do chráněných systémů.
- **Neexistující doklad totožnosti:** útočník vytvoří zcela nový typ dokladu, který není založen na žádném existujícím vzoru. Takové dokumenty jsou často používány v kontextech, kde kontrolní mechanismy nejsou dostatečně robustní na odhalení atypických vzorů.

Další útoky jsou zaměřeny na falšování biometrických charakteristik, tzv. prezentační útoky [17]:

- **Získání a nahrání fotografie:** útočník použije fotografii cílové osoby k vytvoření falešného důkazu o její přítomnosti, čímž může obejít systémy kontroly živosti.
- **Předtočení a přehrání videa:** tato metoda spočívá v nahrání videa, které je poté přehráno během procesu identifikace, aby se simulovala reálná interakce.
- **Využití 3D masek:** vysoce kvalitní masky mohou imitovat biometrické rysy jiné osoby, což umožňuje útočníkům přesvědčivě napodobit cíl a obejít biometrické bezpečnostní systémy.
- **Synteticky tvořené deepfaky:** použití uměle vytvořených videí nebo obrázků, které mohou zobrazovat jakoukoliv osobu v různých situacích, je další sofistikovanou metodou, která může zneužívat identitu a manipulovat s elektronickými důkazy.

2.5.2 Jak předcházet útokům?

Každé řešení může implementovat různé metody pro předcházení útokům na proces identifikace. Bezpečnostní mechanismy lze obvykle rozdělit do dvou základních skupin: opatření zaměřená na "Liveness"ověření[5] osoby a pravosti dokumentu. Agentura ENISA ve své zprávě uvedla nejpoužívanější a nejčastěji zaváděné metody, které společnosti používají k prevenci výše uvedených útoků [17].
Při "Liveness"ověření cílem je rozpoznat, zda interakci provádí skutečná osoba a eliminovat riziko podvodu prostřednictvím fotografie, videa nebo jiných prostředků:

- **Záznam videosekvence:** během online identifikačního procesu je nahráno video, během kterého je osoba vyzvaná k provedení určité akce (například mrknutí nebo otočení hlavy), což pomáhá ověřit, že interakce probíhá v reálném čase.
- **Metody ověření živosti (Active/Passive Liveness):** aktivní metody vyžadují od uživatele interakci (např. hlasový příkaz), zatímco pasivní metody analyzují vstupní data na pozadí bez nutnosti uživatelovy interakce, což zvyšuje pohodlí a snižuje riziko odhalení metodou útočníka (viz více v sekci č. 3.2.2).

[5] "Liveness"je ověření, zda je osoba živá.

- **Porovnání obličejů:** systémy porovnávají aktuálně získaný obraz obličeje s fotografií na oficiálním dokladu totožnosti, aby potvrdily shodu.

Opatření spojené s ověřením pravosti dokladu se zaměřují na potvrzení autenticity identifikačních dokladů a ověření, že nebyly pozměněny nebo padělány:

- **Analýza videosekvence:** stejně jako u ověření živosti, videosekvence zaznamenaná během procesu může být analyzována na známky manipulace nebo falšování dokladů.
- **Validace více bezpečnostních prvků:** kontrola různých bezpečnostních znaků dokladu, jako jsou vodoznaky, hologramy a mikrotisky, a jejich vzájemné ověření zvyšuje spolehlivost identifikace.
- **Využití elektronických záznamů v čipech:** soubory uložené v čipu digitálních dokladů totožnosti, jako jsou biometrické pasy, obsahují chráněné záznamy, které lze číst speciálními zařízeními, což ztěžuje falšování.

S implementací a zavedením spolehlivějších a bezpečnějších metod však často přicházejí různá omezení, včetně potřeby většího úložného prostoru, vyžadované kvality internetového připojení, kvality použitých zařízení, rychlosti zpracování, délky procesu, úspěšnosti implementace a nákladů na řešení. Je tedy nezbytné zvážit předpoklady a prostředky použití těchto metod a s nimi spojená rizika. Jinými slovy, čím bezpečnější je systém, tím méně je pohodlný, protože uživatelé mohou být systémem falešně odmítnuti.

V této kapitole byl podrobně zkoumán proces ověřování identity, který představuje klíčový prvek pro zajištění bezpečnosti a důvěryhodnosti v digitálním prostředí. Analýza je věnována konkrétně vzdálené identifikaci fyzických osob, zejména v kontextu úvěrových a finančních institucí, což představuje hlavní oblast užití systému Trask ZenID. Zvláštní pozornost byla věnována průběhu tohoto procesu a legislativním předpisům, které udržují jeho vysokou bezpečnostní úroveň. Dále byly zkoumány hlavní výzvy, s nimiž se společnosti nabízející vzdálené ověřování identity setkávají, a metody, které slouží k odvrácení útoků na tato řešení.

Zjištění poukázala na to, že integrace technologií pro ověřování elektronických dokladů, jak je naznačeno v části č. 2.5.2, může být efektivní strategií pro zlepšení identifikačních procesů. Tato integrace nabízí solidní základ pro argumentaci, že integrace zpracování obsahu digitálních dokladů může přinést významné výhody v kontextu rostoucích nároků na bezpečnost a regulaci.

V následující kapitole bude provedena detailnější analýza systému Trask ZenID a metod, které toto řešení nabízí pro ověřování identity zákazníků. Vzhledem k tomu, že systém Trask ZenID nebyl předmětem certifikace a tudíž se nekvalifikuje jako Důvěryhodný poskytovatel služeb (TSP) ani Komponenta (TSC), zvláštní pozornost bude věnována analýze splnění systémem Trask ZenID požadavků uvedených v sekci č. 2.4.2.

Tato analýza poskytne další předpoklady pro rozhodování o možnostech a nutnosti integrace zpracování digitálních dokladů totožnosti do systému Trask ZenID a spojené s tím přínosy.

Kapitola 3

Trask ZenID - řešení pro automatizovanou identifikaci klientů

V této kapitole je představeno řešení pro automatizovanou identifikaci klientů na dálku, známé pod názvem Trask ZenID, které bylo vyvinuto společností Trask Solutions a.s. Trask ZenID je úspěšně provazováno na českém trhu po dobu šesti let a ačkoliv je primárně orientováno na úvěrové a finanční instituce, jeho využití není tímto sektorem omezeno. Řešení našlo uplatnění i v dalších oblastech a podařilo se ho rozšířit také za hranice České republiky.

Trask ZenID se zaměřuje na řešení klíčových problémů, které byly popsány v předchozích částech (viz sekce č. 2.5), a snaží se poskytnout svým klientům moderní a spolehlivé řešení pro identifikaci. Významný důraz je kladen na flexibilitu a konfigurovatelnost softwaru, což umožňuje jeho efektivní integraci do různých zákaznických prostředí.

Kapitola poskytuje detailní popis tohoto řešení vytvořený na základě veřejně dostupných informací, interní dokumentace projektu, osobních zkušenosti s produktem a taky konzultací s projektovým týmem. Popis začíná seznamem modulů, které Trask ZenID obsahuje, následně je přistoupeno k popisu funkcionalit a integrace systému do zákaznických prostředí, včetně způsobu licencování. Tato kapitola slouží jako základ, na kterém bude postavena další analýza a diskuse o možnostech rozšíření Trask ZenID.

3.1 Případy užití

Jak již bylo dříve uvedeno (viz sekce č 2.1), fyzická a digitální identifikace klientů mají široké spektrum uplatnění napříč různými obory. Systém Trask ZenID působí v mnoha sektorech, kde mezi jeho primární zákazníky a partnery patří instituce z finančního sektoru, pojišťovnictví, loterií a herního průmyslu, telekomunikací, energetiky a cestovního ruchu. Dominantní podíl zákazníků Trask ZenID připadá na osoby povinné k AML (viz sekce č. 2.4.1), zejména finanční a úvěrové instituce.

Trask ZenID poskytuje flexibilní řešení pro různé případy užití, přičemž zákazníci si mohou vybrat moduly podle svých specifických potřeb a integrovat je do svých systémů. Vzhledem k tomu Trask ZenID nemá přímý přehled o všech specifických využitích svých služeb u zákazníků. Následná tabulka č. 3.1 sumarizuje základní sektory působení Trask ZenID a poskytuje přehled typických případů užití identifikace na dálku, které zahrnují jak běžné, tak unikátní scénáře v

různých odvětvích.[1] Tyto informace byly shromážděny na základě osobních zkušenosti s produktem a také diskuze s týmem Trask ZenID.

Je důležité zdůraznit, že proces digitalizace je dynamický a neustále se vyvíjí, přičemž se rozšiřuje i do oblastí, kde bylo tradičně předpokládáno pouze manuální ověření totožnosti. V důsledku toho poptávka po službách umožňujících identifikaci klientů prostřednictvím automatizovaného řešení neustále roste. Trask ZenID proto rozšiřuje své služby i do dalších sektorů, pro které je automatizace ověření identity klientů klíčová.

Případy užití	**Financování**	**Pojišťovnictví**	**Loterie a hry**	**Telekomunikace**	**Energetika**	**Cestování**
Ověření totožnosti při otevření účtu	✓	✓				
Registrace nového zákazníka	✓	✓	✓	✓	✓	✓
Aktivace / reaktivace účtu	✓	✓	✓	✓	✓	✓
Ztráta / zapomenutí přístupových údajů	✓	✓	✓	✓	✓	✓
Přístup k online službám			✓	✓	✓	✓
Ověření věku a identity	✓	✓	✓	✓		
Zabezpečení proti podvodům	✓	✓	✓	✓	✓	✓
Sjednání produktu	✓	✓	✓	✓	✓	✓
Průběžné kontroly totožnosti	✓	✓		✓		
Ověření klienta před výplatou výhry			✓			
Aktivace služby bez fyzické přítomnosti				✓		
Zajištění compliance a regulatorních požadavků	✓	✓	✓			
Online check-in						✓

Tabulka 3.1 Přehled případů užití Trask ZenID v různých odvětvích

3.2 Struktura systému

Centrálním prvkem Trask ZenID je modulární systém, který lze rozdělit na několik samostatných částí, označovaných Moduly. Moduly představují nejvyšší vrstvu, jež určuje, které identifikační kontroly budou zákazníky využívány.

Jádrem Trask ZenID jsou čtyři základní moduly, které si zákazníci mohou zařadit do svého portfolia při sjednání licenční smlouvy (viz. podrobnější informace v sekci č. 3.6):

- **Modul OCR (Optické rozpoznávání znaků):** představuje základní modul umožňující nahrání, zpracování a aplikaci základních kontrol pro ověření pravosti předložených dokladů totožnosti.
- **Modul Kontroly Podvodu:** rozšiřuje možnosti modulu OCR o pokročilé kontroly ověřující integritu a autenticitu dokladů prostřednictvím analýzy širšího spektra bezpečnostních prvků.

[1] Tabulka byla vytvořena autorem na základě konzultací s vedením projektu Trask ZenID

- **Modul Tvář:** nezávislý modul umožňující pořizování a nahrávání fotografií či videí držitelů dokladů a jejich zpracování s ověřením, zda se jedná o reálné osoby odpovídající identitě na poskytnutých dokladech.
- **Modul Tvorba reportů:** slouží k podpoře operativních procesů poskytnutím přehledu o prováděných kontrolách prostřednictvím agregace a seskupení klíčových informací napříč systémem.

Moduly jsou dále strukturovány do komponent, což umožňuje lepší a přehlednější orientaci v možnostech systému. Podrobnější přehled jednotlivých modulů a jejích komponent bude poskytnut v další části práce (viz sekce č. 3.2.2).

Celkově lze systém Trask ZenID a jednotlivé moduly využít v různých konfiguracích, které pokrývají široké spektrum požadavků na proces identifikace tak, aby vyhovovaly potřebám zákazníků. Interní nastavení modulů a komponent zákazníci mohou libovolně upravovat prostřednictvím uživatelského rozhraní backendu (více v části č. 3.5.1). Pro aktivaci nebo deaktivaci modulu je nezbytná spolupráce obou stran (dodavatelé a zákazníka) s ohledem na aktualizaci licenčních podmínek.

3.2.1 Koncept profilů, validátorů a provádění kontrol

Důležitou roli v procesu ověřování identity pomocí systému Trask ZenID hraje sada kontrol, které systém nabízí. Tyto kontroly jsou označovány termínem „validátory“. Validátory lze konfigurovat pro různé profily, které odpovídají jednotlivým případům užití systému. Níže následuje podrobnější vysvětlení tohoto konceptu.

Validátory

Každá komponenta je představená seznamem validátorů, respektive kontrol, které jsou aplikovány na vzorek (digitální kopii dokumentu nebo biometrických charakteristik) při jeho zpracování. Každý validátor umožňuje základní nastavení jednotlivých kontrol, včetně možnosti kalibrace přípustné prahové hodnoty, a také deaktivaci nebo aktivaci kontroly v rámci komponenty. Pokud není prahová hodnota dosažena, validátor vrátí chybu po dokončení zpracování.

Validátory se liší podle komplexnosti: **jednoduché validátory** obvykle reprezentují jednu kontrolu vystavenou zákazníkům, zatímco **složené validátory** zahrnují několik vnořených subkontrol, které lze konfigurovat samostatně. Navíc jsou validátory rozdělené podle typu výsledku, který vracejí: **binární validátory** poskytují odpověď úspěšné/neúspěšné (100/0); **analogové validátory** vrací stupeň úspěšnosti v konfidenčním intervalu od 0 do 100, přičemž úspěšnost validátora závisí na nastavené prahové hodnotě. Dále se validátory rozlišují podle prostředí, na které jsou aplikovány: **backendové validátory** jsou spouštěny v rámci kontroly prováděné přímo na hlavním serveru systému, **SDK validátory** jsou spouštěny na straně klienta, a **validátory kombinující** backend a SDK jsou využívány oběma částmi systému.

V rámci této práce nebudou analyzovány všechny validátory a kontroly, které jsou jejich součástí. Některé kontroly mohou být sloučeny dohromady pro lepší přehlednost procesu. Pro účely této práce je takový přístup považován za dostatečný. V případě potřeby detailnější analýzy mohou být specifické části systému, včetně kontrol, prozkoumány do většího detailu, pokud to konceptuálně dává smysl.

Profily

Jak již bylo naznačeno v tabulce č. 3.1, zákazníci mohou využívat jednu instanci Trask ZenID k uspokojení více různých obchodních požadavků . Každý požadavek může být realizován prostřednictvím různých kanálů v kontextu interakce se zákazníkem (na dálku, fyzicky na pobočkách,

nebo za využití smíšených kanálu). Společnosti tak potřebují nástroj, který jim umožní jednoduše nastavit specifika procesu co se týče průchodnosti, zabezpečení, úrovně spolehlivosti a uživatelského zážitku, zvláště pro různé procesy, aby tyto požadavky splnily. Trask ZenID nabízí konfiguraci několika profilů jako abstrakční vrstvu. Každý profil odpovídá konkretnímu obchodnímu procesu. Tento mechanismus umožňuje ukládat různé sady validátorů a různá nastavení napříč validátory pro různé profily.

3.2.2 Přehled modulů a komponent

Modul OCR

Modul Optického Rozpoznávání Znaků, známý pod anglickou zkratkou OCR, tvoří fundamentální prvek systému Trask ZenID. Je zaměřen na zpracování digitálních verzí osobních dokladů, jako jsou skeny či fotografie. Tento modul automatizovaně identifikuje typ a model dokladu, extrahuje údaje a v případě potřeby provádí anonymizaci, čímž umožňuje další bezpečnou manipulaci, uchování a integraci informací do následných procesů. V rámci tohoto modulu se rovněž vykonávají elementární kontroly nad extrahovanými daty.

Komponenta OCR. Optické rozpoznávání znaků je technologie, která umožňuje transformaci tištěného textu z obrazové podoby do formy, jež je strojově čitelná a zpracovatelná. Úspěšná detekce a extrakce dat jsou závislé na dostupnosti předem natrénovaného modelu strojového učení (dále jen ML model) pro odpovídající typ fyzického dokladu totožnosti.

Komponenta jako vstup přijímá elektronickou kopii jednoho nebo více dokladu, to jest fotografie či video záznamy dokladů.

Následně systém identifikuje relevantní typ a model dokladu (více v sekci č. 3.3). Pokud identifikace proběhla úspěšně, provádí extrakci údajů a aplikuje na doklad aktivované kontroly. Jako výstup komponenta poskytuje původní obraz doplněný o extrahované údaje, přesnost extrakce jednotlivých polí dokumentu, výsledky kontrol odpovídajících validátorů vyjádřené skóre od 0 do 100 a celkové hodnocení operace.

Mezi nabízené kontroly patří:

- Ověření integrity
  1. **Kontrola konzistence mezi doklady:** ověřuje, zda informace na různých poskytnutých dokladech jsou vzájemně konzistentní a neobsahují rozpory.
  2. **Validátor podpisu SDK (viz sekce č. 3.2.3):** pokud pro pořízení dokladu bylo využité proprietární frontendová knihovna, zajišťuje, že obraz dokladu nebyl změněn po odeslání a je shodný s originálním záznamem.
  3. **Kompletnost dokladu:** kontroluje, že doklad obsahuje všechny požadované strany a údaje.
  4. **Neznámé soubory a povinná pole**: zajišťuje, že formát nahrávaného souboru odpovídá požadavkům a že jsou vyplněna všechna povinná pole.
- Ověření vůči externím službám
  1. **Kontrola insolvence:** zjišťuje, zda držitel karty není zapsán v insolvenčním rejstříku, což může signalizovat potíže s autenticitou dokladu.
  2. **Kontrola neplatného čísla OP:** ověřuje, že číslo občanského průkazu je platné a není uvedeno v databázích jako neplatné nebo ztracené.
- Ověření bezpečnostních prvků a křížové kontroly

1. **Kontrola rozsahu platnosti:** ověřuje, že číslo dokladu odpovídá vydávaným rozsahům a není již expirované.
2. **Kontrola MRZ:** provádí kontrolu dle algoritmu pro generování strojové čitelné zóny, srovnává údaje obsažené v strojově čitelné zóně s údaji na dokladu a kontroluje správnost všech uvedených hodnot.
3. **Kontrola čárového kódu:** provádí extrakci dat z čárového kódu a porovnává s daty na dokladu.
4. **Kontrola rodného čísla:** porovnává rodné číslo s datem narození a s pohlávím.
5. **Kontrola validity identifikačního čísla na dokladu:** kontroluje, zda je číslo průkazu totožnosti v platném rozsahu pro datum jeho vydání.

- Analýza obrazových prvků dokladu

1. **Přítomnost obrazu dokladu:** kontroluje, zda byl k dokladu nahrán jeho obraz.
2. **DPI a zaostření:** prověřuje kvalitu obrazu dokladu, zda není nízké rozlišení nebo špatné zaostření, což by mohlo ukazovat na nekvalitní kopie nebo možnou manipulaci.
3. **Ověření odlesků na fotografii:** kontroluje, zda na obrazu dokladu nejsou viditelné odlesky, které by mohly naznačovat nekvalitní sken nebo fotografii.

- Další zabezpečení a ochrana proti manipulaci

1. **OCR - kontrola správnosti přepisu údajů**: analyzuje text extrahovaný z dokladu a indikuje spolehlivost extrakce.
2. **Naklonění obličeje na dokladu:** ověřuje správné umístění a náklon fotky držitelé na identifikačních dokladech.
3. **Ověření metadat repliky:** prověřuje metadata spojená s obrazem, například datum a čas pořízení fotky, což může pomoci identifikovat neautorizované úpravy.

Komponenta Censor. Nařízení o ochraně osobních údajů GDPR omezuje možnost společnostem uchovávat nebo zprostředkovávat citlivá osobní data svých zákazníků třetím stranám.

Funkcionalita "Censor"v rámci systému Trask ZenID poskytuje možnost automatického zatemnění citlivých informací na osobních dokladech podle předdefinovaných parametrů, což vede k anonymizaci dokumentu. Tento proces se uplatňuje na výsledky zpracování dokladu před jejich distribucí prostřednictvím API Trask ZenID (viz více v sekci č. 3.4).

Je třeba poznamenat, že tato funkce sama o sobě neprovádí žádné kontroly autenticity nebo integrity dokladů.

Modul Kontrola podvodů

Modul Kontrola podvodu se soustředí na rozšířené ověřování integrity, pravosti a autenticity dokladů. Během verifikace se zkoumá celá řada viditelných i strojově ověřitelných bezpečnostních prvků na dokladech, včetně barevnosti, typografie, hologramů a pokrytí. Modul přijímá elektronickou kopii dokladu ve formě obrázku nebo videa a na výstupu poskytuje výsledky aplikovaných kontrol.

Komponenty Kontrola podvodů a Detekce reálného dokladu. Tyto komponenty jsou nadstavbou modulu OCR. Na základě obdržené kopie dokladu nebo videozáznamu je komponenta schopna provádět pokročilé kontroly pro ověření pravosti a autenticity dokladů:

- Kontrola vizuální integrity a autenticity dokladu

1. **Vzhled písma:** kontrola, zda jsou typografické prvky normální a nebyly pozměněné.

2. **Mezery mezi písmeny:** ověření, že rozestupy mezi znaky jsou standardní a neukazují na úpravu textu.
3. **Vertikální zarovnanost:** ověření správného vertikálního uspořádání textových prvků.
4. **Poškození karty:** kontrola fyzického stavu dokladu pro odhalení známek opotřebení nebo poškození.
5. **Manipulace s políčky:** detekce nepravidelností na hranách dokladu, které by mohly indikovat neautorizované změny.
6. **Barva fotografie tváře:** ověření, že barvy na fotce jsou věrohodné a neprokazují známky manipulace.

- Analýza obrazové kvality a obsahu

1. **Obličej na dokladu:** analýza obličeje pro odhalení netypických vizuálních změn nebo pokusů o maskování identity.
2. **Maska na obličeji:** kontrola, že obličej na dokladu není zakrytý ani není pozměněn pomocí masky.
3. **Obrazovka nebo papír:** detekce znaků, že doklad nebyl vyfotografován nebo naskenován z nevhodné podložky jako je obrazovka nebo jiný papír.
4. **Podezřelé artefakty v obraze:** identifikace artefaktů, které by mohly být indikátory padělání nebo nepravých dokladu.

Komponenta Detekce hologramů. Na základě videozáznamu komponenta ověřuje přítomnost hologramu. Kontrola zahrnuje ověření, zdali dokument obsahuje hologram, jeho správné umístění a změny vizuálních prvků, jako je barevnost a tvar, při pohledu z různých úhlů v závislosti na pohybu dokladu.

1. **Kontrola hologramu:** kontrola přítomnosti a integrity holografických prvků na dokladu.
2. **Video bez střihu:** ověření, že video dokumentující identitu je nepřerušené a bez střihů, což naznačuje průběžný záznam.
3. **Odraz na videu:** kontrola, aby v obrazech z videa nebyly viditelné odrazy, které by mohly zkreslit informace.
4. **Přítomnost videozáznamu dokladu:** zajištění, že k dokladu existuje doprovodné video, což může být požadováno pro některé formy digitálního ověření.

Modul Tvář

Modul Tvář v systému Trask ZenID pracuje s fotografiemi nebo videozáznamy držitelů dokladů a snímkem jejich obličejů, které byly extrahované z dokladů totožnosti. Tento modul je integrován s externími službami pro detekci obličejů, porovnávání shody mezi dvěma obličeji a rozpoznání emocí. Zajišťuje srovnání fotografie z dokladu s autoportrétem (selfie), kontrolu živosti a možnost verifikace existence podobizny držitele v databázi obličejů.

Komponenta Detekce obličeje. Z názvu komponenty je zřejmé, že provádí detekci obličeje na dodaných obrázcích nebo videích a zahrnuje základní kontroly:

1. **Přítomnost selfie:** zajišťuje, že snímek obličeje byl ve skutečnosti nahrán během ověřovacího procesu.
2. **Tvář na fotografii:** ověřuje, že obličej na nahrávaném dokladu odpovídá subjektu identifikace.

3. **Přítomnost selfie videa:** kontroluje existenci videozáznamu autoportrétu požadovaného pro podrobnější verifikaci.
4. **Párování selfie:** realizuje biometrické srovnání autoportrétu s obličejem na dokladu, což umožňuje potvrzení totožnosti.

Komponenta srovnání selfie s databází. Komponenta verifikuje shodu obličejů ze selfie nebo dokladu vůči databázi obličejů. Analyzuje, zda daná osoba v databázi nevystupuje pod jinou identitou, a testuje podobnost s jinými subjekty v databázi. Trask ZenID neuchovává vlastní databázi obličejů z důvodů ochrany osobních údajů a přidružených regulací. Přesto systém disponuje funkcionalitou pro snadnou integraci s databázemi, které vytvořili klienti, nebo které poskytují třetí strany.

1. **Jedna tvář - několik čísel občanských průkazů**: porovnává fotografii osoby s dalšími záznamy v databázi.
2. **Jedno číslo občanského průkazu - několik tváří**: ověřuje shodu fotografie uživatele s jeho dřívějšími snímky uloženými v databázi.

Komponenta ověření živosti. Komponenta ověřuje, zda je subjekt na autoportrétu živá osoba prostřednictvím aktivních změn, jako jsou úsměvy a pohledy, zda nedochází ke změně obličejů během záznamu, zda osoba nenosí 2D nebo 3D masku, zda jsou splněny požadované akce, hodnotí kvalitu videozáznamu a podmínky jeho pořízení, kontroluje, že obličej nebyl částečně zakryt a že všechny referenční body pro spolehlivou detekci živosti jsou viditelné. Pro pochopení funkcí tohoto modulu je nutné rozlišit dva typy ověření živosti:

- **Aktivní ověření živosti**: na základě náhodně generované sekvence jsou subjekty vyzvány k provedení řady akcí. Systém je pak schopen za běhu posoudit, zda provedené akce odpovídají nastaveným požadavkům, a tím potvrdit, že subjekt je živý a přítomný během kontroly.
- **Pasivní ověření živosti:** snímky nebo videozáznamy subjektů jsou podrobeny důkladné analýze na backendové části systému bez přímé účasti identifikované osoby.

Modul Trask ZenID tedy nabízí následující typy kontrol pro ověření živosti:

1. **Dynamický obličej:** provádí ověření pohybu hlavy a změn mimiky, kontroluje správné provedení sekvence akcí a jejich pořadí.
2. **Kontinuita obličeje:** analyzuje, zda nedošlo k výměně obličeje během kontroly, posuzuje konzistenci mezi jednotlivými snímky záznamu.
3. **Autenticita obličeje:** ověřuje, že obličej není pouhá 2D nebo 3D imitace, a využívá pokročilé neuronové sítě pro detekci masek.
4. **Ověření nepraveného videomateriálu:** kontroluje, zda video neobsahuje upravené nebo předem připravené sekvence, a umožňuje nastavení specifických akcí a jejich pořadí pro ověření.
5. **Kvalita obrazu:** zajišťuje, že obličej na záznamu není částečně skrytý nebo znejasněný, což by mohlo ovlivnit spolehlivost detekce živosti.

Je důležité podotknout, že pro detekci obličeje, porovnání shody a rozpoznání emocí Trask ZenID využívá služby externí společnosti, specificky Microsoft Cognitive Services, což umožňuje využití jejich pokročilých algoritmů a rozsáhlých datových souborů pro zajištění vysoké přesnosti a spolehlivosti výsledků.

Modul Tvorba reportů

Modul Tvorba reportů neprovádí žádné kontroly; jeho primární funkcí je agregace informací, které poskytují základ pro podrobnou analýzu specialisty. Cílem je identifikovat možné problémy nebo nedostatky v navrženém procesu. Modul shromažďuje a centralizuje data z různých částí aplikace, včetně údajů o nahrávání vzorků a výsledcích kontrol, a vytváří z nich strukturovaný přehled pro další evaluaci.

Mezi hlavní funkcionality modulu patří:

1. **Agregace dat:** modul efektivně sbírá a syntetizuje informace, aby poskytl komplexní pohled na operace systému.
2. **Podrobný pohled:** umožňuje detailní prohlížení vzorků a investigací, seskupených podle specifických profilů nebo validátorů.
3. **Úprava výsledků v reportech**: uživatelé mohou v sekci filtrů upravit obsah reportu podle různých kritérií, jako jsou časové období, typy dokumentů, profily podléhající šetření, validátory.
4. **Stahování reportů:** přehled je dostupný ke stažení ve formátu CSV pro provádění vybraných analýz.

3.2.3 Mobilní a Webové SDK

Dalšími částmi služby Trask ZenID jsou digitální SDK (Software Development Kits). Tyto sady knihoven umožňují integraci do webových nebo mobilních aplikací klientů s cílem realizovat omezený rozsah kontrol pro zpracování dat bez přímého připojení k Internetu a jejich následnou integraci do backendové části Trask ZenID. Obvykle se doporučuje kombinace využití SDK společně s dalším zpracováním na straně serveru. K dispozici jsou knihovny pro webové aplikace, iOS a Android.

SDK pro mobilní a webové aplikace nabízí určitou sadu kontrol, které lze aplikovat na identifikované subjekty při sběru dat. Tyto kontroly zahrnují inicializaci a ovládání kamery zařízení, navedení uživatele procesem pořízení kvalitní fotografie dokladu, real-time identifikaci dokladu s paralelním zobrazením instrukcí a zpětnou vazbou, průvodce kontrolou živosti s pokyny pro interakce uživatele (např. pohled do kamery, otáčení hlavou, úsměv), plně přizpůsobitelnou integraci vizualizací a zpětné vazby, kontroly a validátory pro optimalizaci kvality snímku a jednoduchou implementaci do hostitelské aplikace. Bezpečnostní opatření SDK zajišťují, že veškerá komunikace probíhá nezávisle na Internetu, s plnou kontrolou provozovatele aplikace.

Mobilní SDK navíc podporuje ovládání osvětlení kamery pro proces ověření hologramů na dokladech totožnosti. Tato speciální funkcionalita poskytuje uživatelům mobilních zařízení pokročilé nástroje pro zajištění autenticity a bezpečnosti procesu ověřování identity.

Trask ZenID aktuálně nabízí dva **režimy zpracování výsledků získaných z mobilního SDK**: synchronní a asynchronní. V asynchronním režimu jsou výsledky po každém kroku verifikace (skenování přední/zadní strany dokladu, verifikace hologramu, ověření Selfie/Liveness) odesílány na backend ihned po dokončení pro průběžné zpracování, a nečeká se na dokončení celého procesu verifikace. Na konci procesu se odesílá poslední vzorek a předchozí výsledky jsou kombinovány do jedné investigace. Asynchronní režim nabízí zrychlení procesu verifikace. Naopak synchronní režim čeká na dokončení posledního kroku verifikace a pak najednou zpracovává a validuje všechny vzorky shromážděné mobilním SDK.

Pro účely testování a propagace jsou udržovány **DEMO aplikace** pro každé prostředí, včetně webu, iOS a Android. Tyto aplikace implementují všechny dostupné kontroly a demonstrují možnosti jejich konfigurace a vzájemného propojení, což umožňuje uživatelům efektivně využívat SDK ve svých aplikacích.

3.3 Pokrytí dokumentů v systému Trask ZenID

Termín dokumentové pokrytí zahrnuje takové pojmy jako typ dokladu, model dokladu, země a taky kontroly, které mohou být na daný doklad aplikované.

Typ dokladu odpovídá roli, kterou daný doklad plní a účel, pro který se používá.

Pod pojmem model se rozumí konkrétní verze jednoho typu dokladu, odpovídající roku vydání nové verze tohoto dokladu. Jak již bylo naznačeno v kapitole č. 2.1.2, v rámci Evropské unie se udržuje veřejně dostupný rejstřík PRADO, který obsahuje seznam všech uznaných modelů dokladů v EU a dalších zemích, včetně specifických charakteristik a bezpečnostních prvků. Tento rejstřík slouží jako hlavní důvěryhodný zdroj pro možnost základního zpracování nových modelu v rámci systému.

Zatímco přidání podpory optického rozpoznávaní znaků pro konkretní model je relativně rychlý proces, využití kontrol z komponenty pro detekci podvodu vždy bude vyžadovat robustnější přípravu a delší proces integrace. Pro dosažení spolehlivých výsledků je potřeba velká sada testovacích dat, včetně originálů dokladů a synteticky vytvořených replik.

Společnost Trask solutions je orientována zejména na trhy České republiky a Slovenska, a následně západní Evropy a v Severní Ameriky. Tomu odpovídá i dokumentové pokrytí, zejména v rámci České republiky a Slovenska je dokumentové pokrytí největší. Mimo zmíněné trhy se Trask ZenID zaměřuje i na jihovýchodní Evropu, zejména balkánský poloostrov, kde aktuálně i pro chorvatské doklady má velmi kvalitní dokumentové pokrytí pro odhalování podvodů. Přidání dalších dokladů včetně tvorby relevantní testovací sady je možné v případě projevení zájmu ze strany zákazníků.

Aktuálně systém Trask ZenID rozlišuje deset typů dokladů, které mají buď plnou, nebo omezenou podporu:

- Občanský průkaz (ID) - je oficiální doklad totožnosti, vydávaný státními úřady občanům pro potvrzení jejich identity a státní příslušnosti, obvykle s platností 10 let.
- Cestovní pas (PAS) - mezinárodně uznávaný doklad, vydávaný státními úřady, který umožňuje cestování a překročení státních hranic, obvykle s platností 5 nebo 10 let.
- Řidičský průkaz (DL) - povolení k řízení motorových vozidel, vydávané státními nebo autorizovanými institucemi po úspěšném složení příslušných zkoušek, s různou platností v závislosti na věku a typu vozidla.
- Povoleni k pobytu (RES) - dokument vydaný imigračními úřady cizím státním příslušníkům, kterým je umožněno dočasně nebo trvale žít v dané zemi, s platností obvykle od jednoho roku do několika let.
- Rodný list (BIRTH) - oficiální záznam o narození osoby, vydávaný místními úřady nebo civilními registry krátce po narození, sloužící jako základní doklad totožnosti.
- Kartička pojištěnce (EHIC) - identifikační karta vydávaná zdravotní pojišťovnou, která potvrzuje členství v pojišťovně, s obnovou podle pravidel pojišťovny.
- Vízum (VISA) - povolení vložené do cestovního pasu, vydávané zemí, do které držitel cestuje, umožňující vstup, tranzit nebo pobyt na jejím území na určitou dobu.
- Zbrojní průkaz (GUN) - oficiální povolení k držení a nošení zbraně, vydávané státními nebo autorizovanými institucemi po splnění přísných kritérií, s periodickou obnovou.
- Osvědčení o registraci vozidla (CAR) - doklad, který potvrzuje registraci motorového vozidla s nutností obnovy v případě změny vlastníka nebo údajů o vozidle.
- Karta adres (ADD) - systém evidující adresy fyzických a právnických osob, v některých zemích vydávaný ve formě kartičky, sloužící jako důkaz o registraci bydliště nebo sídla firmy.

Následující tabulka zobrazuje zjednodušený seznam pokrytí dokladů a zemí (alespoň jedna verze daného typu dokladu pro konkrétní zemi):[2]

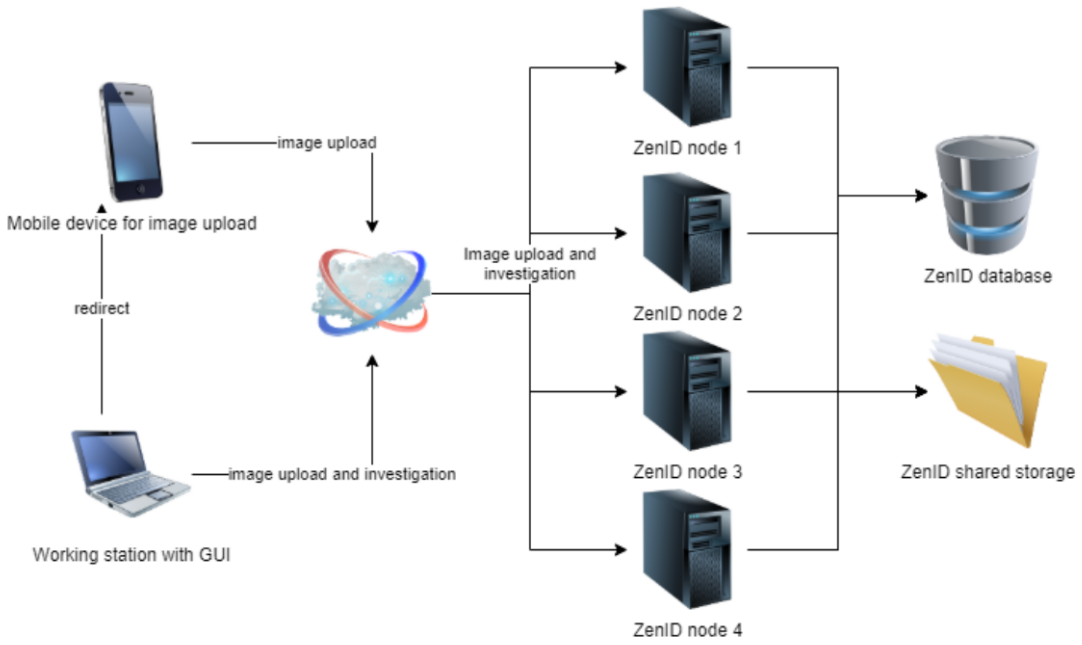
Země	Podporované doklady	Podporované moduly
Albánie	Pas	OCR
Belgie	ID, Pas	OCR
Bělorusko	Pas	OCR
Bosna a Hercegovina	ID, Pas	OCR
Bulharsko	ID, Pas	OCR
Černá Hora	Pas	OCR
Česko	ID, Pas, ŘP, Gun, Res, RL	OCR, Fraud
Dánsko	Pas	OCR
Estonsko	ID, Pas	OCR
EU	Visa, EHIC	OCR
Finsko	ID, Pas	OCR
Francie	ID, Pas	OCR
Chorvatsko	ID, Pas, ŘP	OCR, Fraud
Irsko	Pas	OCR
Island	Pas	OCR
Itálie	ID, Pas	OCR
Kypr	ID, Pas	OCR
Litva	ID, Pas	OCR
Lotyšsko	ID, Pas	OCR
Lucembursko	ID, Pas	OCR
Maďarsko	ID, Pas, ŘP, Add	OCR
Makedonie	ID, Pas	OCR
Malta	ID, Pas	OCR
Moldavsko	Pas	OCR
Německo	ID, Pas	OCR
Nizozemsko	ID, Pas	OCR
Norsko	Pas	OCR
Polsko	ID, Pas, ŘP	OCR
Portugalsko	ID, Pas	OCR
Rakousko	ID, Pas, ŘP	OCR
Rumunsko	ID, Pas	OCR
Řecko	Pas	OCR
Slovensko	ID, Pas, ŘP	OCR, Fraud
Slovinsko	ID, Pas	OCR
Spojené Království	Pas	OCR
Srbsko	Pas	OCR
Španělsko	ID, Pas	OCR
Švédsko	ID, Pas	OCR
Švýcarsko	Pas	OCR
Turecko	Pas	OCR
Ukrajina	ID, Pas, ŘP	OCR
Vietnam	Pas	OCR

Tabulka 3.2 Trask ZenID: Pokrytí dokladů a zemí

[2]Tabulka byla převzata z dokumentace Trask ZenID.

3.4 Architektura

Služba Trask ZenID je konfigurována s využitím jednoho či více uzlů propojených do klastru, umístěného ve fyzickém nebo virtuálním prostředí. Tyto uzly představují jádro systému, které bezprostředně zpracovává a validuje poskytnutá data prostřednictvím kontrol nabízených moduly a následně poskytuje výsledky. Data shromážděná od zákazníků, včetně videí a fotografií dokladů či jejich držitelů, spolu se syntetickými daty (obrazy odpovídající datovým polím na dokladech, zarovnané doklady a další podpůrné výsledky zpracování) jsou uchovávána na sdíleném souborovém úložišti. Tato data mohou být uložena buď lokálně, nebo přenesena do cloudového souborového systému. Výsledky kontrol, aplikační logy, agregovaná data a obohacené informace související s evidencemi, nastavení validatorů a údaje o profilech jsou uloženy v sdílené databázi. Další části systému tvoří rozhraní provozované společností Trask, které zajišťuje napojení na externí služby pro ověřování specifických parametrů v rámci modulů Kontrola podvodů a Tvář. Vysokoúrovňová architektura systému je znázorněná na obrázku č. 3.1. [3]



Obrázek 3.1 Trask ZenID High level Architektura

3.5 Forma provozu

Trask ZenID lze pořídit ve dvou režimech: jako SaaS nebo On-premise.

Režim SaaS, tedy software jako služba, představuje model, kde je aplikace hostována provozovatelem služby (Trask) a nabízena zákazníkům prostřednictvím Internetu. Tento model umožňuje eliminaci potřeby instalace a údržby aplikace na vlastních zařízeních zákazníků, což vede k redukci nákladů, rychlému nasazení a možnosti outsourcingu.

On-premise řešení umožňuje, aby primárním uživatelem a správcem systému Trask ZenID byl zákazník, který systém hostuje ve svém prostředí. Společnost Trask, jako vlastník produktu Trask ZenID, na základě smlouvy poskytuje API, podporu produktu a záruky služeb. Zákazník v

[3] Diagram byl převzat z dokumentace Trask ZenID.

rámci licenčních podmínek využívá jednotlivé moduly jádra Trask ZenID. Správa a konfigurace jádra systému Trask ZenID je v kompetenci zákazníka a jádro je dostupné z vnitřní sítě zákazníka.

3.5.1 Uživatelské rozhraní systému

Backendová část systému pro administrativní účely nabízí uživatelské rozhraní "Trask ZenID Admin Console", umožňující efektivní správu a konfiguraci aplikace. Toto rozhraní je strukturováno do několika záložek, z nichž pro účely této práce budou představeny pouze ty, které jsou relevantní pro další analýzu.

Přístup k rozhraní je regulován pomocí přístupových rolí, což zajišťuje, že uživatelé mohou interagovat pouze s daty a funkcemi, na které mají oprávnění.

- Rozhraní obsahuje záložku **"Samples"**, která poskytuje přehled všech nahrávaných vzorků s možnostmi zobrazení detailů jednotlivých vzorků, jejich filtrování a vyhledávání.
- **"Investigace"** přináší přehled o dokončených ověřovacích procesech dokladů, přičemž opět umožňuje vyhledávání, filtrování a prohlížení detailů každé investigace, včetně seznamu všech spuštěných kontrol a jejich výsledků.
- Záložka **"Problems"** nabízí přehled jednotlivých kontrol, které byly neúspěšné, s funkcemi pro filtrování a vyhledávání, a umožňuje také přechod k specifické investigaci, v níž byl problém identifikován.
- **"Sensitivity"** je stránka se seznamem všech implementovaných validátorů, která poskytuje možnosti jejich konfigurace.
- Konečně, záložka **"Reporting"** zahrnuje všechny možnosti, které Reporting modul nabízí.

Další možnosti nabízené v rámci uživatelského rozhraní aplikace byly v této práci záměrně vynechány.

3.6 Cenový model a licencování

Trask ZenID nabízí dva cenové modely: objemový a pásmový. Principy a výše poplatků odpovídajících těmto modelům nejsou na webových stránkách Trask ZenID zveřejněny. Na základě konzultace s manažerem projektů Trask ZenID byla sestavena tabulka, která reflektuje hlavní rozdíly mezi modely (viz tabulka č. 3.3).[4] Celková cena za řešení zahrnuje také další poplatky, které se liší v závislosti na formě provozu (SaaS nebo On-premise). Tyto rozdíly jsou uvedeny v tabulce č. 3.4.[5]

[4] Tabulka byla vytvořena na základě konzultace s vedením projektu Trask ZenID.
[5] Tabulka byla vytvořena na základě konzultace s vedením projektu Trask ZenID.

	1. Model - Objemový	2. Model - Pásmový
Vhodnost	Společnosti s dopředu známým a rovnoměrným očekávaným počtem čerpání licencí během jednoho měsíce.	Podniky, které nemají fixní očekávané čerpání licencí. Nerovnoměrná poptávka s možnými piky během roku.
Princip	Definuje se množství licencí zvlášť pro každý modul, který si zákazník pro dané období koupí.	
Cena	Pásmový princip: jednotková cena za licenci klesá na základě nakoupeného objemu.	
Zúčtovací období	1 kalendářní měsíc.	1 rok od termínu nákupu.
Přečerpávání	Pokud je smluvně povoleno, cena za čerpání licencí nad stanoveným limitem je vypočítaná na základě jejich objemu (uplatňuje se pásmový princip: za vyšší přečerpávaní jednotková cena klesá). Rozdíl se účtuje na začátku dalšího zúčtovacího období. Pokud není přečerpávání ve smlouvě povoleno, stanoví se dvoutýdenní termín pro obnovení smlouvy.	
Nevyčerpané licence	Není možné přenést do dalšího období.	

Tabulka 3.3 Srovnání objemového a pásmového licenčních modelů

	SaaS	On-premise
Cenový model	Objemový nebo Pásmový	Pouze Pásmový
Součástí subskripci jsou	Údržba	Údržba, podpora při instalaci
Povinné poplatky (měsíčně)	Azure prostředí, základní SLA 5*8, náklady spojené s provozováním serveru. [6]	
Jednorázové poplatky	Instalační poplatek, poplatek za SDK, aktivace Reporting modulu	Poplatek za SDK, aktivace Reporting modulu

Tabulka 3.4 Porovnání SaaS a On-premise subskripčních modelů

Jak vyplývá z tabulky, nezávisle na cenovém modelu zákazníci získávají určitý objem licencí, který je definován individuálně pro každý modul. Pojem licence zde odpovídá využití služby konkrétního modulu. Rozlišení mezi komponentami jednotlivých modulů slouží primárně marketingovým a obchodním účelům, aby byly možnosti systému jasné rozlišitelné (viz taky sekce č. 3.2.2). Pro licenční model však tento rozdíl není podstatný. Licence se konzumuje za využití modulu jako celku, nikoliv za jednotlivé komponenty.[7] V případě, že zákazník má aktivovány všechny komponenty modulu a využívá pouze jednu z nich, je to považováno za stejnou situaci z hlediska čerpání licencí, jako kdyby byla aktivována pouze jedna komponenta.

Pro modul OCR platí, že licence se konzumuje za zpracování jednoho dokladu (nikoli jedné strany). Pokud systém úspěšně identifikuje doklad jako předplacený (je součástí smlouvy a byl přidán do licence zákazníka v licenčním serveru), konzumuje se jedna licence. U dokladů, kde je vyžadováno nahrání dvou stran, jako jsou občanské průkazy nebo povolení k pobytu, je licence účtována za zpracování celého dokumentu skládajícího se ze dvou stran. Identifikace dokladu pro účely licencování se provádí na základě přední strany, která je povinná u všech typů dokladů.

[6] SLA 5*8 - typ dohody o úrovni služeb (SLA), která stanovuje, že poskytovatel služby se zavazuje k poskytování technické podpory během pracovních hodin, konkrétně 5 dní v týdnu a 8 hodin denně.

[7] Jakmile je licence využita (konzumována), nelze ji vrátit.

Komponenta Censor může být využívána neomezeně, pokud je součástí smlouvy, bez dalšího strhávání licencí.

Modul pro kontrolu podvodů konzumuje jednu licenci, pokud byla spuštěna investigace a to nezávisle na počtu dokladů v rámci této investigace. Podmínkou je, že v investigaci musí být aktivován alespoň jeden validátor související s kontrolou podvodů, detekcí hologramů nebo pravosti dokladu. Mezi komponentami se, stejně jako u modulu OCR, nerozlišuje.

Podobný princip platí i pro modul Tvář, kde se licence konzumuje za provolání investigace s alespoň jedním aktivním validátorem, který spadá do skupiny pro modul Tvář.

Za modul Tvorba reportů se účtuje jednorázový poplatek, který se platí po jeho aktivaci. Další poplatky nejsou účtovány.

Souhrnná tabulka s přehledem licencování modulů je uvedena na tabulce č. 3.5.[8]

Modul	Účtování	Poznámka
OCR	1 licence = 1 doklad	Licence se strhává jen v případě, že byl doklad identifikován a jedná se o předplacený doklad.
Fraud	1 licence = 1 investigace	Licence se strhává, pokud součástí investigace je alespoň jeden zapnutý Fraud validator (nebere se v potaz kompletnost dokladu)
Face	1 licence = 1 investigace	Licence se strhává, pokud součástí investigace je alespoň jeden zapnutý Face validator
Reporting	jednorázový poplatek	Poplatek je účtován při aktivaci modulu, poté bez poplatku.

Tabulka 3.5 Přehled účtování licencí pro moduly systému

Licenční poplatky za jednotlivé moduly nejsou zveřejněny na základě dohody s vedením Trask ZenID.

Další služba, která zahrnuje jednorázový poplatek, je nákup jednotlivých SDK (viz sekce č. 3.2.3). Cena za nákup SDK je významná pro účely této práce a bylo dovoleno ji publikovat po dohodě s vedením Trask ZenID (viz tabulka č. 3.6).[9] Každé SDK se prodává samostatně a zákazníci si mohou vybrat, které typy potřebují. Při nákupu více knihoven pro různé platformy se uplatňuje sleva dle přiložené tabulky. Je důležité zmínit, že za první rok je povinná údržba softwaru ze strany dodavatele, což je zaúčtováno zákazníkovi. Pro další období je údržba volitelná, což má za následek omezení přístupu k novým verzím knihoven. Proto běžnou praxí je zakoupit SDK včetně údržby, která je pak obnovována na začátku dalšího účtovacího období.

Množství	1 SDK	2 SDKs	3 SDKs	Údržba
Cena	250 tis. Kč	400 tis. Kč	500 tis. Kč	20% od částky[10]

Tabulka 3.6 Ceník SDK a Údržby

[8] Tabulka byla vytvořena na základě konzultace s vedením projektu Trask ZenID.

[9] Tabulka byla vytvořena na základě konzultace s vedením projektu Trask ZenID.

[10] Částka ve výši 20% představuje dodatečný poplatek, který je aplikován na cenu pořízení jednoho SDK nebo zvýhodněného balíčku obsahujícího více SDKs.

3.7 Analýza splnění požadavků dle obecných pokynů EBA

Jak již bylo nastíněno v předcházející sekci č. 3.1, platforma Trask ZenID poskytuje své služby klientům z různých sektorů, ve kterých se uplatňuje identifikace. Speciální důraz je kladen na bankovní a úvěrové instituce, které vyžadují vysokou úroveň důvěry od řešení zajišťujícího identifikaci. Jak bylo diskutováno v sekci č. 2.4.2, v případě outsourcingu jsou požadavky považovány za splněné, pokud třetí strana poskytne vysokou či dostatečnou úroveň důvěryhodnosti a prokáže to příslušným potvrzením, bez nutnosti dalšího zkoumání. Vzhledem k tomu, že v případě systému Trask ZenID odpovědnost za hodnocení spolehlivosti tohoto řešení při jeho implementaci a začlenění do interních systémů nese samotný odběratel (viz také závěr kapitoly č. 2.1.3), bylo rozhodnuto provést revizi požadavků a doporučení vydávaných EBA a zhodnotit, do jaké míry Trask ZenID tyto požadavky splňuje. Cílem analýzy je poskytnout další předpoklady pro rozhodování o vhodnosti integraci zpracování digitálních dokladu do stávajícího systému. Jak je vidět z popisu systému v sekci č. 3.2, Trask ZenID přímo nepodporuje proces Iniciace a Vydání potvrzení, jak je to popsané v části č. 2.2. Vzhledem k tomu analýza se primárně zaměřuje na procesy "Sběr důkazů a atributů", "Validace dat", a "Vazba a verifikace". Splnění jednotlivých požadavků na tyto fáze systémem Trask ZenID je ilustrováno v tabulkách č. 3.9, 3.8, a 3.7.[11]

Požadavky kladené na proces sběru důkazů a atributů		**Trask ZenID Realizace**
RQ1	**Aktuálnost dat:** zajištění, že data získaná od klienta jsou aktuální, což znamená, že odrážejí nejnovější dostupné informace o klientovi v čase ověřování.	Systém je možné integrovat s externími registry za účelem ověření platnosti poskytnutých dokumentů. Identifikace provedená v reálném čase prostřednictvím SDK zajistí, že data byla shromážděna v momentě průchodu identifikačním procesem. (viz sekce č. 3.2.3, 3.2.2)
RQ2	**Dostatečnost dat:** data získaná od klienta musí být dostatečná pro účely ověření identity, což zahrnuje množství a typ dokladů a informací potřebných k úspěšnému procesu ověření.	Podle nařízení ČNB při vzdálené identifikaci je vyžadováno předložení dvou dokladů totožnosti (viz sekce č. 2.4.3). Trask ZenID podporuje ověření a extrakci nezbytných informací u všech dokladů totožnosti akceptovaných v České republice a většiny mezinárodně uznávaných dokumentů (viz sekce č. 3.3).
RQ3	**Čitelnost dat:** data musí být čitelná pro možnost následného ověření, což zahrnuje jasnost a srozumitelnost informací poskytnutých klientem, jejích uchování ve zpracovatelné podobě.	Analýza kvality obrázku v rámci SDK a backendu zajišťuje, že nic nebrání extrakci dat (Kontrola DPI, zaostření, odlesky, atd.). (viz sekce č. 3.2.2) Extrahovaná data jsou doplněna k původnímu obrazu a strukturovaně uložena ve zpracovatelné formě do databáze. Extrahovaná data jsou doplněná k původnímu obrázku a strukturovaně uložená ve zpracovatelné podobě do DB (viz sekce č. 3.4).

Pokračování na další straně

[11] Tabulky byly vytvořeny autorem na základě dokumentace Trask ZenID a konzultací s vedením projektu.

– pokračování na předchozí straně

Požadavky kladené na proces sběru důkazů a atributů		Trask ZenID Realizace
RQ4	**Bezpečnost uchovávání dat:** zajištění bezpečnosti uchovávání dat získaných od klientů, včetně ochrany před neoprávněným přístupem a zneužitím.	Přístup k datům je řízen pomocí přístupových práv definovaných pro různé uživatelské role v systému. Klienti mohou propojit své Active Directory (AD) skupiny s konkrétními rolemi pro správu přístupu. Všechny manipulace s daty a jejich prohlížení jsou zaznamenány, což umožňuje sledování auditní stopy (viz sekce č. 3.5.1).
RQ5	**Okolní podmínky během sběru dat:** data jsou pořizována za vhodných podmínek během sběru důkazů pro zajištění jejich kvality a jednoznačnosti.	SDK poskytuje vizualizace během procesu identifikace a zahrnuje kvalitativní validátory (ostření, světelné podmínky, odlesky, zarovnání), které zabraňují pořízení nekvalitních fotografií. Tyto kvalitativní kontroly jsou aplikovány také na backendové straně (viz sekce č. 3.2.3).
RQ6	**Časování pořízení dat:** zajištění, že data byla pořízena v době provedení ověření, aby byla relevantní a aktuální.	SDK umožňuje identifikaci dokumentu v reálném čase, čímž zajišťuje jejich aktuálnost. K dispozici jsou také další kontroly pro ověření aktuálnosti konkrétních informací, jako je Validátor podpisu SDK, Ověření metadat repliky a Aktivní ověření živosti (viz sekce č. 3.2.3, 3.2.2).
RQ7	**Doba uchování dat:** data mají jasně definovanou dobu uchování, po kterou musí být zachována pro případnou revizi nebo audit. Po termínu mají byt ze systému smazána.	Na úrovni celého systému a specifických profilů je možné nastavit dobu uchování vzorků. Data starší než nastavená doba budou ze systému automaticky odstraněna.

Tabulka 3.7 Realizace požadavků spojených s procesem sběru důkazů a atributů v systému Trask ZenID

Požadavky kladené na proces validace dat		Trask ZenID Realizace
RQ8	**Bezpečnostní prvky na dokladu:** ověření, že předložená kopie dokladu totožnosti obsahuje bezpečnostní prvky vložené do původního dokladu.	Implementovány jsou validátory pro Ověření bezpečnostních prvků a křížové kontroly, Ověření integrity. Mezi konkrétní ověřované prvky patří hologramy, barkódy, strojově čitelné zóny (MRZ), identifikační čísla, RČ a vestavěné fotografie u vybraných modelů dokumentů (viz sekce č. 3.2.2).

Pokračování na další straně

– pokračování na předchozí straně

Požadavky kladené na proces validace dat		Trask ZenID Realizace
RQ9	**Dodržení specifikací modelu dokladu**: ověření, že předložená kopie dokladu dodržuje specifikace (typ, velikost znaků, struktura) kladené na původní doklad.	Zajištěno validátory pro Ověření bezpečnostních prvků a křížové kontroly, Ověření integrity. Konkretně se kontroluje kompletnost dokladu, vzhled písma, mezery, zarovnání, přítomnost fotky, její barva (viz sekce č. 3.2.2).
RQ10	**Absence zásahu:** předložená kopie dokladu nesmí obsahovat viditelných příznaků zásahu a manipulace s osobními údaji a fotografií držitele.	Zajištěno modulem Kontrola podvodu. Konkretně se kontroluje manipulace s poličky, jestli se jedná o obrazovku nebo papír, kontrolují se podezřelé artefakty na dokladu (viz sekce č. 3.2.2).
RQ11	**Integrita algoritmu pro generování ID:** zajištění integrity algoritmu použitého pro generování jedinečného identifikačního čísla.	Zajištěno validátorem Kontrola validity identifikačního čísla na dokladu (viz sekce č. 3.2.2).
RQ12	**Kvalita a rozlišení:** ověření dostatečné kvality a rozlišení předložené kopie dokladu totožnosti.	Zajištěno validátory DPI a zaostření, Ověření odlesků na fotografii, OCR.
RQ13	**Původ dokladu:** zkoumání, zda se jedná o reprodukci poskytnutou vyfocením obrazovky, tištěné kopie, nebo skenu.	Validátor Obrazovka nebo Papír (viz sekce č. 3.2.2).
RQ14	**Přesnost a konzistence automatizovaného čtení:** zajištění přesnost a konzistenci funkcí pro automatické čtení informací z dokladu, pokud je použito.	Validátor OCR - kontrola správnosti přepisu údajů (viz sekce č. 3.2.2).
RQ15	**Ověření informací z čipů:** ověření souladu informací získaných z vestavěných čipů, s daty z jiných zdrojů, pokud je to technicky možné.	Není implementováno.
RQ16	**Ověření pravosti bezpečnostních prvků na dokladu:** ověření pravosti bezpečnostních prvků použitých na dokladu vůči jejich známým a ověřitelným charakteristikám.	Probíhá ověření Čárového kódu, MRZ, Hologramu, ID, RČ, vestavěné fotky u vybraných modelů (viz sekce č. 3.2.2, 3.2.2).

Tabulka 3.8 Realizace požadavků spojených s procesem validace dat v systému Trask ZenID

Požadavky kladené na proces vazby a verifikace		Trask ZenID Realizace
RQ17	**Shoda s fyzickou osobou:** zajistit ověření shody mezi viditelnými informacemi o fyzické osobě a poskytnutou dokumentací.	Zajištěno validátory Přítomnost Selfie, Tvář na Fotografii, Párování Selfie (viz sekce č. 3.2.2).

Pokračování na další straně

– pokračování na předchozí straně

Požadavky kladené na proces vazby a verifikace		**Trask ZenID Realizace**
RQ18	**Spolehlivost při ověření shody:** použít odolné a spolehlivé algoritmy k ověření shody mezi biometrickými údaji v dokladu a klientem.	Použití Microsoft Cognitive Services (viz sekce č. 3.2.2).
RQ19	**Doplňkové kontroly při nedostatečné důvěře:** Pokud není zajištěná požadovaná úroveň důvěry, musejí být uplatněny další kontroly.	Komponenta pro Ověření Živosti, v kombinaci s proprietárním SDK, realizuje Aktivní a Pasivní ověření živosti, pořízení videozáznamů a nabízí možnost integrace na vyžádaní s externími službami pro sekundární ověření získaných dat (viz sekce č. 3.2.2, 3.2.3).
RQ20	**Detekce živosti:** provádět ověření detekce živosti pro ověření, že klient je přítomen v komunikační relaci, a to pomocí vyžádání k provedení akcí od klienta (aktivní ověření) nebo pomocí analýzy přijatých dat, které nevyžadují konkrétní akci (pasivní ověření).	Realizováno komponentou Ověření Živosti v kombinaci s proprietárním SDK (viz sekce č. 3.2.3, 3.2.2).
RQ21	**Náhodnost v posloupnosti úkonů:** zajistit náhodnost v posloupnosti úkonů během detekce živosti, pokud je to možné.	Zajištěno (viz sekce č. 3.2.3, 3.2.2).

Tabulka 3.9 Realizace požadavků spojených s procesem vazby a verifikace v systému Trask ZenID

Jak vyplývá z uvedených tabulek, platforma Trask ZenID podporuje většinu zmíněných požadavků v různé míře. Nicméně, zvláštní pozornost je vyžadována u požadavků č. RQ8 na bezpečnostní prvky v reprodukci, RQ15 na ověření informací z čipů, RQ16 na ověření pravosti bezpečnostních prvků na dokladech a RQ19 na doplňkové kontroly při nedostatečné důvěře.

Požadavky RQ8 a RQ16 se zaměřují na detekci a ověření bezpečnostních prvků. Analýza možností systému (viz sekce č. 3.2.2) ukázala, že Trask ZenID ověřuje některé bezpečnostní charakteristiky, avšak seznam není vyčerpávající, což by mohlo znamenat další možnosti integrace pro zvýšení důvěryhodnosti a bezpečnosti systému. Pro identifikaci konkrétních možnosti byla provedena základní kontrola bezpečnostních prvků uvedených v rejstříku PRADO (viz sekci č. 3.8).

Požadavek RQ15 přesně odpovídá aktuálnímu záměru společnosti ohledně integrace zpracování digitálních dokladů totožnosti. Ačkoli tento požadavek není povinný, může přispět k zvýšení bezpečnosti díky možnosti načítání a ověření čipů integrovaných do dokladů. Tuto funkci Trask ZenID aktuálně nepodporuje, přestože 84% poskytovatelů vzdálené identifikace nabízí extrakci dat z čipů, jak uvádí zpráva společnosti Gartner [18]. Tato funkcionalita by vyžadovala přiměřené náklady na implementaci, jelikož nepředpokládá zdlouhavé vytváření testovacích sad a trénovaní neuronových sítí. Vzhledem k tomu je považována za klíčovou pro udržení konkurenceschopnosti a zvýšení bezpečnosti Trask ZenID.

RQ19, Doplňkové kontroly při nedostatečné důvěře, nespecifikuje metody, které by mohly být využity k zvýšení bezpečnosti. V Trask ZenID jsou dostupné některé standardní kontroly, pokrývající minimální rozsah požadavků. Jako možná kontrola bylo zmíněno ověření živosti (viz sekce č. 3.2.2). Pro určení možností rozšíření Trask ZenID o další kontroly byla provedena povrchní analýza přímých konkurentů Trask ZenID (viz sekce č. 3.9).

Z provedené analýzy splnění požadavků vyplynulo, že existují specifické aspekty, které by mohly v budoucnu přispět k rozvoji a zdokonalení produktu Trask ZenID. V rámci dalšího rozvoje této práce bude důležité podrobněji se věnovat těmto požadavkům. Navazující analýza bude zaměřena na zkoumání bezpečnostních prvků obsažených na dokladech totožnosti a možnosti jejich zpracování, což poskytne hlubší porozumění požadavkům RQ8, RQ15 a RQ16 (viz sekce č. 3.8). Současně bude provedeno srovnání Trask ZenID s obdobnými konkurenčními řešeními, aby bylo možné prakticky pochopit, jakým směrem by se měl produkt ubírat pro zajištění nejvyššího možného standardu bezpečnosti a uživatelské spokojenosti vzhledem k požadavku RQ19 (viz sekce č. 3.9).

3.8 Přehled bezpečnostních prvků

Za účelem posouzení splnění požadavků RQ8, RQ15 a RQ16, zaměřených dle popisu v sekci č. 3.7 na detekci a ověření bezpečnostních prvků, byla provedena analýza databáze PRADO [7]. Tato část kapitoly hodnotí, zda by měly být před integrací zpracování digitálních dokladů implementovány další bezpečnostní prvky. Hlavním zdrojem pro analýzu byl Glosář PRADO, sloužící jako komplexní referenční zdroj pro termíny používané v databázi, organizovaný abecedně s četnými křížovými odkazy. Glosář obsahuje termíny týkající se vytváření a ověřování ID dokumentů a zahrnuje i další zařízení, metody či databáze [19].

Seznam bezpečnostních prvků pro nejběžnější české identifikační dokumenty (pas a občanský průkaz) byl vytvořen extrakcí informací z PRADO a doplněním prvků odvozených z viditelných charakteristik dokumentů. Uvedený seznam, který nemusí být vyčerpávající, je dostupný jako Excel soubor v podpůrných materiálech práce (viz soubor ”Analýza PRADO.xlsx”v elektronické příloze práce).

Vytvořená tabulka prezentuje seznam bezpečnostních prvků rozdělených do identifikovaných kategorií. Tabulka také poskytuje informace o tom, zda Trask ZenID aktuálně detekuje/ověřuje daný prvek, požadované vybavení pro detekci bezpečnostního prvku a důvody pro částečnou detekci/ověření (podrobnější informace o struktuře a popisu souboru jsou uvedené v příloze A).

Na základě analýzy byly bezpečnostní prvky rozdělené do sedmi hlavních kategorií, které lze dále dělit na podkategorie. Tyto kategorie se někdy překrývají, jako například strojově ověřitelné prvky implementované do dokladu různými technikami.

3.8.1 Kategorie bezpečnostních prvků

- Prvky ověřitelné strojem: klíčová kategorie pro potenciální implementaci. Do této kategorie například spadají proměnlivé laserové obrazy, Kinegramy, fluorescenční přetisky, bezkontaktní a kontaktní čipy.
- Pozadí/Bezpečnostní tisk: prvky, které tvoří pozadí dokladů nebo ovlivňují jeho barvení a bezpečnostní texty.
- Personalizace: techniky pro integraci osobních údajů do dokladů. Tyto informace jsou systémem Trask ZenID ověřovány bez ohledu na metodu integrace.
- Číslování: metody pro identifikaci dokumentu.
- Tiskové techniky: přístupy pro přenos textu na dokument. Pro ověření se systémem Trask ZenID používá OCR, ale neprobíhá hodnocení metody integrace.
- UV prvky: prvky viditelné pod UV světlem.
- Ostatní: zahrnuje různé barvy, perforace, šicí nitě.

Vzhledem k tomu, že Trask ZenID neplánuje další integraci zařízení a přístrojů pro podporu procesu identifikace, prvky, které mohou být detekované a zpracované za využití speciálního podpůrného zařízení nebo světla (viz sloupce "Ligth"a "Special HW") jsou mimo aktuální dosah, jelikož telefon a jeho kamera s osvětlením jsou pro tyto účely nedostatečné.

Z analýzy vyplývá, že pro další rozvoj a zvýšení bezpečnosti procesu identifikace je vhodné investovat do vývoje a implementace technologií umožňujících vzdálené čtení dat z bezkontaktních čipů prostřednictvím technologie NFC (Near Field Communication) přímo mobilními zařízeními držitelů dokladů. Tento závěr je podpořen faktem, že mnoho klíčových bezpečnostních prvků již bylo implementováno nebo jejich implementace vyžaduje speciální vybavení, což je mimo dosah běžného uživatele. Před návrhem integrace této technologie do stávajících procesů Trask ZenID bylo rozhodnuto provést také analýzu konkurenčních řešení pro posouzení dalších metod a technik, které by bylo možné využít pro rozšíření procesu vzdálené identifikace (viz sekce č. 3.9).

3.9 Srovnaní Trask ZenID vůči konkurenci

Za účelem vyhodnocení požadavku RQ19 (viz sekce č. 3.7) je v této sekci věnována pozornost srovnávací analýze dodavatelů řešení pro online verifikaci identity. Cílem je identifikovat inovativní technologie a metody, které by mohly být začleněny do produktu Trask ZenID. Tato analýza se opírá o průzkum zahrnující mezinárodně uznávané dodavatele zmíněné v reportu společnosti Gartner a konkurenční řešení operující na českém trhu: Daon, Inverid, Jumio, Innovatrics, Zentity, Wultra a iProov [20].

Přestože zkoumané platformy adresují podobné výzvy v kontextu identifikačních procesů, činí tak někdy za využití různých technologií. Analýza je zaměřena na odhalení specifických prvků a metod aplikovatelných pro implementaci do Trask ZenID, s ohledem na optimalizaci nákladů a časových investic potřebných k udržení konkurenceschopnosti.

Analýza se zaměřila na porovnání podporovaných funkcí a metod určených pro identifikaci klientů (specificky extrakce dat, detekce podvodů a ověřování autenticity dokladů, analyzované bezpečnostní prvky, provedené křížové kontroly), technologií použitých pro biometrické ověřování, a celkově přístupů k biometrické verifikaci.

Následuje podrobnější pohled na jednotlivé dodavatele a unikátní charakteristiky jejich řešení.

- **Daon** poskytuje rozšířené ověřovací služby, včetně verifikace vodních znaků a pečetí na identifikačních dokladech. V rámci procesů detekce živosti vyžaduje Daon interakci subjektu s identifikačním dokladem, doplňuje to o hlasovou verifikaci a autenticitu, včetně analýzy zorniček [21].
- **Jumio** se vyznačuje pokročilou detekcí mikroprintů, ghost images a perforací na identifikačních dokladech (viz více v sekci č. 3.8). Jumio také implementuje inovativní techniku pro ověřování živosti, která vyžaduje od uživatelů, aby předvedli svůj doklad a obličej před kamerou, a zároveň nabízí možnost další kontroly prostřednictvím svého backoffice. Tato funkce poskytuje dvojí ověření, kde software prvně analyzuje a poté umožňuje lidským operátorům provést finální verifikaci, čímž zvyšuje celkovou spolehlivost a bezpečnost procesu [22].
- **Veridas** se vyznačuje především díky svému pokročilému hlasovému rozpoznávání. Tato technologie umožňuje verifikaci identity prostřednictvím analýzy hlasových vzorků, což představuje bezkontaktní a nenáročnou metodu pro koncového uživatele. Hlasové rozpoznávání od Veridas tak přidává další vrstvu biometrické bezpečnosti, která může být užitečná v různých aplikačních scénářích, od finančních služeb až po kontrolu přístupu [23].
- **Innovatrics** přináší inovace v oblasti detekce živosti s technologií MagnifEye, která vyzývá uživatele, aby zaměřili kameru na své oko, a tím ověřili svou přítomnost. Přestože původní

technologie EyeGaze, vyzývající uživatele sledovat bod na obrazovce svými očima, byla v současnosti vyřazena z nabídky, MagnifEye představuje významný krok vpřed v metodách ověřování skutečné přítomnosti uživatele [24].

Kromě těchto specifických technologických aspektů, všichni dodavatelé s výjimkou **Zentity** nabízejí možnost extrakce dat z digitálních dokladů totožnosti prostřednictvím načtení bezkontaktních čipů za využití NFC technologie (více o digitálních dokladech a NFC je uvedeno v sekci č. 4.1.3) [25]. Tato vlastnost je zásadní pro moderní řešení ověřování identity, umožňující rychlou a bezpečnou verifikaci dat uložených na čipech v pasu nebo občanském průkazu.

Inverid se vymyká jako společnost specializující se primárně na extrakci a validaci dat z bezkontaktních čipů. Toto zaměření činí Inverid jedinečným hráčem na trhu, poskytujícím vysokou úroveň odbornosti a inovací v této oblasti. Inverid svými službami pokrývá klíčovou potřebu trhu pro rychlou a bezpečnou autentizaci a ověření identity, což má zásadní význam pro široké spektrum aplikací, od bankovnictví po vládní služby [26].

Na základě provedené analýzy konkurenčních řešení lze odvodit, že pro udržení konkurenceschopnosti v oblasti vzdálené identifikace integrace a zpracování digitálních dokladů totožnosti za využití NFC technologie se jeví jako nejlepší možnost.

V rámci této kapitoly byla provedena rozsáhlá analýza řešení Trask ZenID, která zdůraznila jeho schopnosti, zaměření a podporované funkcionality v oblasti identifikace klientů. Na základě této analýzy bylo zjištěno, že systém splňuje většinu požadavků definovaných dle doporučení EBA. Přesto existují oblasti, kde by další rozvoj mohl výrazně přispět k zvýšení bezpečnosti a konkurenceschopnosti systému. Jedná se zejména o omezené zpracování bezpečnostních prvků na identifikačních dokladech, a také o schopnost provádět pokročilejší podpůrné kontroly vzdálené identifikace.

Analýza rejstříku PRADO ukázala, že mezi neověřovanými bezpečnostními prvky systémem Trask ZenID se vymyká zejména bezkontaktní čip, který je vestavěn do digitálních dokladů totožnosti. Tento prvek je zvláště významný, jelikož nevyžaduje dodatečné vybavení kromě mobilního telefonu pro jeho zpracování, což potvrzuje smysluplnost jeho implementace.

Následná analýza konkurence potvrdila, že strategie integrace zpracování digitálních dokladů totožnosti prostřednictvím technologie NFC je vhodná. Implementace této technologie by umožnila Trask ZenID udržet konkurenceschopnost, jelikož zkoumané společnosti již tuto kontrolu podporují. Na základě těchto zjištění lze konstatovat, že zvolená iniciativa je správná a přispěje k rozvoji projektu při přijatelném poměru cena - přínos. Tato zjištění poskytují pevný základ pro přechod k další fázi projektu, kterou bude vytvoření business case[12] pro danou iniciativu a posouzení její proveditelnosti.

[12]Po konzultaci s vedoucím práce bylo dohodnuto, že výraz "business case"bude ve všech případech uváděn v základní anglické formě a nebude skloňován.

Kapitola 4
Business case

Před podrobným technickým návrhem integrace zpracování digitálních dokladů totožnosti (viz navazující kapitola č. 5) bude definován pouze základní koncept začlenění této iniciativy do existujících procesů systému Trask ZenID. Výstupy této části následně budou použité v této kapitole pro vytvoření business case projektu, zahrnující přípravu projektového plánu, odhad nákladů a hodnocení návratnosti investic. Tyto údaje budou klíčové pro rozhodnutí společnosti o spuštění integrace. Kapitola obecně stanovuje rámec pro pochopení základních integračních, regulačních a ekonomických faktorů spojených s implementací zpracování digitálních dokladů totožnosti.

4.1 Úvod do NFC technologie a digitálních dokladů

Před popisem NFC technologie a jejím využitím v kontextu ověřování identity je nezbytné provést vymezení existujících typů dokladů pro pochopení, které z nich mohou být pomocí této technologie zpracované. V předchozí části byla provedena kategorizace dokladů s ohledem na jejich využití a obsažené informace (viz sekce č. 3.3), zatímco zde je kategorizace uvažována z pohledu formy uchování, distribuce a přístupu k informacím.

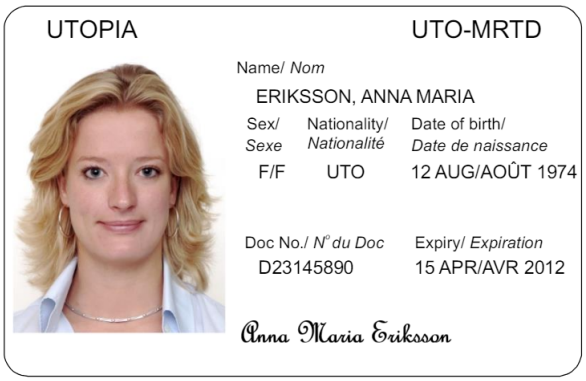
Doklady totožnosti se dělí do dvou základních kategorií: fyzické a digitální.

4.1.1 Fyzické doklady

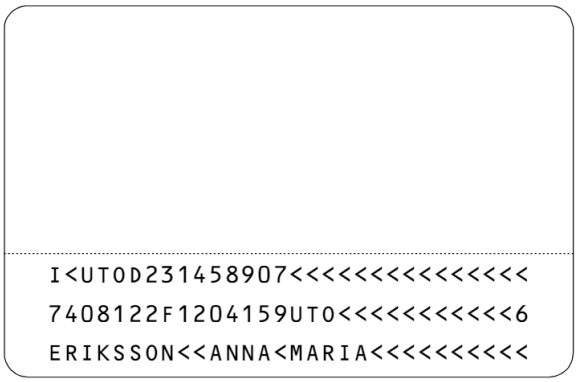
Fyzické doklady totožnosti, tradiční dokumenty tištěné na papíře nebo jiných materiálech, umožňují fyzické přenášení a obsahují nezbytné informace pro identifikaci osoby, která doklad předkládá. Mezi nejrozšířenější typy patří občanský průkaz, cestovní doklad, řidičský průkaz a průkaz pojištěnce [27].

Fyzické doklady, které jsou opatřeny strojově čitelnou zónou (MRZ), je možné rozdělit do tří skupin podle viditelných charakteristik a umístění informací v rámci dokladu, včetně MRZ.

První skupinou jsou doklady ve **formátu TD1** (viz obrázky č. 4.1, 4.2). Tyto doklady mají na přední straně osobní informace držitele, zatímco zadní strana je opatřena MRZ, obsahující tří řádky. Umístění osobních údajů na přední straně se může lišit v závislosti na vydávajícím státu. Zadní strana, kromě MRZ, může obsahovat další nepovinné informace umístěné na prázdném místě. Umístění a formát MRZ zóny však zůstává neměnný. Typickými příklady TD1 jsou běžné průkazy totožnosti nebo kartičky pojištěnce široce používané v různých státech, včetně České republiky a Slovenska. Doklady typu TD1 jsou obecně známé jako MROTDs (zkratka od anglického „Machine Readable Official Travel Documents“) [28].

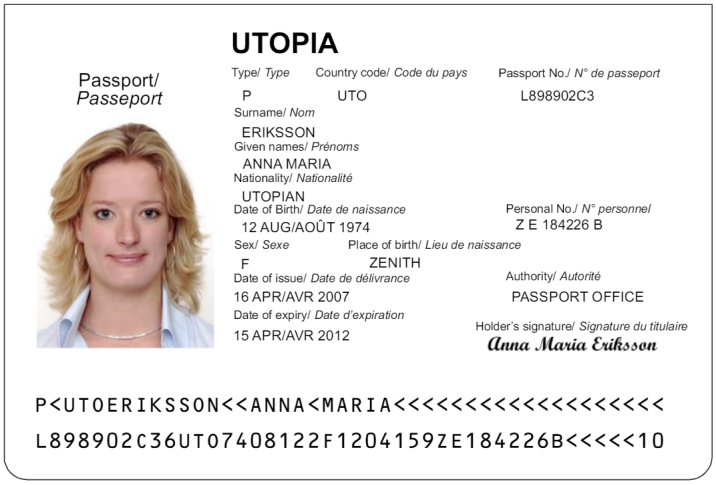


Obrázek 4.1 Přední strana MROTD velikosti TD1, převzato z ICAO 9303, Část 5. [28]



Obrázek 4.2 Zadní strana MROTD velikosti TD1, převzato z ICAO 9303, Část 5. [28]

Obrázek 4.3 Typické uspořádání MROTD velikosti TD2, převzato z ICAO 9303, Část 6. [29]



Obrázek 4.4 Typické uspořádání MRP velikosti TD3, převzato z ICAO 9303, Část 4. [30]

Dalším typem jsou doklady ve **formátu TD2** (viz obrázek č. 4.3), kde je MRZ umístěna přímo na přední straně dokladu do dvou řádků. Tyto doklady jsou předchůdci TD1 a v současné době nejsou tak rozšířené. Doklady typu TD2 jsou také označovány jako MROTDs [29].

Posledním typem jsou dokumenty ve **formátu TD3** (viz obrázek č. 4.4), které obsahují personalizované informace o držiteli obvykle vložené do knížky cestovního pasu. MRZ zóna je umístěna na přední straně do dvou řádků. Další informace o držiteli mohou být umístěny různě, v různých formátech, v závislosti na státu vydání. Doklady typu TD3 jsou běžně nazývány MRTDs (zkratka od anglického „Machine Readable Travel Documents“) nebo MRPs (zkratka od anglického „Machine Readable Passports“) [30].

4.1.2 Digitální doklady

Digitální (nebo také elektronické) doklady totožnosti představují elektronické ekvivalenty fyzických dokladů, které jsou uznané státními orgány pro účely identifikace na dálku. Tyto dokumenty existují ve formě digitálních záznamů, běžně přístupných prostřednictvím specializovaných

aplikací nebo systémů [31]. Jako příklady mohou sloužit digitální kopie dokladů uložené v mobilních zařízeních nebo fyzické doklady obsahující strojově čitelné prvky (čárové kódy, vestavěné kontaktní a bezkontaktní čipy), které uchovávají klíčové informace příslušné držiteli dokladu, obvykle zabezpečené kvalifikovaným elektronickým podpisem pro zajištění jejich integrity [32].

Digitální doklady slouží k prokazování totožnosti ve světě informačních systémů a Internetu. S použitím digitálních dokladů se rozvíjí pojem digitální nebo elektronická identita, což představuje sadu vlastností existujících v elektronické podobě, které slouží k jednoznačnému určení konkrétní osoby [33].

Nejrozšířenějším a nejpoužívanějším příkladem elektronického dokladu je například česká eObčanka, což je průkaz totožnosti se strojově čitelnými údaji a čipem [33].

V obecnějším kontextu lze k výše popsaným typům dokladů TD1, TD2, TD3 přidat čip obsahující digitální identifikační informace o držiteli, čímž vznikají elektronické (digitální) doklady totožnosti. Tyto doklady budou mít názvy eMROTD, eMRTD, eMRP, což jsou elektronické ekvivalenty formátů TD1, TD2 a TD3, kde předpona „e“ značí „elektronický“.

4.1.3 NFC technologie a RFID čipy

Čipy vestavěné do definovaných dokladů totožnosti se dělí na **kontaktní** a **bezkontaktní**, v závislosti na typu komunikace a způsobu předání informace. Kontaktní čipy vyžadují přímý fyzický kontakt s čtečkou, zatímco bezkontaktní fungují na malé vzdálenosti bez přímého kontaktu. Pro čtení dat z kontaktního čipu je nutné, aby byl doklad, například karta s čipem, vložen do slotu čtečky vybavené kontaktními piny kompatibilními s kontakty na čipu. Po fyzickém spojení je čip aktivován čtečkou, která z něj může číst nebo do něj zapisovat data. Bezkontaktní čipy využívají technologii RFID pro bezkontaktní přenos informací.

Obecně technologie RFID (z anglického ”Radio-Frequency Identification”) využívá rádiové frekvence pro identifikaci objektů, na které jsou připevněny RFID štítky obsahující elektronicky uložené informace. Tato technologie je využívána pro automatizovanou identifikaci a je také klíčová pro bezpečnostní aplikace, jako jsou biometrické pasy a bezkontaktní vstupní systémy, což usnadňuje ověřování identity [34]. Čipy v dokladech totožnosti obvykle používají pasivní RFID, což znamená, že uložené údaje jsou určeny výhradně ke čtení. Čip obsahuje anténu, která přenáší data na vysoké frekvenci [35]. Každý čip eMRTD vysílá rádiové vlny, ale používá komunikaci v blízkém poli, vyžadující těsný kontakt pro odeslání signálů na rozdíl od čistých RFID zařízení, která pracují na vzdálenost od 25 do 100 metrů. Při provádění čtecí operace z čipu eMRTD by měla být čtečka držena co nejblíže k dokladu, aby byla umožněna komunikace peer-to-peer [36].

Samostatná čtečka, umožňující přístup a čtení dat z bezkontaktních čipů, využívá technologii NFC (z anglického ”Near Field Communication”). Tato technologie umožňuje bezdrátovou komunikaci na krátké vzdálenosti, typicky do 4 cm. Za využití NFC dvě zařízení, jako jsou chytré telefony, platební karty a čtečky, mohou bezpečně si mezi sebou vyměňovat informace prostřednictvím jednoduchého přiblížení. NFC je široce využívána v mobilních platebních systémech a také pro bezpečné sdílení klíčů při autentizaci identity v rámci kontrolních a přístupových systému [37]. NFC technologie, která pracuje na stejné frekvenci jako RFID, ale s omezením na krátký dosah čtení, je běžně integrována do moderních mobilních telefonů, což otevírá možnosti pro její využití nejen na pobočkách za použití speciálních zařízení, ale i pro běžné využití během identifikace na dálku obyčejnými lidmi.

Využití digitálních dokladů totožnosti v praxi

V období 2005 až 2006 bylo zahájeno vydávání biometrických pasů, které integrují čipy pro uchování biometrických dat. Tento proces byl iniciálně podpořen Mezinárodní organizací pro civilní letectví (ICAO) v roce 2003, kdy byl přijat plán pro implementaci těchto strojově čitelných

cestovních dokladů s RFID čipy za účelem zlepšení bezpečnosti a efektivity hraničních kontrol. Projekt si získal podporu 188 států a mnohé z nich, včetně Spojených států a států Evropské unie, začaly tyto pasy vydávat krátce poté. Ve Spojených státech bylo od roku 2007 zakázáno vydávat pasy bez integrovaného čipu [38]. Dle zprávy společnosti Inverid publikované v prosinci 2023, v současnosti vydává biometrické pasy 177 zemí a očekává se, že jejich počet bude nadále růst v důsledku globalizace a standardizace pravidel [26].

Pokud jde o integraci čipů do dalších typů dokladů, jako jsou občanské průkazy nebo povolení k pobytu, načasování se v různých zemích liší. Evropská unie například krok za krokem zavádí biometrické prvky do různých identifikačních dokladů po úspěšném přijetí biometrických pasů.

V České republice byl zahájen proces vydávání elektronických pasů v roce 2006 [39]. Pasy vydané před tímto datem již ztratily svou platnost, což znamená, že nyní jsou v oběhu pouze elektronické pasy [7].

Podle statistik Ministerstva vnitra ČR, zveřejněných na jejich webu, výroba občanských průkazů s integrovanými kontaktními čipy začala v roce 2012. Od roku 2019 jsou vydávány výhradně občanské průkazy s čipy, a od roku 2021 - výhradně s bezkontaktními čipy [40].

4.1.4 ICAO - klíčová role ve vývoji online identifikace

V kontextu vzdálené identifikace a ověřování prostřednictvím bezkontaktních čipů je klíčové dodržování standardů, které zajistí bezproblémovou identifikaci napříč různými státy. Tato sekce se proto bude věnovat seznámení s Mezinárodní organizací pro civilní letectví (ICAO), která tyto standardy zastřešuje. ICAO hraje klíčovou roli v oblasti identifikace na dálku. Přestože přímé zapojení ICAO v online identifikaci je omezené, její normy mají významný vliv na ověřovací procesy digitální identity, především skrze regulaci vydání cestovních dokladů. Organizace se primárně soustředí na standardizaci procedur a dokumentace v mezinárodním civilním letectví. K tomuto účelu byl vydán Dokument 9303 ICAO, který definuje specifikace pro strojově čitelné cestovní doklady. Tento standard byl poprvé publikován v roce 1980 a od té doby byl několikrát aktualizován za účelem integrace nejnovějších bezpečnostních technologií a norem. Nejaktuálnější, osmé vydání, bylo vydáno v roce 2021. Aktualizace se zaměřuje na standardizaci elektronických pasů a dalších cestovních dokladů. Tyto dokumenty musí splňovat globální bezpečnostní a interoperabilní standardy a obsahují komplexní specifikace pro inkorporaci biometrických identifikátorů a elektronických paměťových prvků, což přispívá k zvýšení bezpečnosti na hranicích a efektivitě cestování [41].

Dokument, ačkoliv je primárně určen státním institucím vydávajícím elektronické doklady, nachází široké uplatnění i v soukromém sektoru, zvláště mezi firmami specializujícími se na řešení pro identifikaci na dálku. Tento dokument poskytuje sadu pravidel pokrývající procesy přístupu, čtení a verifikace dat z čipů, což je využíváno k zajištění spolehlivosti a bezpečnosti při ověřování identity.

Na základě poskytnutých informací je možné učinit závěr, že budoucí integrace se zaměří na elektronické doklady totožnosti, jako jsou eMROTD, eMRTD a eMRP, konkrétně na modely obsahující bezkontaktní čip, které lze načíst prostřednictvím NFC technologie. Pro analýzu konkrétních technických požadavků, která proběhne po připravě business case, má být využit dokument ICAO 9303, zveřejněný příslušnou organizací, který standardizuje pravidla práce s elektronickými doklady totožnosti. Tento dokument poskytuje důležité směrnice, které pomáhají zabezpečit kompatibilitu a bezpečnost při výměně a ověřování identifikačních údajů na mezinárodní úrovni.

4.2 Návrh integrace digitálních dokladů do Trask ZenID

4.2.1 Základní průběh procesu

Aby bylo možné správně navrhnout odhad integrace zpracování digitálních dokladů totožnosti do systému Trask ZenID, byla provedena základní analýza procesu načítání a verifikace dat z čipu dokladu totožnosti na základě zjednodušeného popisu přístupu k čipu zveřejněného ICAO na svých webových stránkách [42].

Jediným vybavením, které je vyžadováno při validaci dat z čipu, je mobilní telefon obsahující NFC čtečku.

Obecně proces načítání a verifikace čipu pomocí NFC technologie se skládá ze tří kroků. V prvním kroku má ověřující systém získat klíč, který je následně využit pro přístup k čipu, vestavěnému do dokladu totožnosti. Pro získání klíče je nezbytné přečíst MRZ zónu na dokladu, z níž je klíč odvozen.

V dalším kroku může systém na základě získaného klíče přistoupit k samotnému čipu vestavěnému do zkoumaného dokladu totožnosti. Jestliže čip potvrdí validitu klíče, proces pokračuje extrakcí dat.

Pokud je proces extrakce úspěšně dokončen, ověřující systém kontroluje platnost získaných dat a ověřuje platnost čipu.

V posledním kroku jsou data včetně potvrzení zobrazena uživateli.

AS-IS stav: Proces online identifikace prostřednictvím mobilního SDK

Jako první krok přípravy k integraci byla provedena analýza aktuálního stavu procesu. Cílem analýzy bylo prozkoumat business perspektivu procesu ověření identity pomocí mobilního SDK od začátku do konce. V tomto kontextu byl analyzován proces průběhu verifikace s využitím existující DEMO aplikace Trask ZenID (viz sekci č. 3.2.3), která implementuje mobilní SDK a nabízí kompletní sadu nástrojů pro identifikaci na dálku. Analýza byla provedena s využitím zjednodušené notace BPMN 2.0. Pro zobecnění, diagram mapuje synchronní komunikaci (viz sekce č. 3.2.3). Proces je zmapován na diagramu č. 4.5. Popis procesu je uveden v tabulce č. 4.1.[1][2]

#	**Název**	**Popis**	**Akce**	**Následující kroky**
1	Začátek procesu	Proces začíná otevřením DEMO aplikace.	-	Přechod na definici procesu
2	Definice průběhu procesu	Na úvodní obrazovce uživatel definuje, který doklad totožnosti chce naskenovat (země a model) a kroky, které budou součástí procesu identifikace (hologram, selfie/liveness)	-	Inicializace procesu
3	Inicializace	Mobilní SDK inicializuje se vůči backendu	-	Načtení konfigurace validátorů
Pokračování na další stránce				

[1] Diagram a jeho popis v tabulce byly vytvořeny autorem.

[2] Zdrojové soubory ve formátu .bpmn, obsahující všechny diagramy vytvořené v rámci analýzy této práce, jsou k dispozici ve složce "BPMN diagrams"v elektronické příloze.

– pokračování z předchozí stránky

#	Název	Popis	Akce	Následující kroky
4	Obdržení konfigurace validátorů	Mobilní SDK čeká na dokončení procesu inicializace, které končí obdržením aktuálních nastavení validátorů z Trask ZenID backendu	-	Začátek skenování dokladu
5	Skenování přední strany dokladu	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na přední stranu dokladu totožnosti a provést skenování	-	Rozhodnutí o potřebě skenování zadní strany
6	Rozhodovací bod o skenování zadní strany dokladu	Mobilní SDK na základě modelu dokladu určí, jestli je potřeba skenovat zadní stranu	Ano/Ne	Pokud ano, přejít k skenování zadní strany. Pokud ne, přejít k rozhodnutí o hologramu
7	Skenování zadní strany	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na zadní stranu dokladu totožnosti a provést skenování	-	Skenování zadní strany dokladu
8	Rozhodovací bod o ověření hologramu	Na základě definovaného průběhu procesu v rámci kroku 1 aplikace provede rozhodnutí o nutnosti skenovat hologram	Ano/Ne	Pokud ano, ověření hologramu. Pokud ne, rozhodnutí o Selfie/Liveness
9	Verifikace hologramu	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na stranu dokladu totožnosti obsahující hologram a provést jeho skenování	-	Provedení verifikace hologramu
10	Rozhodovací bod o ověření pomocí Selfie/Liveness	Na základě definovaného průběhu procesu v rámci kroku 1 aplikace provede rozhodnutí o nutnosti ověření pomocí Selfie/Liveness	Ano/Ne	Pokud ano, ověření pomocí Selfie/Liveness. Pokud ne, ověření výsledků
11	Verifikace pomocí Selfie/Liveness není vyžadována	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na svůj obličej a provést kroky nezbytné pro Selfie/Liveness verifikaci	-	Přímý přechod k ověření výsledků
13	Ověření výsledků	Mobilní SDK pošle nasbírané výsledky z jednotlivých procesů na backend Trask ZenID pro následné ověření a čeká na výsledky investigace	-	Zobrazení výsledků verifikace
14	Zobrazení výsledků	V okamžiku obdržení výsledku z investigace aplikace zobrazí je uživateli pro potvrzení	-	Ukončení procesu verifikace

Pokračování na další stránce

– pokračování z předchozí stránky

#	Název	Popis	Akce	Následující kroky
15	Konec verifikace	-	-	-

Tabulka 4.1 Aktuální stav procesu identifikaci - dokumentace

TO-BE stav: Integrace zpracování digitálních dokladů do stávajícího procesu

V následném kroku, na základě poskytnutého úvodu o RFID čipech a jejich využití v procesech identifikace, byl definován návrh procesu integrace této technologie do platformy Trask ZenID do stávajícího diagramu identifikace.

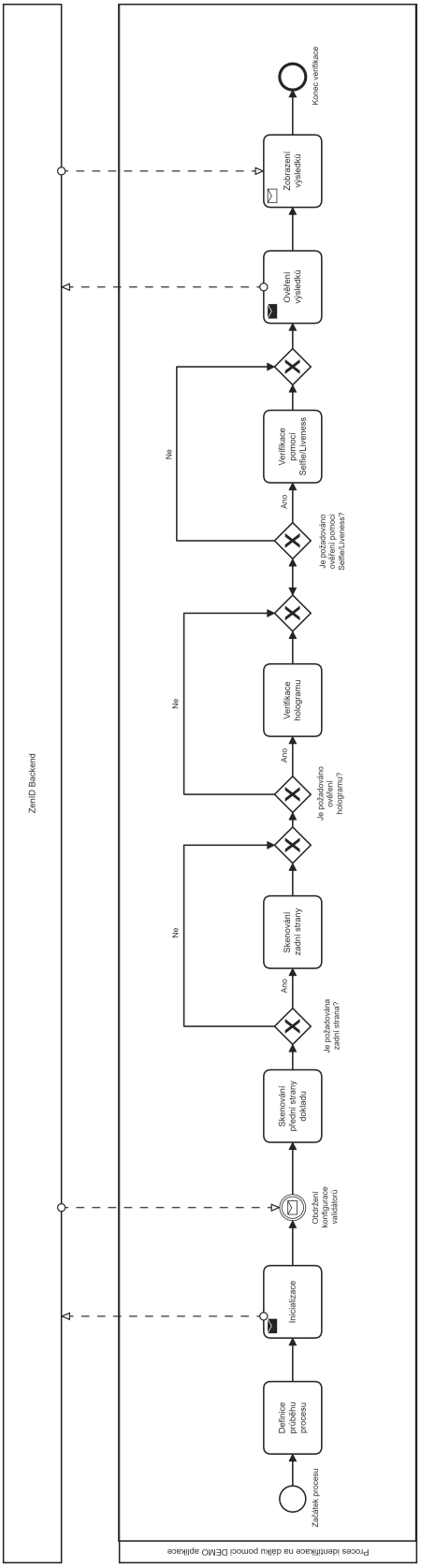
Jak bylo zmíněno výše, základním vybavením pro možnost provedení verifikace je čtečka v mobilním telefonu koncového uživatele. Ověřujícím systémem pak je mobilní SDK ve spolupráci se Trask ZenID Backendem.

Bylo identifikováno několik základních změn:

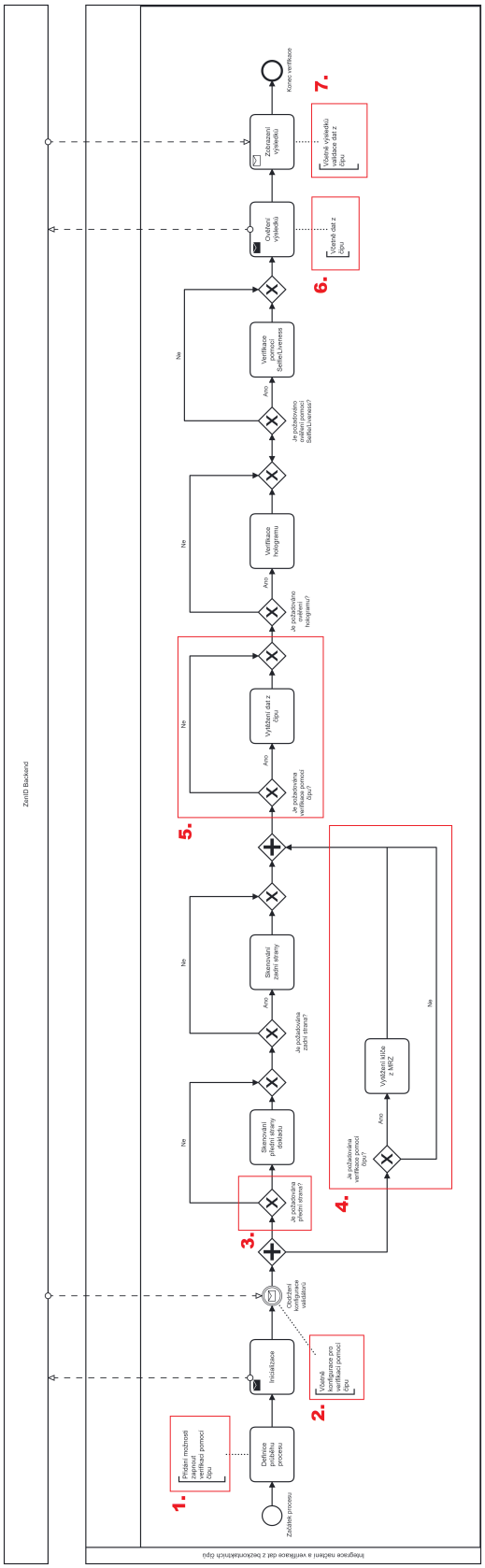
1. Zapojení do rozhraní mobilního SDK a samotné DEMO aplikace možnosti řízení spuštění procesu verifikace pomocí čipu v dokladech totožnosti.
2. Zvážení nutnosti vytvoření nového validátoru na backendové straně Trask ZenID, jehož konfigurace by byly odesílány mobilnímu SDK v rámci inicializace procesu verifikace. Nastavení validátoru by pak řídilo celý proces vytěžení a validace dat z bezkontaktních čipů.
3. Vzhledem k tomu, že iniciativa předpokládá i samotné použití verifikace pomocí čipu bez nutnosti zapojovat další typy verifikace, má být provedena změna v původním návrhu procesu identifikace. Aktuálně proces předpokládá povinné skenování přední strany dokladu, zatímco skenování zadní strany je dáno modelem dokladu. Pro přístup k čipu je nezbytné naskenování MRZ zóny pro získání klíče, která není povinně umístěna na přední straně. Jak bylo vidět na popisu kategorizace fyzických dokladů, doklady formátu TD1 mají MRZ umístěnou na zadní straně, což znamená, že pro verifikace čipu skenování přední strany může být vynecháno.
4. Součástí procesu skenování přední/zadní strany dokladu má být i OCR, které umožní SDK načíst MRZ zónu již na frontendu a aplikovat na ni algoritmus pro získání přístupového klíče k čipu. Vzhledem k tomu skenování dokladu a detekce MRZ zóny musí probíhat paralelně.
5. Přidání samotného kroku přístupu a vytěžení dat z čipu pomocí NFC čtečky zabudované do mobilního zařízení uživatele.
6. Společně se vzorky a výsledky verifikací z jiných kroků procesu musí být na backend odeslána i data vytěžená z bezkontaktního čipu, což implikuje nutnost úpravy rozhraní backendu pro schopnost jejich načtení a bezpečného přenosu.
7. Backend má být následně rozšířen o možnost zpracování, validace a uložení dat z bezkontaktního čipu. Výsledky investigace jsou pak společně s jinými daty vraceny na stranu klienta pro jejich zobrazení uživateli a dokončení procesu verifikace.

Integrace úprav do procesu je zmapována na diagramu č. 4.6. Jeho dokumentace je poskytnuta níže v tabulce č. 4.2.[3]

[3]Diagram a jeho popis v tabulce byly vytvořeny autorem.



Obrázek 4.5 Aktuální stav procesu identifikaci za využití mobilního SDK



Obrázek 4.6 Návrh budoucího stavu procesu identifikaci za využití mobilního SDK

#	**Název**	**Popis**	**Akce**	**Následující kroky**
1	Začátek procesu	Proces začíná otevřením DEMO aplikace.	-	Přechod na definici procesu
2	Definice průběhu procesu	Na úvodní obrazovce uživatel definuje, který doklad totožnosti chce naskenovat (země a model) a kroky, které budou součástí procesu identifikace (hologram, selfie/liveness). Uživatel může zvolit verifikaci pomocí čipu, jak v kombinaci s dalšími typy verifikací, tak i samotnou.	-	Inicializace procesu
3	Inicializace	Mobilní SDK inicializuje se vůči backendu.	-	Načtení konfigurace validátorů
4	Obdržení konfigurace validátorů	Mobilní SDK čeká na dokončení procesu inicializace, které končí obdržením aktuálních nastavení validátorů ze Trask ZenID backendu. Seznam konfigurací obsahuje také nastavení pro verifikaci pomocí čipu.	-	Paralelně následují dvě rozhodování: 1. Rozhodování ohledně skenování přední strany 2. Rozhodování ohledně načítání MRZ zóny
5	Rozhodovací bod o skenování přední strany dokladu	Pokud v rámci prvního kroku byla zvolena pouze verifikace pomoci bezkontaktního čipu, aplikace akceptuje stranu obsahující MRZ. Pokud se verifikace čipu kombinuje s kompletní verifikací dokladu, uživatel povinně má naskenovat přední stranu.	Ano/Ne	Pokud ano, přejít k skenování přední stranu. Pokud ne, přejít k rozhodnutí o skenování zadní strany.
6	Rozhodování ohledně nutnosti skenování MRZ	Pokud v rámci prvního kroku byla zvolena verifikace pomocí bezkontaktního čipu, aplikace čeká na detekci MRZ zóny.	Ano/Ne	Pokud ano, přejít k detekci a vytěžení MRZ pomocí OCR. Pokud ne, přejít k rozhodování ohledně verifikace čipu.
7	Skenování přední strany dokladu	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na přední stranu dokladu totožnosti a provést skenování.	-	Rozhodnutí o potřebě skenování zadní strany.
8	Rozhodovací bod o skenování zadní strany dokladu	Mobilní SDK na základě modelu dokladu určí, jestli je potřeba skenovat zadní stranu.	Ano/Ne	Pokud ano, přejít k skenování zadní strany. Pokud ne, přejít k rozhodnutí o hologramu.

Pokračování na další stránce

– pokračování z předchozí stránky

#	Název	Popis	Akce	Následující kroky
9	Skenování zadní strany	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na zadní stranu dokladu totožnosti a provést skenování.	-	Skenování zadní strany dokladu.
10	Rozhodovací bod o ověření bezkontaktního čipu	Na základě definovaného průběhu procesu v rámci kroku 1 aplikace provede rozhodnutí ohledně nutnosti ověření čipu.	Ano/Ne	Pokud ano, ověření bezkontaktního čipu. Pokud ne, rozhodnutí o ověření hologramu.
11	Verifikace bezkontaktního čipu	Aktivuje se NFC čtečka a čeká se na vstup od uživatele. Uživatel má přiložit mobil k dokladu pro aktivaci procesu vytěžení dat z čipu, aplikace následně přečte data.	-	Rozhodnutí ohledně ověření hologramu
12	Rozhodovací bod o ověření hologramu	Na základě definovaného průběhu procesu v rámci kroku 1 aplikace provede rozhodnutí ohledně nutnosti skenovat hologram.	Ano/Ne	Pokud ano, ověření hologramu. Pokud ne, rozhodnutí o Selfie/Liveness.
13	Verifikace hologramu	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na stranu dokladu totožnosti obsahující hologram a provést jeho skenování.	-	Provedení verifikace hologramu.
14	Rozhodovací bod o ověření pomocí Selfie/Liveness	Na základě definovaného průběhu procesu v rámci kroku 1 aplikace provede rozhodnutí ohledně nutnosti ověření pomocí Selfie/Liveness.	Ano/Ne	Pokud ano, ověření pomocí Selfie/Liveness. Pokud ne, ověření výsledků.
15	Verifikace pomocí Selfie/Liveness není vyžadována	Aktivuje se kamera a čeká se na vstup od uživatele. Uživatel má nasměrovat kameru na svůj obličej a provést kroky nezbytné pro Selfie/Liveness verifikaci.	-	Přímý přechod k ověření výsledků.
16	Ověření výsledků	Mobilní SDK pošle nasbírané výsledky z jednotlivých procesů včetně dat načtených z bezkontaktního čipu na backend Trask ZenID pro následné ověření a čeká na výsledky investigace.	-	Zobrazení výsledků verifikace.
17	Zobrazení výsledků	V okamžiku obdržení výsledku z investigace aplikace zobrazí je uživateli pro potvrzení.	-	Ukončení procesu verifikace.
18	Konec verifikace	-	-	-

Tabulka 4.2 Návrh budoucího stavu procesu identifikaci - dokumentace

Na základě získaných informací o zpracování digitálních dokladů totožnosti bylo provedeno zmapování tohoto procesu a vytvořen zjednodušený návrh této integrace do stávajících procesů vzdálené identifikace Trask ZenID. Tato analýza poskytuje pevný základ pro možnost přistoupení k tvorbě projektového plánu (viz sekce č. 4.3).

4.3 Tvorba WBS, odhad pracnosti na projektu

V rámci tvorby business case byla použita metoda "Work Breakdown Structure"(WBS), přibližný odhad trvání jednotlivých aktivit na základě osobních konzultaci s projektovým týmem a následný odhad pracnosti v člověkodnech (MDs) místo tradičního harmonogramu s fixními termíny. Toto rozhodnutí bylo motivováno především potřebou vyšší flexibility v plánování, která je nezbytná vzhledem k charakteru projektu, jehož specifikace a priority se mohou dynamicky měnit a aktivity se mohou vzájemně překrývat vzhledem k aktuální dostupnosti kapacit. Využití WBS umožňuje flexibilnější řízení a alokaci zdrojů podle skutečných potřeb jednotlivých úkolů bez zbytečného zatěžování specifickými termíny, což napomáhá efektivnější adaptaci na změny během životního cyklu projektu. Tato metodologie byla projednána a odsouhlasena vedením Trask ZenID, což zajišťuje, že je v souladu s předpisy společnosti.

Projekt integrace verifikace pomocí digitální identity uložené na bezkontaktních čipech bude realizován ve formě projektu s pevně stanoveným časem a cenou, známým jako Fixed Time Fixed Price (FTFP). Tento model projektového řízení je charakterizován pevně stanovenými smluvními podmínkami, včetně ceny a doby dodání, což minimalizuje rizika spojená s překročením rozpočtu a termínů ze strany dodavatele [43]. Zatímco náklady budou jasně definovány již po finalizaci business case, konkrétní čas a návaznost budou definovány projektovým týmem v okamžiku rozhodnutí o jeho realizaci na základě předložených odhadů trvání jednotlivých aktivit.

4.3.1 WBS a Projektový plán

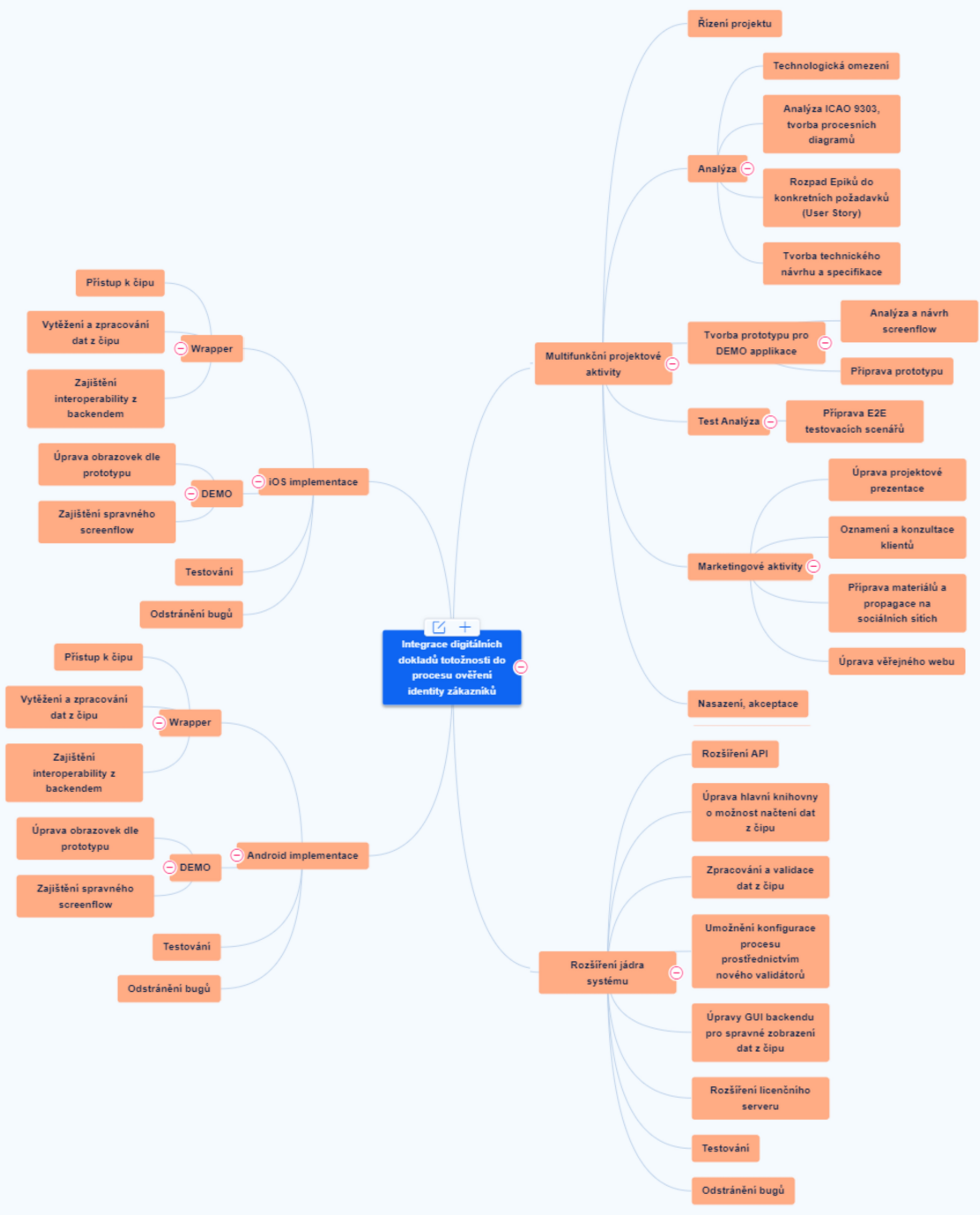
V první fázi byla vytvořena WBS na základě změn popsaných v sekci č. 4.2 týkající se budoucího stavu (To-Be stav). WBS je znázorněná na diagramu č. 4.3.[4]

V následující fázi byly jednotlivé části WBS transformovány do strukturovanější podoby, která lépe reflektuje specifika řízení projektu a jeho iterativní přístup. Bylo rozhodnuto využít stejnou metodiku, která je aktuálně využívaná pro řízení Trask ZenID. Jedná se o metodiku Scrum, agilní framework pro řízení projektů, který je organizován do iniciativ, epiků, úkolů a příběhů. V daném kontextu iniciativa odpovídá Integraci digitálních dokladů totožnosti do procesu ověření identity zákazníků. Epik představuje velký blok práce, rozdělený na menší části - příběhy a úkoly.

Byly definovány čtyři hlavní epiky:

- **Multifunkční aktivity** - epik vyhrazený pro úkoly spojené s řízením, analýzou a marketingem projektu. Úkoly v tomto epiku mohou trvat po celou dobu trvání projektu, pro jejich správu byly zařazeny do samostatného epiku.
- **Rozšíření jádra systému** - zahrnuje úkoly spojené s rozšířením funkcionality backendové části Trask ZenID včetně úprav API a uživatelského rozhraní. Úpravy zahrnují přidání možnosti konfigurace procesu verifikace pomocí bezkontaktního čipu, zpracování, validaci a ukládání extrahovaných dat s možností opětovného zobrazení.
- **Úpravy v mobilních SDK** - aktivita je představená dvěma epiky, které jsou spojené s implementaci v obou mobilních knihovnách (viz "iOS Implementace"a "Android Implementace"na obrázku č. 4.7). Epiky budou zahrnovat úpravu jádra knihoven, které umožní přístup k čipu, načítání dat a odesílání na připravené rozhraní backendu pro následnou validaci. Součástí epiku budou také úpravy DEMO aplikace, které se využijí pro testování a jako materiály

[4] Diagram na obrázku byl vytvořen autorem.



Obrázek 4.7 Rozpad projektových aktivit

pro propagaci projektu mezi zákazníky Trask ZenID. Integrace do webového SDK provedená nebude z důvodů omezené podpory NFC technologie prohlížeči, což bude detailně popsané v další kapitole (viz sekce č. 5.1).

Tato struktura byla doplněna o role zodpovědné za realizaci dílčích částí pro možnost následného odhadu nákladů (viz tabulka č. 4.3). Rozpad a trvání aktivit jsou v této fázi považovány za hrubý odhad. Naplnění epiků příběhy a úkoly není konečné a bude upřesňováno v průběhu první analytické fáze projektu. Z tohoto důvodu nejsou stanoveny fixní termíny pro jednotlivé úkoly, ale jsou poskytovány pouze odhady trvání, které byly stanovené po komunikaci s odpovědnými rolemi. Takovýto flexibilní přístup umožňuje efektivnější a přizpůsobivější způsob řízení projektu, který může reagovat na nečekané změny a potřeby. Výsledky analýzy projektového plánu jsou uvedeny v tabulce č. 4.8.[5]

4.3.2 Odhad nákladů na projekt

Celková pracnost projektu byla po diskuzi s týmem a vedením projektu naplánována na čtyři a půl měsíce a je prezentována v následující tabulce č. 4.9.[6] Rozvržení práce je vyjádřeno v MDs a je rozděleno podle měsíců a specifických rolí v projektu, jako jsou Analytik, Projektový Manažer, Vývojáři různých specializací, Tester a Designer UX/UI.

Větší část práce analytika, která předchází samotné implementaci, bude v následujících měsících převážně spočívat v podpoře při detekci a zapracování změn do projektu. Řízení projektu bude probíhat kontinuálně po celou dobu plánu. Vývoj jádra integrace je naplánován na druhý měsíc a bude se koncentrovat během dvou měsíců s předpokládanou alokací dvou vývojářů. Práce na mobilních aplikacích začne měsíc po přípravě jádra a umožnění komunikace s backendem, přičemž se počítá s alokací jednoho vývojáře pro jednu platformu. Tester se zapojí do iterativního testování backendové části, po kterém bude pokračovat v testování mobilních aplikací. Designer bude využit pouze pro návrh obrazovek pro DEMO aplikaci. Celkový odhad pracnosti je stanoven na 185.5 MDs.

V dalším kroku byl na základě sazeb pro každou roli proveden výpočet odhadu celkových nákladů. Sazba představuje pevně stanovenou cenu za jeden pracovní den pro danou roli. Výpočet celkových nákladů pro každou roli vychází ze spočítaných pracovních dnů za dané období a vynásobení počtu těchto dnů danou sazbou. Celkové náklady projektu jsou pak součtem všech individuálních nákladů pro jednotlivé role, což ve výsledku dává celkovou sumu **1,250,500 Kč** (viz tabulka č. 4.3).[7] Ceny byly stanoveny na základě sazby, která byla komunikována vedením projektu. Při výpočtu se nepočítá s dalšími náklady, jelikož Trask ZenID je dávno běžící projekt, jehož tým již disponuje všemi potřebnými hardwarovými a softwarovými prvky nezbytnými pro vývoj.

[5] Tabulka na obrázku byla vytvořena autorem.
[6] Tabulka na obrázek byla vytvořena autorem.
[7] Tabulka byla vytvořena autorem na základě konzultace s vedením projektu.

Typ	Název	Trvání (Týdny)	Role
Epik	**Multifunkční Projektové Aktivity**	**18**	
Fáze	**Řízení projektu**	**18**	Projektový manažer
Fáze	**Analýza**	**18**	
Úkol	Technologické omezení	0.4	Analytik
Úkol	Analýza ICAO 9303, tvorba procesních diagramů	2	Analytik
Úkol	Rozpad Epiků do konkretních požadavků (User Story)	1	Analytik
Úkol	Tvorba technického návrhu a specifikace	1	Analytik, Vývojář CPP, iOS, Android
Fáze	**Tvorba prototypu pro DEMO applikace**	**3**	
Úkol	Analýza a návrh screenflow	1	Analytik
Úkol	Příprava prototypu	2	Designer
Fáze	**Test Analýza**	**3**	
Úkol	Příprava E2E testovacích scenářů	3	Tester, Analýtik
Fáze	**Marketing**	**8**	
Úkol	Úprava projektové prezentace	1	Marketing&Sales, Analytik
Úkol	Oznamení a konzultace klientů	1	Marketing&Sales, Analytik
Úkol	Příprava materiálů a propagace na sociálních sítích	6	Marketing&Sales, Analytik
Úkol	Úprava věřejného webu	2	Marketing&Sales, Analytik
Fáze	**Nasazení, akceptace**	**1**	Vývojář CPP, iOS, Android
Epik	**Rozšíření jádra systému**	**12**	
Úkol	Rozšíření API	0.3	Vývojář CPP
Úkol	Úprava hlavní knihovny o možnost načtení dat z čipu	2	Vývojář CPP
Úkol	Zpracování a validace dat z čipu	1	Vývojář CPP
Úkol	Umožnění konfigurace procesu prostřednictvím nového validátorů	1	Vývojář CPP
Úkol	Úpravy GUI backendu pro spravné zobrazení dat z čipu	3	Vývojář CPP
Úkol	Rozšíření licenčního serveru	0.3	Vývojář CPP
Úkol	Testování	4	Tester, Vývojář CPP
Úkol	Odstránění bugů	4	Vývojář CPP, Tester
Epik	**Android Implementace**	**8**	
Fáze	**Wrapper**	**5**	Vývojář Android
Úkol	Přístup k čipu	1	Vývojář Android
Úkol	Vytěžení a zpracování dat z čipu	2	Vývojář Android
Úkol	Zajištění interoperability z backendem	2	Vývojář Android
Fáze	**DEMO**	**6**	Vývojář Android
Úkol	Úprava obrazovek dle prototypu	1	Vývojář Android
Úkol	Zajištění spravného screenflow	1	Vývojář Android
Úkol	Testování	5	Tester, Vývojář Android
Úkol	Odstránění bugů	5	Vývojář Android, Tester
Epik	**iOS Implementace**	**8**	
Fáze	**Wrapper**	**5**	Vývojář iOS
Úkol	Přístup k čipu	1	Vývojář iOS
Úkol	Vytěžení a zpraování dat z čipu	2	Vývojář iOS
Úkol	Zajištění interoperability z backendem	2	Vývojář iOS
Fáze	**DEMO**	**6**	Vývojář iOS
Úkol	Úprava obrazovek dle prototypu	1	Vývojář iOS
Úkol	Zajištění spravného screenflow	1	Vývojář iOS
Úkol	Testování	5	Tester, Vývojář iOS
Úkol	Odstránění bugů	5	Vývojář iOS, Tester

Obrázek 4.8 Projektový plán

Měsíc	Týden / staff	Analytik	Projektový Manažer	Marketing&Sales	Vývojář CPP	iOS Vývojář	Android Vývojář	Tester	Designer UX/UI
1. měsíc	1	3	1	0	0	0	0	0	
	2	3	1	0	0	0	0	0	0
	3	4	1	0	0	0	0	0	0
	4	4	1	0	0	0	0	0	0
2. měsíc	5	4	1	0	6	0	0	0	0
	6	4	1	0	6	0	0	0	2
	7	2	1	0	6	0	0	1	2
	8	2	1	0	8	0	0	1	2
3. měsíc	9	2	1	0	8	3	3	1	0
	10	2	1	0	8	3	3	1	0
	11	1	1	0.5	8	3	3	1	0
	12	1	1	0.5	6	3	3	1	0
4. měsíc	13	1	1	1	1	3	3	1	0
	14	1	1	2	1	3	3	1	0
	15	1	1	2	1	2	2	1	0
	16	0.5	1	2	1	2	2	1	0
5. měsíc	17	0.5	1	2	0	0	0	0	0
	18	0.5	1	1	0	0	0	0	0
	MDs	36.5	18	11	60	22	22	10	6

Obrázek 4.9 Odhad pracnosti

Role	MD rate (Kč)	Celkové náklady (Kč)
Vývojář CPP	6,500.00	390,000.00
iOS vývojář	7,500.00	165,000.00
Android vývojář	7,500.00	165,000.00
Business Analytik	7,000.00	255,500.00
Tester	4,500.00	45,000.00
Designer UX/UI	7,500.00	45,000.00
Project Manager	6,000.00	108,000.00
Marketing&Sales	7,000.00	77,000.00
	Celkem	**1,250,500.00**

Tabulka 4.3 Výpočet celkových nákladů

4.3.3 Zisk a návratnost projektu

Po diskuzi s vedením projektu bylo rozhodnuto, že výsledek integrace bude prodáván jako samostatný modul pod názvem NFC, a cena bude zahrnovat jednorázový poplatek za jeho aktivaci ve výši **100 000 Kč**, což je podobný cenový model jako u modulu Tvorba Reportů (viz sekce č. 3.6). Pro odhad proveditelnosti a návratnosti projektu byli stávající zákazníci rozděleni do dvou základních skupin na základě jejich aktuálního použití mobilního SDK. První skupinu tvoří zákazníci, kteří již mají zakoupené knihovny, zatímco druhou ti, kteří je nemají. V případě aktivace NFC modulu první skupinou se počítá s dodatečnými příjmy spojenými s nákupem a údržbou mobilních knihoven. V případě zájmu se počítá s tím, že zákazníci zakoupí zvýhodněný balíček obsahující dvě SDK pro platformy iOS a Android, což je obvyklá praxe. Pokud by modul NFC vzbudil zájem nových zákazníků, kteří nemají u Trask ZenID zakoupené ani OCR, je také do výpočtu zisku nezbytné zahrnout příjmy spojené s nákupem OCR modulu. Ačkoliv cena tohoto modulu v současnosti není veřejně dostupná a v odhadech je uvedena jako 0 Kč, v případě potřeby lze tuto částku nastavit na požadovanou hodnotu v dokumentu Business case (viz soubor "Business Case.xlsx"v elektronické příloze práce a také popis dokumentu v příloze B). Odhad bude automaticky přepočítán tak, aby odrážel stanovenou částku. Ceník za sjednané služby je také uveden v tabulce č. 4.4.[8]

[8]Tabulka byla vytvořena autorem na základě konzultace s vedením projektu Trask ZenID.

Ceník					
Položka	1 SDK	2 SDKs	Údržba SDK	NFC	OCR, dalsí OTF
Cena	250,000	400,000	20%	100,000	0

Tabulka 4.4 Ceník Trask ZenID

Oběma skupinám byly následně komunikovány informace ohledně iniciativy Trask ZenID o rozšíření svého stávajícího balíčku o nový modul s cílem zjistit zájem mezi klienty. Výsledek komunikace je zobrazen v tabulce č. 4.5

		Stávající počet zákazníků	Projevili zájem o NFC modul
Použiívají mobilní SDK	OnPrem	9	5
	Saas	2	0
Nepoužívají mobilní SDK	OnPrem	10	1
	SaaS	3	1

Tabulka 4.5 Zájem mezi stávajícími klienty o nový modul

Následně byly spočítány pesimistický a optimistický odhady návratnosti projektu pro období pěti let od roku 2024 do roku 2028, přičemž tato doba byla určena na základě diskuzí s vedením projektu tak, aby odpovídala obecným pokynům společnosti.

V rámci výpočtu pesimistického odhadu (viz obrázek č. 4.10) návratnosti projektu se počítá s průměrnou 15% úspěšností nákupu modulu mezi stávajícími zákazníky v obou skupinách, což představuje přibližně dva klienty od každé skupiny.[9] Dále se předpokládá, že po propagaci modulu na webových stránkách společnosti, sociálních sítích a dalších kanálech bude možné získat další dva klienty.

V rámci optimistického odhadu (viz obrázek č. 4.11) se spoléhá na přibližně 30% úspěšnost mezi všemi zákazníky, rozdělenou v poměru 5 ku 3 ve dvou skupinách, a na možnost rozšíření zákaznické báze o další čtyři klienty.[10]

Oba plány zahrnují následný výpočet hrubého zisku, který je definován jako zisk spojený s aktivací NFC modulu včetně případného nákupu SDK a s ním spojené údržby. Zisk z nákupu OCR modulu zůstal prázdný a může být doplněn v případě potřeby vedením projektu.

Hrubý zisk byl následně převeden na zisk po zdanění, přičemž daňová sazba byla vzata jako 21% – daň ze zisku platná od roku 2024 pro právnické osoby [44].

Daňová sazba	21%
Zisk v procentech	79%
Míra inflace	5%

Tabulka 4.6 Daňová sazba a úroková míra

Tok peněz byl spočítán s přihlédnutím k míře inflace, spočítané jako průměrná míra inflace v České republice za posledních 10 let (viz tabulka č. 4.6). Čistý zisk z prodeje NFC modulu, přidruženého prodeje mobilních SDK a spojené s tím údržby je pak znázorněn na grafu č. 4.12.[11]

V obou plánech je vidět, že hrubý zisk je záporný v prvním roce a zlepšuje se v dalších letech. Analogicky tok peněz je záporný v prvním roce, ale postupně roste a stává se kladným,

[8] Vytvořeno autorem na základě konzultace s vedením projektu.
[9] Tabulka na obrázku byla vytvořena autorem.
[10] Tabulka na obrázku byla vytvořena autorem.
[11] Graf na obrázku byl vytvořen autorem.

což naznačuje, že projekt bude z dlouhodobého hlediska odhadově generovat pozitivní peněžní tok.

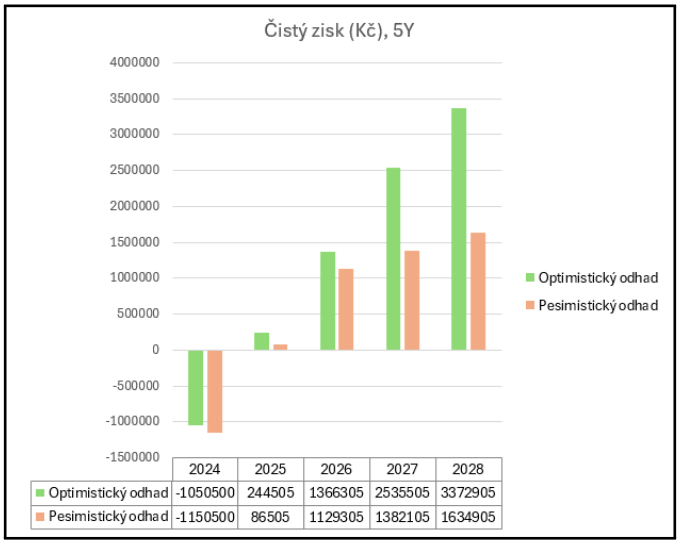
Čistá současná hodnota (ukazatel NPV, který se používá k vyhodnocení výnosnosti investic nebo projektu) vyšla kladná, což naznačuje, že scénáře předpokládají, že budoucí hodnota příjmů a úspor generovaných projektem během jeho životního cyklu je vyšší než hodnota nákladů spojených s projektem [45].

		0	1	2	3	4		
Pesimistický odhad		**2024**	**2025**	**2026**	**2027**	**2028**	Celkem	
	Náklady (Kč)	1250500	0	0	0	0		
	Používají mobilní SDK	1	1	0	0	0	2	
	Nepoužívají mobilní SDK	0	1	1	0	0	2	
	Noví zákazníci	0	1	1	0	0	2	
	Přírůstek	**1**	**3**	**2**	**0**	**0**		
	NFC	100000	300000	200000	0	0		
	SDK	0	800000	800000	0	0		
	Udržba	0	160000	320000	320000	320000		
	Jiné (OCR, OTF)	0	0	0	0	0		
	Celkově (Kč)	**100000**	**1260000**	**1320000**	**320000**	**320000**		
	Hrubý zisk (Kč)	-1150500	109500	1429500	1749500	2069500		
	Po zdanění (Kč)	-1150500	86505	1129305	1382105	1634905		
	CF (Kč)	**-1150500**	**82386**	**1024313**	**1193914**	**1345040**	**2495153**	NPV

Obrázek 4.10 Pesimistický plán

		0	1	2	3	4		
Optimistický odhad		**2024**	**2025**	**2026**	**2027**	**2028**	Celkem	
	Náklady (Kč)	1250500	0	0	0	0		
	Používají mobilní SDK	2	2	1	0	0	5	
	Nepoužívají mobilní SDK	0	1	1	1	0	3	
	Noví zákazníci	0	1	1	1	1	4	
	Přírůstek	**2**	**4**	**3**	**2**	**1**		
	NFC	200000	400000	300000	200000	100000		
	SDK	0	800000	800000	800000	400000		
	Udržba	0	160000	320000	480000	560000		
	Jiné (OCR, OTF)	0	0	0	0	0		
	Celkově (Kč)	**200000**	**1360000**	**1420000**	**1480000**	**1060000**		
	Hrubý zisk (Kč)	-1050500	309500	1729500	3209500	4269500		
	Po zdanění (Kč)	-1050500	244505	1366305	2535505	3372905		
	CF (Kč)	**-1050500**	**232862**	**1239279**	**2190265**	**2774897**	**5386803**	NPV

Obrázek 4.11 Optimistický plán



Obrázek 4.12 Grafické znázornění zisku za období 5 let

V rámci této kapitoly byl podrobně prozkoumán potenciál integrace zpracování digitálních dokladů totožnosti do systému Trask ZenID. Bylo zdůrazněno, jak probíhá NFC komunikace

při zpracování bezkontaktních čipů na dokladech totožnosti, což přináší značné výhody pro zabezpečení a pohodlí při ověřování totožnosti. S ohledem na normy ICAO 9303 a úlohu, kterou hraje ICAO v regulaci a standardizaci digitálních identifikačních procesů, byla tato technologie identifikována jako klíčová pro budoucí rozvoj v oblasti digitálních identit.

Prvotní návrh integrace a plán projektu, který zahrnuje výpočet nákladů a návratnosti investic, byl stanoven jako základ pro další rozhodování ve společnosti o zavádění této inovace.

Celkově se předpokládá, že přijetí NFC technologie by nejen že zvýšilo bezpečnostní standardy Trask ZenID, ale také posílilo jeho konkurenceschopnost na trhu digitální identifikace. S ohledem na pozitivní čistou současnou hodnotu a výsledky analýzy návratnosti investic je projekt považován za finančně životaschopný a strategicky prospěšný pro další růst a inovace firmy. Tato kapitola tak nastavuje pevný základ pro realizaci projektu a další rozvoj služeb Trask ZenID v oblasti digitálních dokladů totožnosti.

Kapitola 5
Funkční analýza

V předchozí kapitole bylo potvrzeno, že integrace zpracování digitálních dokladu totožnosti má velký potenciál jak z procesní, tak finanční stránky projektu. Na základě těchto předpokladu je možné přejít k podrobnějšímu přehledu technické specifikace využití NFC technologie a její podpoře na různých platformách. Tato kapitola bude věnována směrnici ICAO 9303, konkrétně analýze přístupových a bezpečnostních mechanismů, které jsou zásadní pro ověření integrity dat. Tato analýza rovněž zahrnuje detailní zkoumání struktury čipu a rozsahu, na který bude cílena implementace systému Trask ZenID.

Na základě uvedené analýzy budou stanoveny specifické požadavky, které budou transformovány do uživatelských příběhů (z anglického "User Story"). Tyto příběhy pak poslouží jako klíčové vstupy pro další vývoj a implementaci funkcionality. Důležitou součástí kapitoly je také návrh rozšíření DEMO aplikace, včetně vytvoření wireframů a definice testovacích scénářů. Tím se zvyšuje pravděpodobnost, že výsledný produkt bude nejen zohledňovat technické detaily, ale bude také uživatelsky přívětivý a prakticky ověřený.

5.1 Technická omezení spojená s načítáním bezkontaktních čipů

První část analýzy je zaměřena na identifikaci technických omezení, která jsou spojena s možnostmi provádění identifikace na dálku pomocí bezkontaktních čipů. Klíčovým aspektem je zjištění, která zařízení podporují technologii NFC napříč operačními systémy, jako jsou Android a iOS, a zda je možné tuto technologii využít prostřednictvím webového SDK.

Vzhledem k rozmanitosti společností prodávajících mobilní telefony s operačním systémem Android se analýza soustředila na přední výrobce v této oblasti. Výsledky, které specifikují mobilní značky a rok, od kterého zařízení disponují vestavěnými čtečkami, ilustrují, jak se jednotliví výrobci rozhodují o zařazení technologie NFC do svých produktů (viz tabulka č. 5.1).[1] Je vidět, že se rok zahájení podpory NFC technologie pro systém Android liší v závislosti na konkretním dodavateli. Zajímavým zjištěním je také to, že koncoví uživatelé mají možnost řídit zapínání NFC čtečky podle svých potřeb [46].

Pro systém iOS byla technologie NFC představena již v modelu iPhone 6 z roku 2014, ale plná podpora čtení a kódování informací z jiných NFC kompatibilních zařízení byla zavedena až v modelu iPhone 6s z následujícího roku [47]. Funkce NFC je od tohoto prvního modelu automaticky povolena, což uživatelům umožňuje využívat služby jako Apple Pay a zajišťuje nepřetržitou funkčnost pro procesy jako zpracování plateb či čtení NFC značek. Systém iOS navíc

[1] Vytvořeno autorem na základě informace ve článku [46].

Společnost	První model z NFC	Podpora NFC ve všech zařízeních
Google	2016	2016
Samsung	2012	2015
Huawei	2017	2017
Xiaomi	2015	2018
OnePlus	2014	2016
LG	2014	2019
Essential	2017	2017
Nokia	2017	2019
Sony	2017	2017
HTC	2014	2019

Tabulka 5.1 Podpora NFC napříč různými modely

neumožňuje NFC funkci úplně vypnout, což zajišťuje bezproblémový chod aplikací závislých na této technologii.

Podpora webového rozhraní NFC API, které je nyní dostupné na 42,29% desktopových a mobilních zařízeních, byla nedávno zavedena ve webových prohlížečích jako Chrome pro Android ve verzi 123 a Baidu Browser ve verzi 13.52. [48].

Vzhledem k těmto informacím byly identifikovány možné překážky během verifikace pomocí bezkontaktních čipů:

- Nedostupnost NFC čtečky: situace, kdy mobilní zařízení nemá k dispozici NFC čtečku, což znemožní identifikaci pomocí bezkontaktních čipů.
- Vypnutá NFC čtečka u Androidu: uživatelé Androidu mohou mít během identifikace na dálku vypnutou NFC čtečku, což zabrání dokončení verifikace.
- Nízká a nejednotná NFC kompatibilita: kompatibilita NFC napříč prohlížeči pro mobilní zařízení je extrémně nízká a není jednotná pro různé operační systémy.

Společně s týmem Trask ZenID pro každý problém byla vybrána řešení, která jsou definována jako požadavky na budoucí systém:

- **Umožnění přeskočení verifikace pomoci čipu:** jako vlastník procesu chci mít možnost konfigurovat proces verifikace identity pomoci bezkontaktního čipu tak, aby uživatelé bez podpory NFC čtečky mohli tento krok přeskočit a pokračovat v dalším kroku identifikace.
  - **Zaznamenání přeskočení:** jako vlastník procesu chci v uživatelském rozhraní aplikace pro administrátory mít záznam, že daný uživatel přeskočil proces s jasně definovaným důvodem.
- **Řízení NFC čtečky:** jako uživatel Android SDK aplikace potřebuji, aby mě aplikace upozornila na stav NFC čtečky (v případe, že je vypnutá nebo nedostupná) a přesměrovala do systémových nastavení pro změnu nastavení NFC čtečky a dokončení verifikačního procesu. (Požadavek není platný pro iOS SDK.)
  - **Neaktivní NFC čtečka:** jako administrátor procesu chci, aby uživatelé, kteří odmítnou zapnout NFC čtečku, neměli možnost dokončit proces identifikace nebo jej obejít.
- **Omezení verifikace pro webové SDK**: jako vlastník produktu chci omezit možnost verifikace pomocí bezkontaktních čipů pro webové SDK s ohledem na NFC kompatibilitu a neopodstatněné investice v případě implementace této funkce do dané knihovny.

Obrázek 5.1 Symbol "Čip uvnitř dokladu" [49]

5.2 Detekce bezkontaktního čipu

Během procesu identifikace na dálku mohou uživatelé předložit různé doklady totožnosti. V okamžiku zahájení verifikace není mobilní SDK omezeno na specifické typy dokladů a může akceptovat široký výčet modelů. Současně mobilní SDK disponuje funkcionalitou pro detekci a rozpoznání dokladů. To znamená, že během skenování stran dokladu SDK porovnává detekovaný doklad a jeho model s předem definovanou sadou dokladů, které jsou pro daný obchodní proces akceptovatelné. Na základě tohoto porovnání SDK buď doklad od uživatele přijme (doklad je automaticky vyfocen), nebo jej odmítne (vyfocení neproběhne).

V rámci skenování dokladu totožnosti (viz diagram č. 4.6) mělo by mobilní SDK navíc provést detekci bezkontaktního čipu. Jak bylo uvedeno v sekci č. 4.1.1, pouze doklady typu TD1, TD2 a TD3, obsahující MRZ zónu, mohou obsahovat integrované čipy, neboť tato zóna obsahuje klíč pro přístup k čipu. Dostupnost čipů se však může lišit v závislosti na konkrétním modelu daného dokladu. Například české občanské průkazy formátu TD1 mají bezkontaktní čipy pouze ve verzích vydaných od roku 2021, zatímco předchozí modely stejného formátu a s obdobnými charakteristikami tento bezpečnostní prvek neobsahují [7].

Podle standardu ICAO 9303 všechny doklady obsahující bezkontaktní čipy musejí být označeny speciálním symbolem (viz obrázek č. 5.1) [49]. Původní nápad detekovat doklady s bezkontaktním čipem pomocí tohoto symbolu byl po dalším zkoumání zamítnut. Symbol na dokladech nemá pevné umístění; zatímco české občanské průkazy mají tento symbol v pravém horním rohu na zadní straně, chorvatské občanské průkazy jej mají posunutý doprostřed a slovenské občanské průkazy jej mají zepředu nahoře. Další komplikací je situace s pasy, kde je označení umístěno na obalu knihy, který obvykle není systémem pro identifikaci, včetně Trask ZenID, ověřován [7].

Po diskuzi s vývojáři byl navržen další přístup k řešení tohoto problému. Řešení spočívá ve vytvoření seznamu, který zaznamenává podporu bezkontaktních čipů podle konkrétního modelu. Na základě MRZ zóny, která obsahuje datum vydání, je mobilní SDK schopno detekovat příslušný model a podle seznamu rozhodnout, zda daný model podporuje bezkontaktní čip. Seznam byl vytvořen na základě informací z rejstříku PRADO a je poskytnut jako příloha této práce (viz příloha E). Tento seznam je průběžně aktualizován týmem Trask ZenID v případě detekce změn v registru.

Na základě uvedených informací byl definován nový požadavek na detekci bezkontaktních čipů během identifikace:

- **Detekce bezkontaktního čipu:** jako vlastník produktu chci, aby mobilní SDK byla schopná na základě seznamu podpory bezkontaktních čipů napříč modely provést detekci bezkontaktního čipu u daného dokladu.
  - **Nedefinované chování:** jako vlastník produktu chci, aby se mobilní SDK řídilo pravidly pro přeskočení identifikace pomocí čipu (viz požadavek v sekci č. 5.1. Umožnění přeskočení verifikace pomoci čipu) v případě, že zkoumaný model, i když je formátu TD1, TD2 nebo TD3, nenabízí podporu bezkontaktního čipu.

5.3 Struktura čipu

Pro správné navržení dalšího průběhu procesu je nezbytné prozkoumat samotný čip a určit, která data jsou dostupná a mohou být zpracována. Analýza byla provedena dle standardu ICAO, konkrétně dokumentu č. 10. [50].

Obsah každého čipu se může lišit v závislosti na státech, které tyto čipy vydávají. Přesto ICAO definuje základní kritéria, která musí vydávající instituce dodržovat, aby zajistily globální interoperabilitu mezi inspekčními systémy a obsahem čipu.

Každý čip může obsahovat jednu nebo dvě struktury nazývané LDS (Logical Data Structure), z nichž každá obsahuje vlastní sadu dat týkajících se dokladu nebo jeho držitele. Seznam všech souborů uložených na čipu včetně jejich popisu je uveden v příloze C.[2]

5.3.1 LDS1

LDS1 je povinná struktura čipu, která obsahuje atributy primárních dat umožňujících propojení držitele s dokumentem. Informace uložené v LDS1 eMRTD jsou v okamžiku vydání statické a nelze je změnit (zaručeno požadavkem na ochranu proti zápisu: po vydání nelze uzamčený čip odemknout). LDS1 zahrnuje seskupené datové soubory s informacemi, které uchovává vydávající stát. Zatímco některé datové soubory jsou povinné, sada může být podle rozhodnutí státu rozšířena o další strojově čitelné údaje považované za důležité. Na obrázku č. 5.2 jsou uvedeny konkrétní soubory, které jsou nebo mohou být součástí LDS1.

Nejdůležitějšími pro identifikaci jsou soubory DG1 a DG2, které obsahují informace z MRZ a biometrická data týkající se držitele dokladu, konkrétně jeho fotografii. Další dva soubory, DG3 a DG4, mohou také nabízet doplňující bezpečnostní ověření, protože obsahují otisky prstů držitele a zobrazení zornic. Tyto soubory jsou chráněny dodatečnou vrstvou kontroly, ale zatím nejsou v zajmu Trask ZenID. Aplikace Trask ZenID by mohla získat přístup ke všem podporovaným skupinám dat, ačkoli další zpracování a šetření se zaměří primárně na DG1 a DG2. Ostatní datové skupiny nejsou v kontextu aktuálně podporovaných případů použití relevantní.

5.3.2 LDS2

Další strukturou, která může být vestavěna do čipu, je LDS2. Jedná se o volitelnou strukturu, která je rozšířením LDS1. Tato struktura může uchovávat cestovní informace o držiteli dokladu, jako jsou víza, razítka a další biometrické údaje po dobu jejich platnosti. Tato struktura není v obchodním zajmu Trask ZenID, a proto nebude následně analyzována a zpracovávána během identifikace. Tuto část lze považovat za příležitost pro další rozšíření modulu NFC.

5.3.3 Master file

Jedná se o hlavní nebo kořenový soubor obsahující informace o bezkontaktním čipu. Tento soubor není povinný a je obsazen v čipu, pokud ten podporuje složitější bezpečnostní kontroly pro získání přístupu a oprávnění k čtení uložených dat. Obsahuje informace o podporovaných protokolech a instrukce pro jejich použití (více v sekci č. 5.4).

5.3.4 Rozsah využití Trask ZenID

Pro zajištění správného navržení a implementace procesů souvisejících s identifikací pomocí bezkontaktních čipů je klíčové zaměřit se na zpracování datových souborů DG1 a DG2, což je znázorněno na obrázku č. 5.2.[3] Tyto skupiny poskytují nejen MRZ zónu, ale i fotografii držitele

[2] Tabulky v příloze byly vytvořeny autorem na základě interpretace dokumentu ICAO 9303 č.10 [50].
[3] Obrázek byl vytvořen autorem na základě analýzy dokumentu ICAO 9303 č.10 [50].

dokladu. Dále budou zpracovány i soubory obsahující informace o čipu, které jsou využívány pro přístup k obsahu čipu a zajištění integrity dat.

Na základě poskytnutých informací o čipu lze definovat následující požadavky:

- **Zajištění interoperability mezi backendem Trask ZenID a mobilním SDK:** jako vlastník produktu požaduji, aby rozhraní Trask ZenID backend bylo připraveno na možnost nahrání dat z bezkontaktního čipu. Zároveň je nezbytné zajistit, aby mobilní SDK umožnilo správné formátování extrahovaných dat z čipu pro zajištění interoperability s backendem.
- **Zobrazení dat přečtených z čipu:** jako vlastník produktu si přeji, aby data vyextrahovaná z bezkontaktního čipu byla zobrazena v DEMO aplikaci, což umožní úspěšné dokončení tohoto procesu.
- **Uložení přečtených informací:** jako vlastník procesu požaduji, aby všechny soubory včetně informací o čipu a držiteli dokladu, přečtené z bezkontaktního čipu, byly bezpečně uloženy společně se snímkem dokladu v rámci systému a přístupné přes administrátorské rozhraní backendu Trask ZenID.

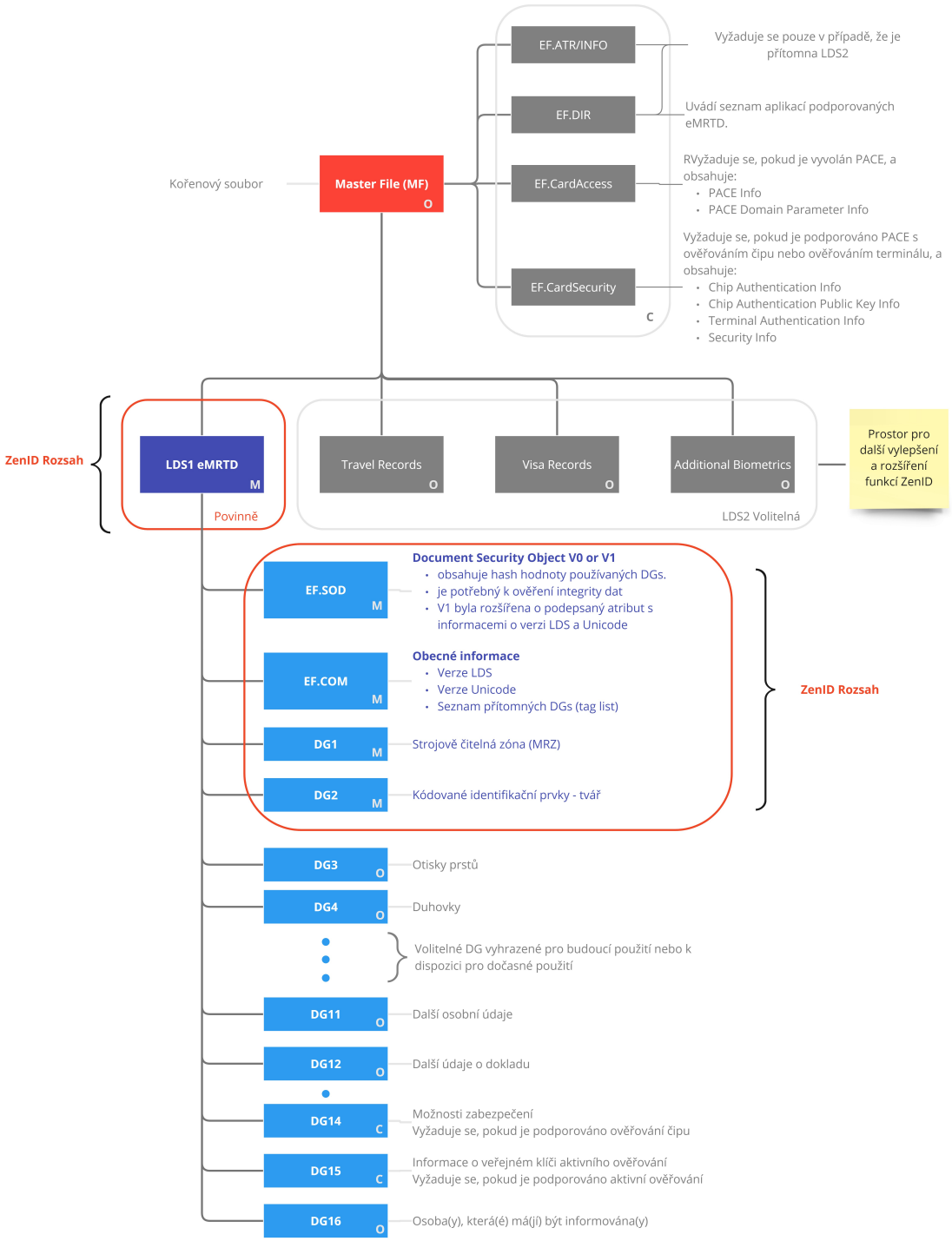
5.4 Bezpečnostní kontroly

Po definici obsahu bezkontaktních čipu v dokladech totožnosti nasledovala analýza mechanismů, které se využívají pro přístup a zpracování dat z čipů.

Bezkontaktní čipy v občanských průkazech a jiných identifikačních dokumentech nabízí různé bezpečnostní funkce a protokoly, které jsou zaměřeny na ochranu osobních a biometrických údajů držitele [51]. Mezi podporované bezpečnostní kontroly patří:

- Přístupové kontroly:
  - **Basic Access Control (BAC):** tento bezpečnostní mechanismus chrání komunikaci mezi čipem a čtečkou. Před čtením dat z čipu musí být zadán klíč, obvykle odvozený z tištěných informací na dokumentu, jako jsou datum narození, datum expirace a číslo dokumentu.
  - **Password Authenticated Connection Establishment (PACE):** jako vylepšení BAC, PACE vytváří silnější autentizaci a šifrování mezi čipem a čtečkou, poskytuje ochranu proti odposlechu a zaručuje důvěrnost a integritu přenesených dat.
  - **Extended Access Control (EAC):** tato vrstva zabezpečení se využívá hlavně k ochraně citlivějších biometrických údajů, jako jsou otisky prstů a skeny obličeje, a vyžaduje, aby čtečka prokázala své oprávnění k přístupu k těmto datům.
- Kontroly zajišťující autenticitu a integritu dat a samotného čipu:
  - **Passive Authentication (PA):** tato metoda kontroluje, že data uložená na čipu nebyla neautorizovaně změněna.
  - **Active Authentication (AA):** mechanismus zabraňuje neoprávněnému kopírování a klonování čipů tím, že vyžaduje od dokladu prokázání, že obsahuje soukromý klíč odpovídající veřejnému klíči uloženému v čipu.

Podle ICAO jsou inspekční systémy povinny nabízet podporu BAC a PA. Další typy kontrol jsou volitelné a mají být implementovány dle potřeb inspekčního systému. Přestože PACE není povinný k implementaci, ICAO doporučuje jeho využití, pokud je podporován čipem. Od ledna 2018 se u dokumentů implementujících PACE dle normy ICAO nevyžaduje implementace BAC z důvodu zpětné kompatibility. Od roku 2020 některé země přestaly podporovat BAC v nově vydávaných dokumentech a vyžadují PACE k získání přístupu k obsahu čipu [52].



Obrázek 5.2 Obsah čipu

Vzhledem k tomu, že EAC chrání data, která nejsou v zajmu Trask ZenID, o implementaci této kontroly zatím není uvažováno. Ačkoli AA poskytuje robustní bezpečnostní vrstvu odolnou proti kopírování čipu, jedná se o volitelnou kontrolu, která byla po dohodě s vedením zařazena do možného rozšíření modulu a nebude spadat do aktuálního rozsahu implementace.

Vzhledem k tomu součástí implementace modulu NFC budou BAC, PACE a PA. Za účelem lepšího pochopení a možnosti zapojení těchto kontrol do procesu verifikace je každá z nich zmapována podle ICAO 9303 č.11 do formátu BPMN 2.0 a následně analyzována pro definici požadavků.

5.4.1 Přístupové mechanismy

Bezkontaktní čipy jsou chráněny speciálními mechanismy řízení přístupu, které neumožňují přístup k obsahu čipu, pokud inspekční systém nedokáže prokázat své oprávnění. Rozlišují se dva základní bezpečnostní mechanismy: BAC (Basic Access Control) a PACE (Password Authenticated Connection Establishment).

BAC, nejstarší přístupový mechanismus používaný pro ochranu dat na čipech, je založen na symetrickém šifrování. PACE, který představuje vyšší úroveň bezpečnosti, využívá asymetrické šifrování a poskytuje klíče s vyšší entropií.

V rámci obou protokolů je prvním krokem zajištění, že inspekční systém provádějící čtení čipu disponuje informacemi odvozenými z fyzického dokladu. Tyto informace musí být systému poskytnuty ještě před možností čtení bezkontaktního čipu. Informace jsou obvykle získávány opticky z elektronicky strojově čitelných údajů (číslo dokladu, datum narození a datum vypršení dokladu), typicky z MRZ zóny, odkud mohou být potřebné informace extrahovány inspekčním systémem pomocí optického rozpoznávání znaků.

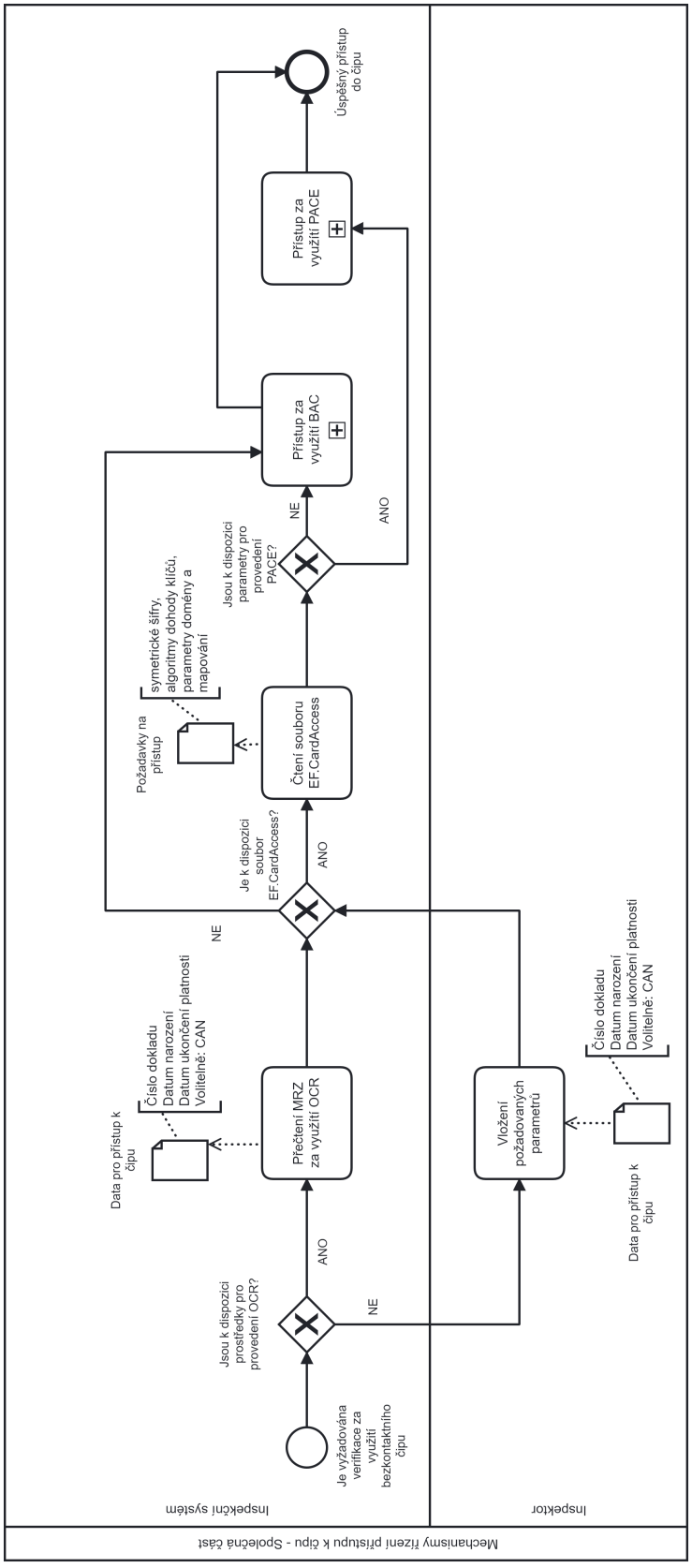
Dle informací v standardu ICAO se procedura přístupu k čipu pro autentizaci inspekčního systému skládá z následujících kroků (viz také diagram č. 5.3):[4]

1. Inspekční systém se pokusí přečíst soubor EF.CardAccess uložený v Master souboru.
2. Pokud je tento soubor na čipu nalezen a obsahuje bezpečnostní informace nezbytné pro použití protokolu PACE, doporučuje se jeho využití a proces pokračuje postupem definovaným pro PACE.
3. Pokud tento soubor neexistuje nebo neobsahuje informace pro připojení k čipu pomocí PACE, použije se protokol BAC a proces pokračuje postupem definovaným pro BAC.

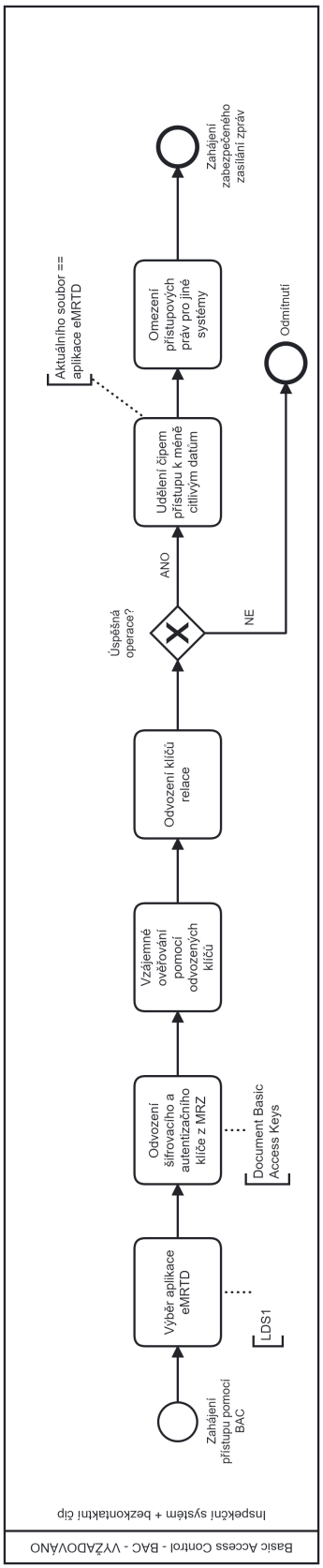
Basic Access Control

BAC začíná procesem, v němž inspekční systém odvodí Document Basic Access Key z informací uvedených v MRZ, konkrétně číslo dokladu, datum narození a datum vypršení platnosti dokladu. Následně se inspekční systém ověří vůči čipu s využitím odvozených klíčů a odvodí klíče relace pro výměnu informací. Pokud ověření proběhlo úspěšně, čip zajistí bezpečný kanál pro výměnu zpráv a potvrdí přístup inspekčního systému k souborům ve struktuře LDS1, které nemají dodatečnou ochranu a omezení přístupových práv jiných systémů, aby byla zajištěna bezpečnost výměny informací. V případě neúspěšného ověření, například z důvodu poskytnutí špatných klíčů, nebo pokusu o přístup k chráněným informacím bez ověření, k výměně informací nemůže dojít (viz také diagram č. 5.4).[5]

[4] Diagram byl vytvořen autorem na základě analýzy dokumentu ICAO 9303 č.11 [51].
[5] Diagram byl vytvořen autorem na základě analýzy dokumentu ICAO 9303 č.10 [50].



Obrázek 5.3 Mechanismy řízení přístupu k čipům (Společná část)



Obrázek 5.4 Basic Access Control (BAC)

Password Authenticated Connection Establishment

Proces začíná tím, že inspekční systém musí odvodit klíč z informací dané MRZ zónou (stejné atributy jako i pro BAC protokol). Alternativně může inspekční systém použít CAN kód, což je šestimístný kód uvedený na přední straně občanských průkazů. Pro účely Trask ZenID bylo rozhodnuto používat MRZ zónu, nikoli CAN kód. Inspekční systém se následně ověří vůči čipu prostřednictvím odvozeného klíče a získá klíče relace. Pokud vše proběhne úspěšně, stejně jako při využití BAC mechanismu, čip zajistí bezpečný kanál pro výměnu zpráv, potvrdí přístup inspekčního systému k méně citlivým souborům a omezí přístupová práva pro bezpečnou výměnu informací (viz také diagram č. 5.5).[6]

Navíc platí, že pokud během procesu přístupu k čipu nebo následně v průběhu procesu výměny informací dojde k přerušení komunikace mezi inspekčním systémem a bezkontaktním čipem, bezpečný kanál pro výměnu zpráv bude uzavřen a proces bude nutné zahájit od začátku.

Na základě poskytnuté analýzy byly definovány následující požadavky:

- **Detekce MRZ:** jako vlastník produktu potřebuji, aby procesu přístupu a čtení čipu předcházela detekce MRZ zóny a odvození nezbytných informací pro přístup k klíči pomoci OCR přímo na straně mobilního SDK.
- **Přístup k čipu:** jako vlastník produktu potřebuji, aby mobilní SDK umožňovalo přístup k čipu pomocí protokolu PACE, pokud je čipem podporováno, v opačném případě se má použít protokol BAC pro zajištění zpětné kompatibility se staršími verzemi dokladů.
- **Ztráta spojení:** jako vlastník produktu potřebuji, aby v případě, že během procesu přístupu nebo výměny informací mezi mobilním SDK a bezkontaktním čipem dojde k přerušení komunikace nebo ztrátě spojení, byl uživatel na tuto skutečnost upozorněn a proces verifikace pomocí bezkontaktního čipu bylo možné ihned opakovat.
- **Použití neplatného klíče:** jako vlastník produktu potřebuji, aby v případě použití neplatného klíče pro přístup k bezkontaktnímu čipu byl uživatel informován a měl možnost opakovat verifikační krok.
  - **Opakované selhání:** jako administrátor procesu chci mít možnost omezit počet povolených pokusů na opakování verifikace pomocí bezkontaktního čipu prostřednictvím administrátorského rozhraní aplikace, aby uživatel nezneužíval proces.

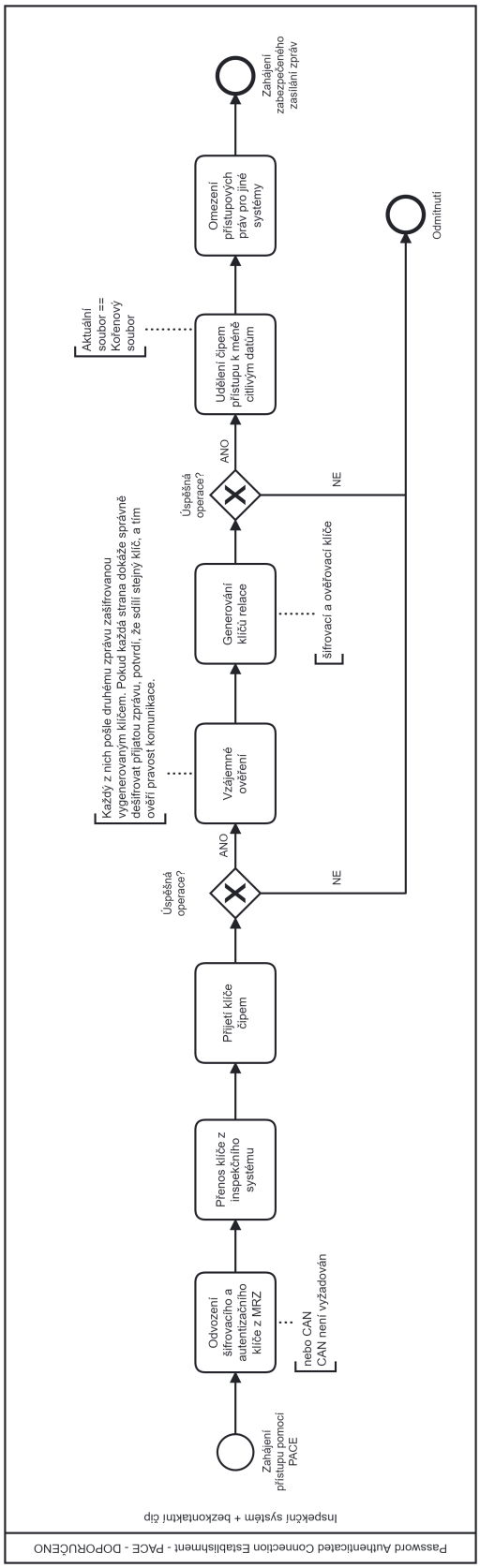
5.4.2 Passive Authentication - kontrola zajišťující autenticitu a integritu dat

Pasivní ověřování prokazuje, že informace uložené v dokumentu jsou autentické a nezměněné. Tento proces nezabraňuje kopírování obsahu bezkontaktního čipu ani záměně čipu. Objekt zabezpečení dokumentu (SOD) je digitálně podepsán vydávajícím státem nebo organizací a obsahuje hashové reprezentace obsahu čipu pro umožnění procesu pasivního ověřování.

Pro realizaci pasivního ověřování musí inspekční systém nejprve přečíst z bezkontaktního čipu bezpečnostní objekt dokumentu (SOD) a certifikát nazývaný Document Signer Certificate. Dále musí systém ověřit, že tento certifikát byl vystaven oprávněnou certifikační autoritou, a použít veřejný klíč podepisující autority k potvrzení podpisu. Po načtení údajů inspekční systém zkontroluje, zda obsah dat odpovídá, což se dělá porovnáním kontrolních součtů s hodnotami uloženými v objektu zabezpečení dokumentu (SOD) (viz také diagram č. 5.6) [51].[7]

Dále se doporučuje použití dodatečných kontrol, které se považují za nejlepší praxi:

[6] Diagram byl vytvořen autorem na základě analýzy dokumentu ICAO 9303 č.10 [50].
[7] Diagram byl vytvořen autorem na základě analýzy dokumentu ICAO 9303 č.10 [50].



Obrázek 5.5 Password Authenticated Connection Establishment (PACE)

- ověření konzistence mezi informacemi, které byly extrahovány z MRZ zóny pomocí OCR a daty, které byly uloženy na čipu v rámci DG1;
- porovnání konzistence mezi kódem státu uvedeným v Document Signer Certificate (DSC) nebo certifikační autoritě (CSCA);
- kontrola platnosti dokladu dle informací uložených v Document Signer Certificate (DSC).

Ověření certifikátu

Pro realizaci PA je nezbytné podrobněji se zaměřit na ověření certifikátu, kterým je podepsán obsah čipu. Nejprve jsou definovány některé základní pojmy (viz také obrázek č. 5.7):[8]

- **Country Signing Certification Authority (CSCA)** představuje hlavní autoritu, která vydává a spravuje certifikáty na úrovni státu. Tato autorita je zodpovědná za vydávání kořenových certifikátů. V České republice například tuto funkci plní Ministerstvo vnitra ČR.
- **Country Signing Certificate (CSC)** je self-signed certifikát, což znamená, že je podepsán pomocí soukromého klíče CSCA. Tento certifikát slouží jako důvěryhodný kořen pro autentizaci ostatních certifikátů vydaných CSCA.
- **Document Signer Certificate (DSC)** jsou certifikáty vydávané CSCA, které jsou používány pro podepisování elektronických pasů a občanských průkazů. Tyto certifikáty jsou také podepsány pomocí soukromého klíče CSCA.

  Pro ověření DSC:

- Veřejný klíč z CSC (kořenového certifikátu), který je široce distribuován a měl by být předem nainstalován v ověřovacích systémech nebo dostupný prostřednictvím důvěryhodného kanálu, je použit k ověření digitálního podpisu DSC.
- Ověření digitálního podpisu DSC se provádí použitím veřejného klíče. Pokud dešifrovaný obsah DSC po použití veřejného klíče CSCA odpovídá hashi uložené v DSC, lze důvěřovat, že DSC je validní a byl vydán důvěryhodnou CSCA.
- Kontrola platnosti certifikátu zahrnuje ověření vůči revokačním listům příslušné CSCA, aby se zjistilo, zda certifikát nebyl zneplatněn.

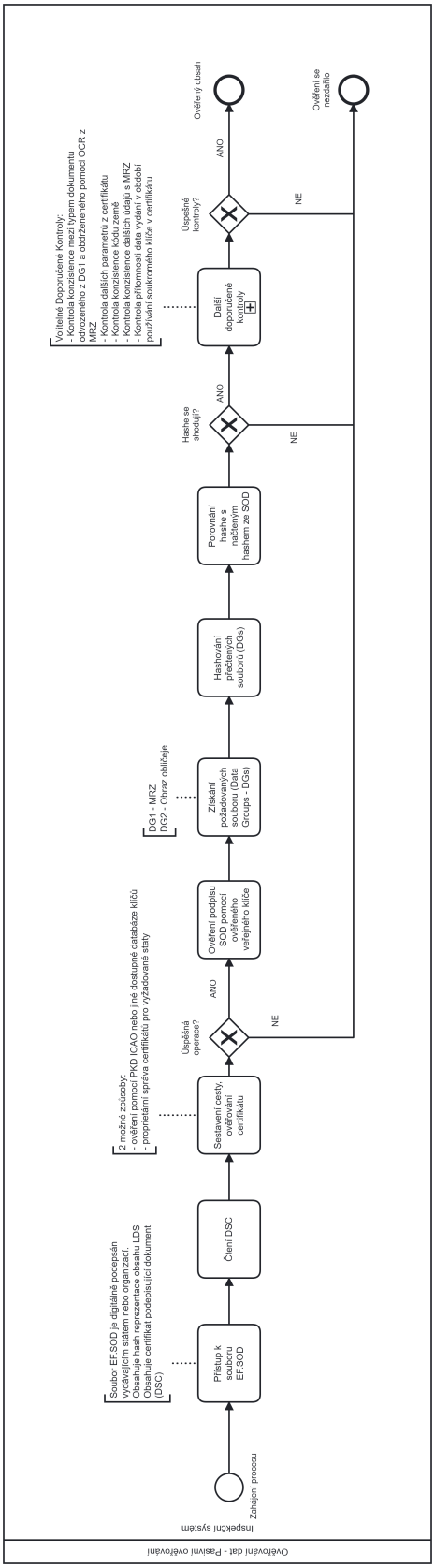
Správa certifikátů

K tomu, aby bylo možné ověřit DSC, musí inspekční systém předem disponovat platnými CSC a revokačními listy pro konkrétní CSCA státu, který vydal zkoumaný doklad.

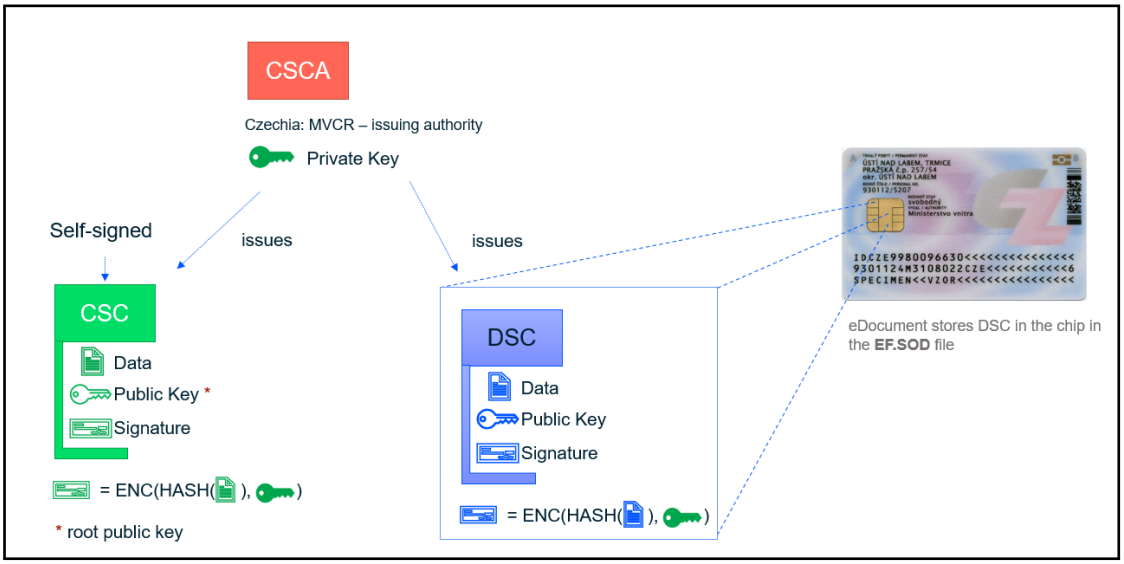
Existují dvě cesty pro získání těchto informací:

- **Ověření pomocí veřejných databází:** získání přístupu k seznamům, které fungují jako ”hub”pro přístup k většině států. Seznamy, které byly poskytnuty a spravovány důvěryhodnou organizací, byly identifikovány během vyhledávání.
- **Manuální správa:** manuální dohledání a správa zveřejněných certifikátů a revokačních listů všech certifikovaných autorit, na které je zaměřená implementace.

[8] Obrázek byl vytvořen autorem.



Obrázek 5.6 Pasivní ověřování dat



Obrázek 5.7 Vysvětlení hierarchie a struktury certifikátů

Ověření pomocí veřejných databází. První variantou jsou seznamy poskytované a spravované důvěryhodnou organizací, z nichž několik bylo úspěšně dohledáno [53].

ICAO PKD

Jednou z možností je databáze certifikátů a revokačních listů udržovaná a distribuovaná přímo organizací ICAO. PKD ICAO obsahuje DSC a CRL účastníků (států) PKD, kteří aktivně nahrávají svoje informace. Ačkoli všechny seznamy jsou veřejně publikovány a zdarma dostupné na stránkách ICAO, jejich využití v komerčních účelech je omezené [54]. Nicméně od roku 2021 byl ICAO spuštěn pilotní projekt s cílem zpřístupnit tyto seznamy pro soukromý sektor. Účastníci projektu získají plný přístup k seznamům a mohou je využívat pro své obchodní účely [55]. V rámci diplomové práce byla kontaktována příslušná autorita jménem Trask ZenID. Požadavek na využití jejich databáze byl odmítnut. Důvodem je to, že zatímco pilotní projekt je zaměřen na společnosti fungující v cestovním sektoru, Trask ZenID se primárně orientuje na finanční sektor. Přesto zástupce ICAO zmiňoval, že Trask ZenID bude informován v případě zmírnění podmínek pro přijetí společnosti do pilotního projektu.

The BSI Master List

Další podobnou databází je seznam udržovaný Spolkovým úřadem pro bezpečnost informací (BSI), který je německou vládní agenturou zodpovědnou za řízení počítačové a komunikační bezpečnosti pro německou vládu. Využití jejich seznamu také klade omezení na komerční užití [56].

Manuální správa. Vzhledem k potřebě realizace PA bylo rozhodnuto využit cestu ruční údržby a správy certifikátů a revokačních listů. Hlavními nevýhodami jsou: nedostatečná možnost okamžitě poskytovat podporu pro všechny státy; komplikace spojené s dohledáním zdrojů s veřejnými certifikáty; a nutnost implementace mechanismu pro průběžné sledování změn na webových stránkách CSCA. Přidání nového certifikátu může navíc způsobit zdržení mezi vydáním dokladu podepsaného novým certifikátem a zajištěním podpory Trask ZenID.

Jako první se tým Trask ZenID rozhodl zahájit podporu v České republice, kde jako Certi-

fikační Autorita vystupuje Ministerstvo vnitra České republiky. Odkazy na zdrojové stránky s certifikáty a revokačními listy jsou uvedeny níže:

- `https://www.mvcr.cz/clanek/csca-certificate-revocation-list.aspx`
- `https://www.mvcr.cz/clanek/ceska-narodni-certifikacni-autorita-csca-2021.aspx`

Na základě poskytnuté analýzy byly definovány následující požadavky:

- **Pasivní ověřování:** jako vlastník procesu potřebují, aby na data obdržená z čipu byl aplikován mechanismus pasivního ověřování, který zajistí jejich autenticitu a integritu.
  - **Monitorování webu CSCA:** jako vlastník procesu potřebuji, aby na straně Trask ZenID byl implementován proces průběžně hlídající webové stránky CSCA s dostupnými certifikačními a revokačními listy a informoval vývojáře v případě, že byly zveřejněny nové certifikáty pro následnou aktualizaci podpůrných dat.
  - **Správa certifikátů:** jako vlastník procesu potřebuji, aby Trask ZenID mělo uložené certifikáty a revokační listy pro příslušnou certifikační autoritu, která se využije během investigace dat z čipu.
  - **Zobrazení výsledků kontrol:** jako vlastník procesu potřebuji, aby veškeré výsledky kontrol aplikované na data získaná z čipu, byly uloženy a přístupné prostřednictvím administrátorského rozhraní Trask ZenID.

Nové požadavky na proces vychazející z analýzy

Po diskuzi s týmem byly definovány další požadavky na proces:

- **Časování verifikačního kroku:** jako vlastník procesu potřebuji, aby administrátory procesu měli nástroj pro řízení doby, která je nezbytná pro dokončení verifikace pomocí bezkontaktního čipu, a to prostřednictvím administrátorského rozhraní aplikace, aby v případě neočekávaných potíží nedocházelo k zaseknutí celého procesu.
- **Absence dat z čipu:** jako vlastník procesu potřebuji, aby byli administrátoři procesu upozorněni během investigace celého procesu identifikace, když dokument byl nahrán bez obsahu čipu, i když byl obsah vyžadován.
- **Křížové kontroly:** jako vlastník procesu potřebuji, aby součástí validace byly provedeny křížové kontroly mezi daty vyčtenými z čipu a obdrženými z dalších verifikačních kroků, zejména porovnání fotografie z kroku Selfie/Liveness vůči fotografii vyčtené z čipu, a porovnání viditelné fotografie na dokladu vůči fotografii vyčtené z čipu.
- **Autokorekce:** jako vlastník procesu potřebuji, aby data obdržená během OCR byla automaticky přepsána daty vyčtenými z čipu pro zajištění správnosti informací o uživateli a předcházení možným nepřesnostem během OCR.
- **Reporting:** jako vlastník procesu potřebuji, aby byl modul Reporting rozšířen o agregované informace spojené s procesem verifikace pomocí bezkontaktních čipů pro jednoduché odhalení případných problematických částí a zlepšení celkového uživatelského zážitku.

5.5 Rozšíření procesu zpracování digitálních dokladů

Na základě již definovaných požadavků byl rozšířen původní odhad procesu identifikace pomocí bezkontaktních čipů a zmapován s větší mírou detailů pomocí rozšířené notace BPMN 2.0. Při mapování byla stále zachována určitá míra zjednodušení, obzvláště během mapování procesů, které nejsou přímo součástí implementace nového modulu. Procesy skenování dokladu, ověření

hologramu, procházení procesem vyfocení obličeje nebo ověření živosti jsou označeny pouze jako subprocesy a nejsou dále analyzovány. Tento diagram poskytuje plnou představu o tom, jaké výjimky, alternativní cesty a chybové hlášky mají být znázorněny při návrhu jak SDK, tak i DEMO aplikace.

Celý proces včetně textové dokumentace je dostupný jako příloha D této práce.[9] V rámci této sekci jsou zvlášť popsány dvě části procesu: detekce a čtení MRZ (viz část diagramu na obrázku č. 5.8) a přístup a čtení čipu vestavěného do dokladu totožnosti (viz část diagramu na obrázku č. 5.9).[10] Tyto dílčí procesy, probíhající jako interakce mezi klientskou aplikací využívající proprietární mobilní SDK a koncovým uživatelem, vyžadují podrobnější vysvětlení.

Jak již bylo uvedeno v sekci č. 4.2.1, SDK je navrženo tak, aby detekovalo a četlo MRZ zónu. Primárně to slouží k detekci dokladu obsahujícího čip s digitálními údaji a, pokud je tato podmínka splněna, dojde k využití dat z MRZ zóny pro odvození klíče pro přístup k čipu. V důsledku těchto požadavků byl původní proces modifikován. Úprava je znázorněna na části diagramu č. 5.8. Během skenování strany dokladu uživatelem na pozadí probíhá proces, který v okamžiku detekce MRZ zóny aktivuje její čtení pomocí OCR. Tento proces je nezávislý na straně dokladu, jelikož SDK nemusí předem vědět, který doklad se očekává a která strana obsahuje MRZ zónu.

Další zásadní úpravou je zavedení procesu přístupu a čtení bezkontaktního čipu, který probíhá pouze v případě, že čip byl detekován a MRZ přečtena. Zmapovaný podproces, vyříznutý z celého procesu identifikace, je uveden na obrázku č. 5.9.

SDK nejprve ověří, zda má přístup k NFC čtečce mobilního zařízení a zda je čtečka připravena k použití. Pokud některá z podmínek není splněna, vyzve uživatele k zásahu do systémových nastavení zařízení. V dalším kroku začíná proces přístupu k čipu. Při detekci signálu bezkontaktního čipu prostřednictvím NFC čtečky zahájí SDK proces inicializace dle popsaného přístupového mechanismu (viz sekce č. 5.4.1). V případě úspěšného přístupu dojde k načtení dat uložených na čipu. Úspěšné dokončení tohoto procesu bude oznámeno a uživatel uvidí přečtená a dekódovaná data na obrazovce zařízení.

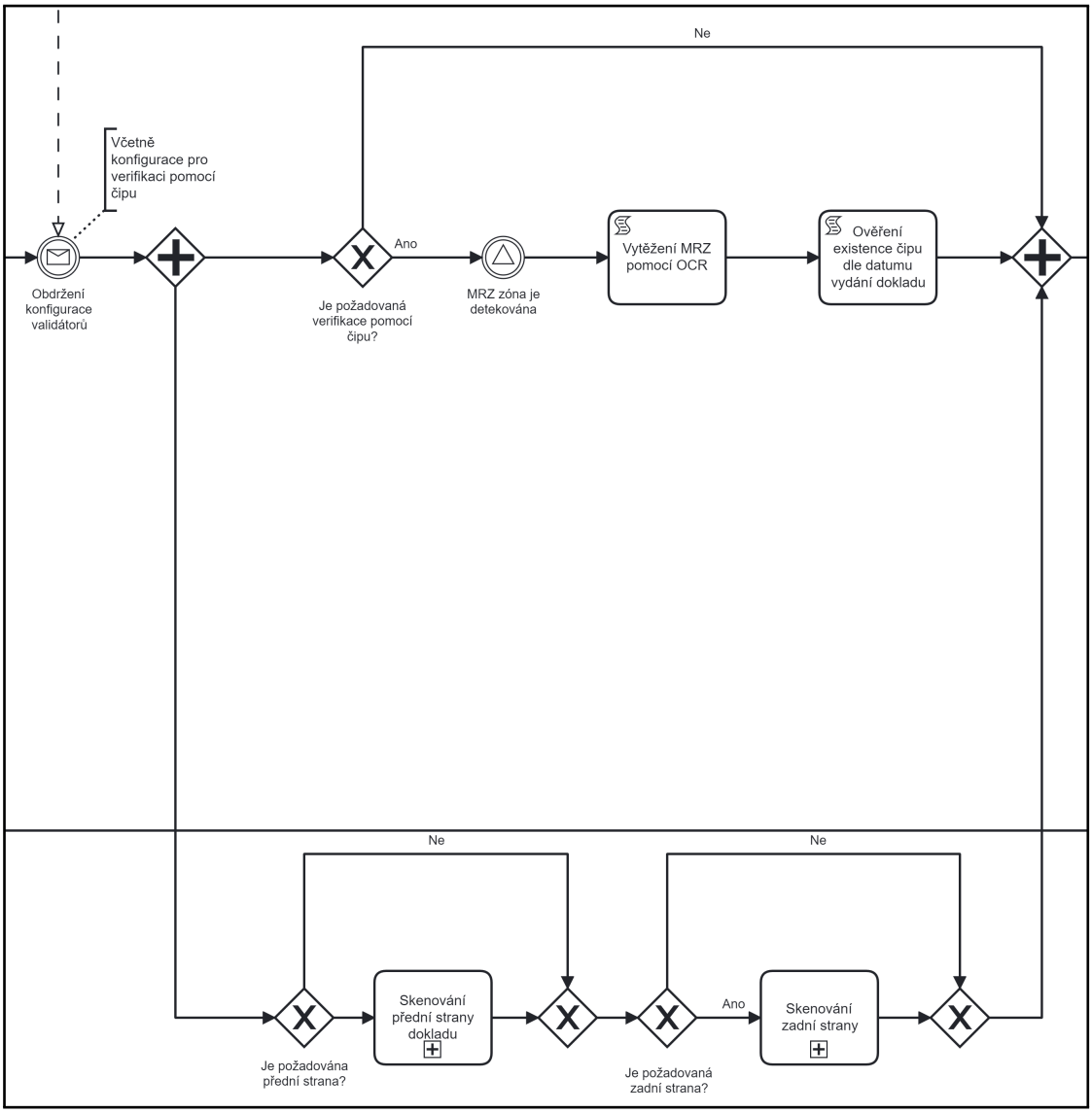
Pokud během procesu dojde k chybám, jako je odmítnutí přístupu z důvodu nesprávně použitého klíče nebo vypršení časového limitu vyhrazeného pro tento verifikační krok, aktivuje se výjimečná cesta procesu. SDK pak posoudí, zda uživateli zbývají nepoužité pokusy pro daný verifikační krok a zda je možné proces opakovat. Pokud administrátor procesu dovoluje přeskočení daného verifikačního kroku, vyzve se uživatele k potvrzení. Jinak se proces musí začít znovu. Méně prioritní výjimku, ztrátu spojení během práce s bezkontaktním čipem, SDK řeší tak, že uživatele informuje o možnosti okamžitého opětovného zahájení verifikace bez penalizace za ztrátu pokusu. Po úspěšném dokončení verifikace pomocí bezkontaktního čipu se přejde k dalšímu verifikačnímu kroku, pokud takový existuje.

5.6 Seskupení požadavků a tvorba uživatelských příběhů

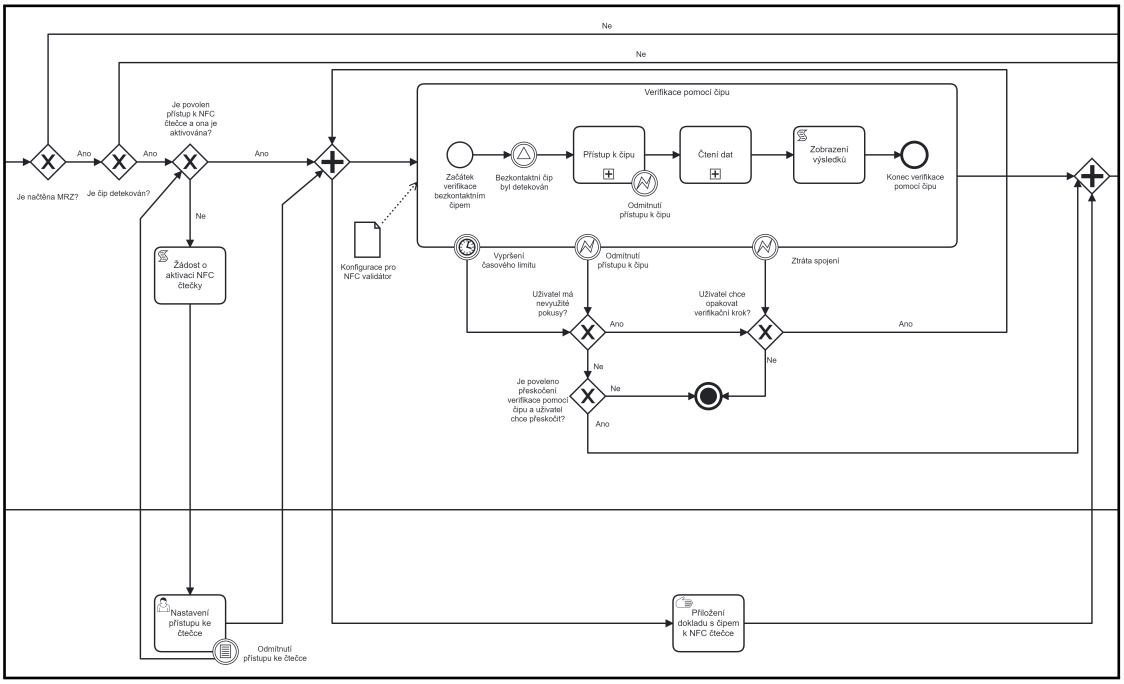
Po definici obecných požadavku došlo k jejich seskupení a transformaci do uživatelských příběhů, které lze přímo použít během plánování a implementace projektu. Pro účely této diplomové práce jsou příběhy prezentovány ve zkrácené formě a mohou odkazovat na implementační detaily, aniž by je podrobně popisovali.

Uživatelské příběhy jsou rozděleny do tří hlavních skupin podle prostředí, do kterého budou začleněny. V první řadě byly definovány příběhy pro jádro systému a pro mobilní SDK. Definice požadavků pro demo aplikaci byla spojena s tvorbou wireframu.

[9] Diagram procesu a jeho dokumentace byly vytvořeny autorem.
[10] Diagramy byly vytvořeny autorem na základě výstupů analýzy.



Obrázek 5.8 Detekce a čtení strojové čitelné zóny



Obrázek 5.9 Detekce a čtení čipu

5.6.1 Rozšíření jádra systému

US1: Licenční server

Jako správce systému chci mít možnost řízení a aktivace nového NFC modulu, abych měl plnou kontrolu nad jeho využitím zákazníky.

Doplňující informace:

- Implementace nového příznaku pro modul NFC v licenčním serveru.
- Přístup zákazníků k funkcím NFC modulu je závislý na jeho aktivaci.

Reference: vytvořeno na základě stanoveného způsobu licencování v části č. 4.3.3.

US2: Zajištění interoperability mezi backendem Trask ZenID a mobilním SDK

Jako vývojář mobilního SDK chci, aby rozhraní Trask ZenID backendu bylo připravené na možnost nahrávání dat z bezkontaktního čipu, abych mohl zajistit interoperabilitu s SDK.

Doplňující informace:

- Nutnost navrhnout a upravit stávající rozhraní Trask ZenID o nové atributy pro možnost nahrávání dat z bezkontaktního čipu.
- Pro návrh rozhraní lze využít specifikace obsahu a struktury dat uložených v čipu, které jsou popsané v kapitole c. 5.3.
- Data z čipu se přenášejí v zakódované formě a ve stejném formátu, v jakém jsou uložena na čipu.

- Součástí požadavku na rozhraní jsou všechny soubory obsažené v LDS1 a informace o úspěšnosti procesu.
- Možné statusy odpovídající úspěšnosti procesu zahrnují: úspěšné dokončení verifikace, uživatel přeskočil proces verifikace, doklad neobsahuje bezkontaktní čip, mobil nedisponuje NFC čtečkou.

Reference: vytvořeno na základě požadavků Zaznamenání přeskočení (viz sekce č. 5.1), Nedefinované chování (viz sekce č. 5.2), Zajištění interoperability mezi backendem Trask ZenID a mobilním SDK (viz sekce č. 5.3.4).

US3: Zpřístupnění dat z čipu v administrátorském rozhraní

Jako správce procesu chci mít přehled o datech nahraných z čipu v rámci detailu dokumentu, aby byl zajištěn snadný přístup k těmto datům.

Doplňující informace:

- V detailu dokumentu mají být místo informací získaných pomocí OCR zobrazena data vyčtená z bezkontaktního čipu.
- Data z bezkontaktního čipu musí být jasně odlišena od ostatních polí v rozhraní.

Reference: vytvořeno na základě požadavků Autokorekce (viz sekce č. 5.4.2), Uložení přečtených informací (viz sekce č. 5.3.4).

US4: Pasivní Ověřování

Jako správce procesu potřebuji mít přehled o autenticitě a integritě dat, aby bylo možné zajistit bezpečnost procesu.

Doplňující informace:

- Po načtení dat z bezkontaktního čipu mají být na ně aplikovány kontroly požadované pro pasivní ověřování.
- Pro návrh kontrol lze využít specifikaci procesu definovanou v sekci č. 5.4.2.
- Výsledky kontrol mají být uloženy společně s daty obdrženými z bezkontaktního čipu v rámci detailu načteného dokladu.

Reference: vytvořeno na základě požadavků Zobrazení výsledků kontrol (viz sekce č. 5.4.2), Pasivní ověřování (viz sekce č. 5.4.2), Absence dat z čipu (viz sekce č. 5.4.2).

US5: Backend NFC validátor

Jako vlastník procesu chci, aby byl do seznamu validátorů přidán nový NFC validátor patřící k NFC modulu, aby bylo možné spustit kontroly pro validaci dat vyčtených z čipu v rámci investigací.

Doplňující informace:

- NFC validátor je binární a složený; pokud je jeho hodnota nastavena na 100, je aktivní v rámci investigace daného profilu, pokud je jeho hodnota 0, není aktivní.
- NFC validátor se má spouštět u investigací, které byly odeslány z mobilního SDK za předpokladu, že verifikace bezkontaktního čipu byla součástí celého procesu verifikace.

- Validátor má ověřit, že součástí vzorku obdrženého z SDK jsou metadata z čipu; pokud data nebyla detekována, validátor má selhat.
- Validátor má opakovaně provést pasivní ověřování dat a související kontroly; v případě selhání validátor spadne a důvod selhání uvede v detailu investigace.
- NFC validátor je dostupný ke konfiguraci pouze pokud klient má zpřístupněný NFC Modul v nabídce.

Reference: vytvořeno na základě požadavků Absence dat z čipu (viz sekce č. 5.4.2), Pasivní ověřování (viz sekce č. 5.4.2), Zobrazení výsledků kontrol (viz sekce č. 5.4.2).

US6: Rozšířená konfigurace procesu pro mobilní SDK

Jako vlastník produktu chci umožnit zákazníkům rozšířenou konfiguraci procesu verifikace pomocí bezkontaktního čipu, aby bylo možné aplikaci přizpůsobit a neomezovat ji na jeden konkrétní případ použití.

Doplňující informace:

- Uživatelé mohou z backendu konfigurovat některá nastavení modulu NFC:
  - Časový limit procesu: doba v sekundách od zahájení procesu identifikace pomocí bezkontaktního čipu. Vypršení může být způsobeno poškozením antény nebo čipu, špatnou polohou karty vůči telefonu, nebo příliš dlouhým procesem přístupu nebo čtení.
  - Počet opakovaných pokusů: limit pro počet pokusů dostupných pro opakování daného verifikačního kroku. Po vyčerpání všech pokusů není možné proces opakovat.
  - Možnost přeskočení kontroly: správce může umožnit přeskočení kroku NFC v případě vyčerpání časového limitu, vypršení pokusů nebo absence NFC čtečky.

Reference: vytvořeno na základě požadavků Umožnění přeskočení verifikace pomoci čipu (viz sekce č. 5.1), Nedefinované chování (viz sekce č. 5.2), Opakované selhání (viz sekce č. 5.4.1), Použití neplatného klíče (viz sekce č. 5.4.1), Časování verifikačního kroku (viz sekce č. 5.4.2).

US7: Porovnání fotografie z čipu se Selfie

Jako vlastník produktu chci rozšířit stávající seznam validátorů o novou kontrolu porovnání obličeje držitele dokladu přečteného z bezkontaktního čipu (pokud je dostupné) s nahraným obrázkem obličeje v rámci Selfie/Liveness kontroly, pro zlepšení přesnosti a bezpečnosti celého procesu.

Doplňující informace:

- Analogový validátor by měl být použit pro kontrolu shody fotografii získanou z bezkontaktního čipu a fotografii obličeje z navazujícího verifikačního kroku Selfie/Liveness, pokud jsou obě fotografie dostupné.

Reference: vytvořeno na základě požadavků Křížové kontroly (viz sekce č. 5.4.2).

US8: Porovnání dat z čipu vůči informacím na dokladu

Jako vlastník produktu chci mít možnost porovnat informace zobrazené na dokladu totožnosti s údaji získanými z čipu, abych si mohl být jistý integritou a pravostí dokumentu.

Doplňující informace:

- Během investigace se porovnají data získaná z dokladu prostřednictvím OCR a data z bezkontaktního čipu (pokud je čip dostupný).
- Validátor se aktivuje, pokud proces OCR dosáhne dostatečné úrovně důvěryhodnosti pro spuštění dalšího porovnání.

Reference: vytvořeno na základě požadavků Křížové kontroly (viz sekce č. 5.4.2).

US9: Úprava GUI pro rozlišení vzorků a vyšetřování s daty z čipu

Jako tester Trask ZenID chci mít na kartách vzorků a investigací jasný přehled o tom, které záznamy obsahují data z bezkontaktního čipu a které ne, abych nemusel otevírat každý detail záznamu pro zjištění této informace.

Doplňující informace:

- Umístění ikony indikující přítomnost dat získaných pomoci NFC (viz sekce č. 5.2).

Reference: vytvořeno na základě požadavků Uložení přečtených informací (viz sekce č. 5.3.4), Absence dat z čipu (viz sekce č. 5.4.2), Zobrazení výsledků kontrol (viz sekce č. 5.4.2).

US10: Integrace a správa certifikátů CSCA pro PA

Jako administrátor potřebuji, aby systém nejen průběžně monitoroval a automaticky informoval vývojáře o nově zveřejněných certifikačních a revokačních listech na webových stránkách CSCA, ale také zajišťoval správné ukládání a aktualizaci těchto informaci v rámci systému.

Doplňující informace:

- Systém pravidelně kontroluje webové stránky CSCA a automaticky odesílá upozornění na nové nebo změněné certifikáty a revokační listy.
- Trask ZenID správně ukládá všechny relevantní certifikáty a revokační listy, které jsou neustále aktualizovány.
- Administrátor má k dispozici nástroje pro snadné přidávání, odstraňování a aktualizaci certifikátů.
- Všechny operace spojené s certifikáty jsou logovány a auditovatelné.
- Systém pravidelně ověřuje platnost uložených certifikátů a informuje o potřebě jejich aktualizace.

Reference: vytvořeno na základě požadavků Monitorování webu CSCA (viz sekce č. 5.4.2), Správa certifikátů (viz sekce č. 5.4.2).

US11: Rozšíření modulu Reporting o agregované informace z procesu verifikace
Jako vlastník procesu potřebuji, aby modul Reporting byl rozšířen o agregované informace z procesu verifikace pomocí bezkontaktních čipů pro jednodušší identifikaci problematických oblastí a zlepšení celkového uživatelského zážitku.

Doplňující informace:

- Data zahrnují statistiky úspěšnosti verifikace, dobu trvání jednotlivých kroků, frekvenci výskytu chyb a další relevantní metriky.

- Systém umožňuje filtrovat a třídit data podle různých parametrů (např. datum, typ zařízení, výsledek verifikačního kroku).
- Reporty mohou být exportovány do běžných formátů (např. CSV, PDF).
- Dashboard modulu Reporting obsahuje vizuální reprezentace dat pro lepší vizualizaci a analýzu.

Reference: vytvořeno na základě požadavků Reporting (viz sekce č. 5.4.2).

5.6.2 Rozšíření možnosti mobilního SDK

US1: Detekce bezkontaktního čipu

Jako vlastník procesu chci, aby SDK dokázalo rozpoznat, zda dokument podporuje čtení bezkontaktního čipu, aby v případě absence bezkontaktního čipu mohl být tento krok automaticky přeskočen.

Doplňující informace:

- Detekce čipu probíhá na základě vytvořeného číselníku (viz příloha E).
- Hodnoty načtené z MRZ (datum vydání, model dokladu) se použijí k ověření, zda je pro daný typ dokumentu čip integrován.
- Vytváření číselníku pro detekci je průběžný proces, který je možné na požádání rozšiřovat.

Reference: vytvořeno na základě požadavků Detekce bezkontaktního čipu (viz sekce č. 5.2), Detekce MRZ (viz sekce č. 5.4.1).

US2: Zpracování MRZ

Jako vlastník procesu chci zajistit, aby procesu přístupu a čtení čipu předcházela detekce MRZ zóny a vyčtení nezbytných informací pro přístup k klíči přímo v rámci mobilního SDK.

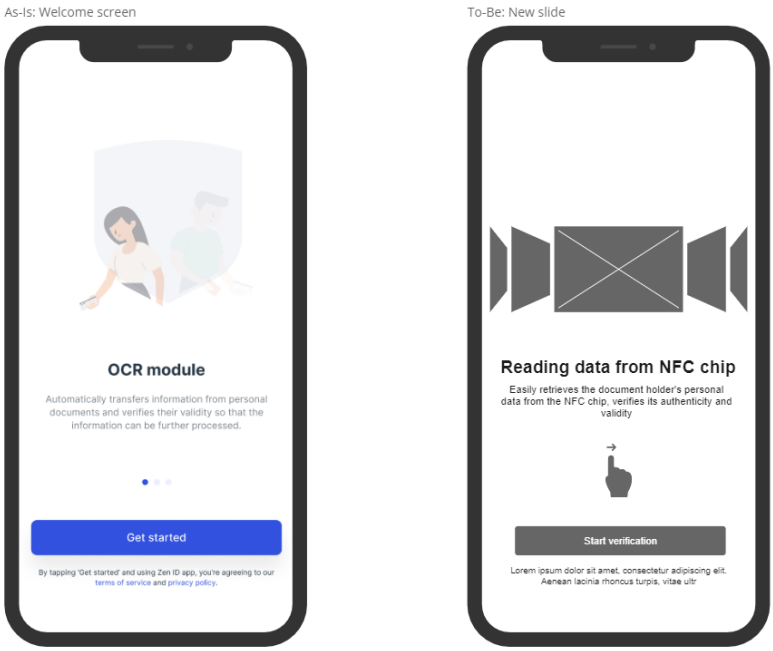
Doplňující informace:

- MRZ čtečka má být spouštěna vždy, když je verifikace pomocí bezkontaktního čipu součástí procesu identifikace.
- Jakmile je detekována strana dokumentu obsahující MRZ, data z MRZ jsou vyčtena a zparsována pro umožnění přístupu k čipu.

Reference: vytvořeno na základě požadavků Detekce bezkontaktního čipu (viz sekce č. 5.2), Detekce MRZ (viz sekce č. 5.4.1), Přístup k čipu (viz sekce č. 5.4.1).

5.7 Příprava prototypu, rozšíření DEMO aplikací

Pro účely integrace byl navržen rozšířený a upravený existující systém aplikace o nové komponenty nutné pro verifikaci pomocí bezkontaktních čipů. Návrh byl vytvořen prostřednictvím Wireframe v aplikaci Miro.com a podle definovaného procesu. Pokud se změna týkala pouze úprav existující obrazovky, byl do popisu zařazen obrázek aktuálního stavu aplikace a popis navržené změny. Pro kompletně nové komponenty je znázorněn návrh obrazovky. K jednotlivým



Obrázek 5.10 Úprava seznamovací komponenty

funkčním celkům a omezeným úpravám byly vytvořeny příslušné uživatelské příběhy pro možnost implementace. High-fidelity prototyp bude vytvořen specialistou po schválení původního návrhu.

US1: Úprava seznamovací komponenty

Jako uživatel mobilní DEMO aplikace chci mít ihned po spuštění aplikace k dispozici stručný popis podporovaných funkcí, abych si byl vědom možností jejího používání.

Doplňující informace:

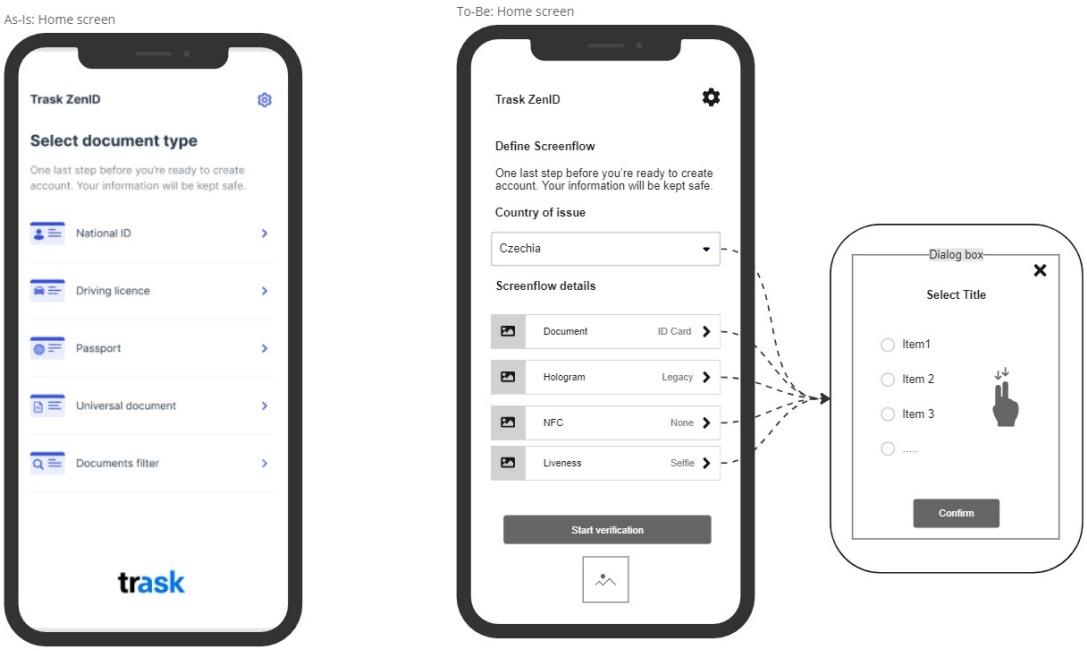
- Aktuální komponenta zahrnuje čtyři obrázky pro stávající moduly: Modul OCR, Kontrola hologramu, Rozpoznání obličeje a Kontrola živosti.
- Plánuje se přidání nového obrázku pro modul NFC, který bude uživatele informovat o načítání a ověření osobních údajů z bezkontaktního čipu.
- Navrhované pořadí obrázků pro optimalizaci uživatelského zážitku: Modul OCR, Kontrola hologramu, Načtení čipu pomoci NFC, Rozpoznání obličeje, Kontrola živosti.
- Pro rozšířený návrh komponenty a následnou implementací se má použit prvotní návrh uvedený na obrázku č. 5.10.

US2: Reorganizace úvodní obrazovky

Jako uživatel mobilní DEMO aplikace chci mít možnost nastavit požadovaný průběh aplikace přímo z domovské obrazovky, abych měl jasnou a přehlednou definici procesu.

Doplňující informace:

- Základní funkce pro nastavení procesu, jako výběr typu dokladu a konfigurace skenování, budou přesunuty z nastavení na úvodní obrazovku.



Obrázek 5.11 Reorganizace úvodní obrazovky

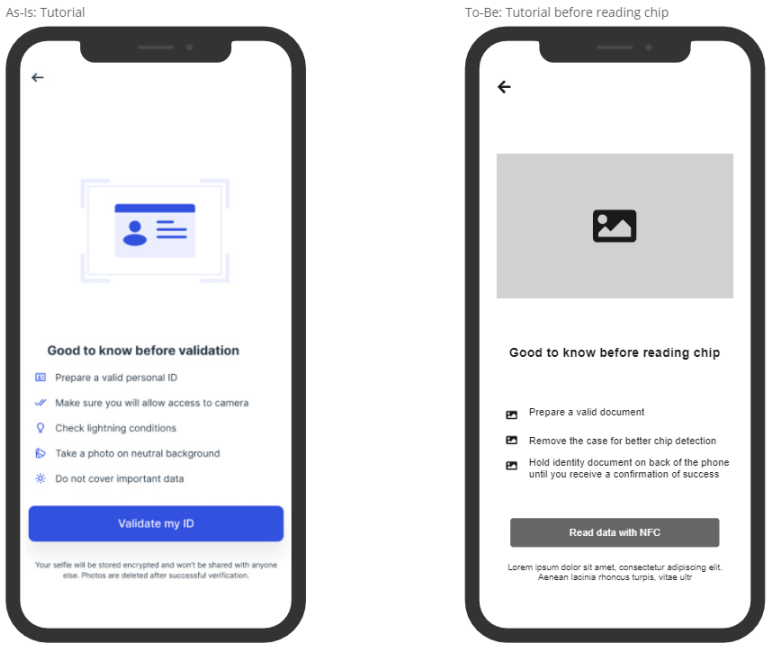
- Nová úvodní obrazovka umožní uživatelům přizpůsobit průběh verifikace přes interaktivní prvky pro výběr dokumentu, režimu hologramu, čtení bezkontaktního čipu a kontroly živosti.
- Je potřeba zajistit přidání nových kontrol pro správný výběr průběhu procesu a odstranění nadbytečných nastavení ze záložky Nastavení.
- Pro rozšířený návrh komponenty a následnou implementací se má použit prvotní návrh uvedený na obrázku č. 5.11.

US3: Tutoriál a aktivace NFC čtečky

Jako uživatel mobilní DEMO aplikace chci, aby se před samotným procesem verifikace pomocí bezkontaktního čipu zobrazovala obrazovka s popisem procesu, abych měl přehled o nadcházejícím průběhu čtení čipu.

Doplňující informace:

- Před zahájením procesu verifikace pomoci bezkontaktního čipu se zobrazí nová informativní obrazovka (viz obrázek č. 5.12).
- Před zahájením procesu uživatel má být vyzván k aktivaci čtečky NFC, pokud není aktivní (viz obrázek č. 5.13).
- Uživatel nemůže pokročit v procesu dál, dokud nebudou aktualizované systémové nastavení umožňující práce s NFC čtečkou.
- Pokud čtečka NFC není k dispozici na daném zařízení, uživatel bude informován o této skutečnosti.
- Chybová obrazovka bude obsahovat možnost přechodu na domovskou obrazovku nebo přeskočení kontroly, pokud je to povoleno správcem systému.



Obrázek 5.12 Úprava tutoriálu

- V případě, že dokument neobsahuje čtečku a přeskočení není povoleno, uživatel bude informován, že tato verifikace není pro jeho zařízení podporovaná.

Reference: vytvořeno na základě požadavků Umožnění přeskočení verifikace pomoci čipu (viz sekce č. 5.1), Řízení NFC čtečky (viz sekce č. 5.1), Neaktivní NFC čtečka (viz sekce č. 5.1).

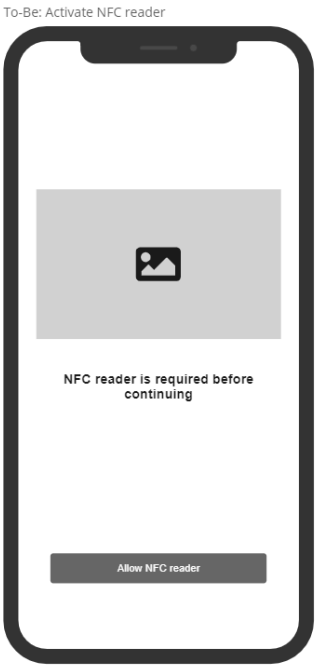
US4: Ukazatel pokroku

Jako uživatel mobilní DEMO aplikace chci mít k dispozici během práci s bezkontaktním čipem responzivní komponentu v rámci uživatelské rozhraní, abych byl informován o probíhajících procesech a jejich výsledcích.

Doplňující informace:

- Při čtení bezkontaktního čipu se zobrazuje progresivní pruh, který reaguje na tři možné události: přístup k čipu, čtení dat a čtení fotografie (viz obrázek č. 5.14).
- Pokud dojde k potížím během přístupu k čipu, ztrátě spojení nebo vypršení časového limitu, zobrazí se odpovídající chybová hlášení (viz obrázek č. 5.15)
- Pokud správcem systému je umožněné přeskočení a uživatel vyčerpal všechny pokusy, bude uživateli navržená možnost přeskočit tento verifikační krok. Jinak musí uživatel proces opakovat. (Detailnější informace k ošetření výjimek během procesu verifikace lze naleznout v rámci návrhu BPMN procesu - viz diagram č. D.1, nebo v rámci znázorněného screenflow aplikace - viz soubor ”Screenflow.pdf”v části č. E)
- Po úspěšném načtení čipu se zobrazí příslušná výslední obrazovka (viz obrázek č. 5.15).

Reference: vytvořeno na základě požadavků Umožnění přeskočení verifikace pomoci čipu (viz sekce č. 5.1), Ztráta spojení (viz sekce č. 5.4.1), Použití neplatného klíče (viz sekce č. 5.4.1),



Obrázek 5.13 Aktivace NFC čtečky

Opakované selhání (viz sekce č. 5.4.1), Časování verifikačního kroku (viz sekce č. 5.4.2).

US5: Zobrazení návodu během verifikace

Jako uživatel mobilní DEMO aplikace chci mít podrobný popis procesu práce s bezkontaktním čipem, abych věděl, jaké akce a jak je mám provést, abych dosáhl úspěšného přístupu k čipu a jeho ověření.

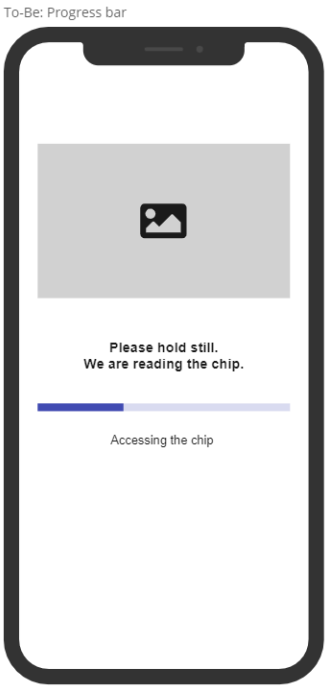
Doplňující informace:

- Kolotoč s podrobným popisem procesu čtení čipu se zobrazuje po přechodu z výukové obrazovky na krok přístupu k čipu a jeho ověření.
- Obsahuje 3 snímky s instrukcemi pro uživatele, každý s časovým limitem pro automatické prohlédnutí obsahu.
- Automatické posouvání snímků se zastaví po manuálním posunu uživatelem.
- Uživatel může kdykoli zavřít kolotoč a vrátit se na výukovou obrazovku.
- Animace v kolotoči zohledňují typ dokumentu (např. občanský průkaz, pas).
- Pro rozšířený návrh komponenty a následnou implementací se má použit prvotní návrh uvedený na obrázku č. 5.17.

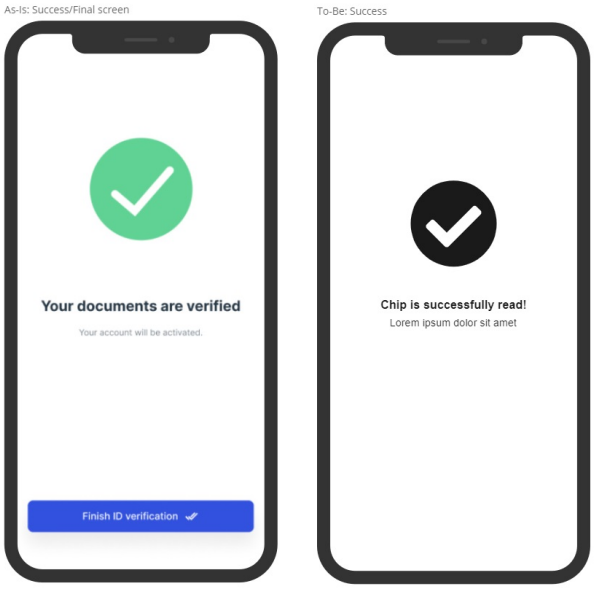
US6: Zobrazení dat z bezkontaktního čipu

Jako tester mobilní DEMO aplikace chci mít přehled o datech a výsledcích validací z vestavěného čipu, abych měl informace o načtených datech a provedených validacích.

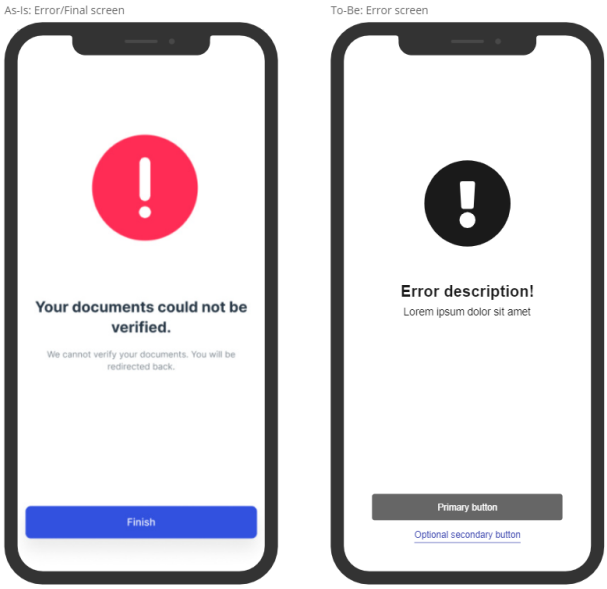
Doplňující informace:



Obrázek 5.14 Ukazatel pokroku

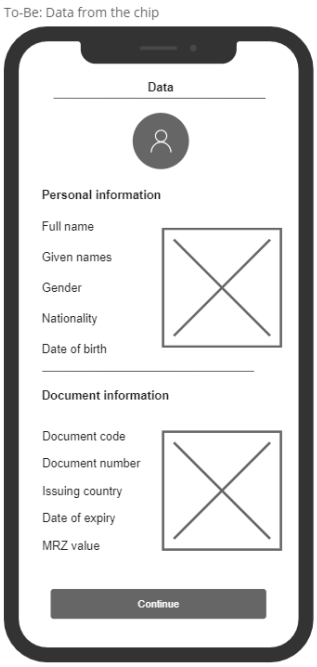


Obrázek 5.15 Úspěšná operace



Obrázek 5.16 Neúspěšná operace

Obrázek 5.17 Zobrazení návodu během verifikace



Obrázek 5.18 Zobrazení dat z bezkontaktního čipu

- Obrazovka s načtenými daty z bezkontaktního čipu se zobrazí po jejich úspěšném získání.
- Zobrazení údajů v rámci komponenty musí odpovídat návrhu na obrázku č. 5.18.
- Uživatel má možnost přejít na další verifikační krok nebo přejít na výsledek celého procesu validace, pokud nejsou k dispozici žádné další kroky.

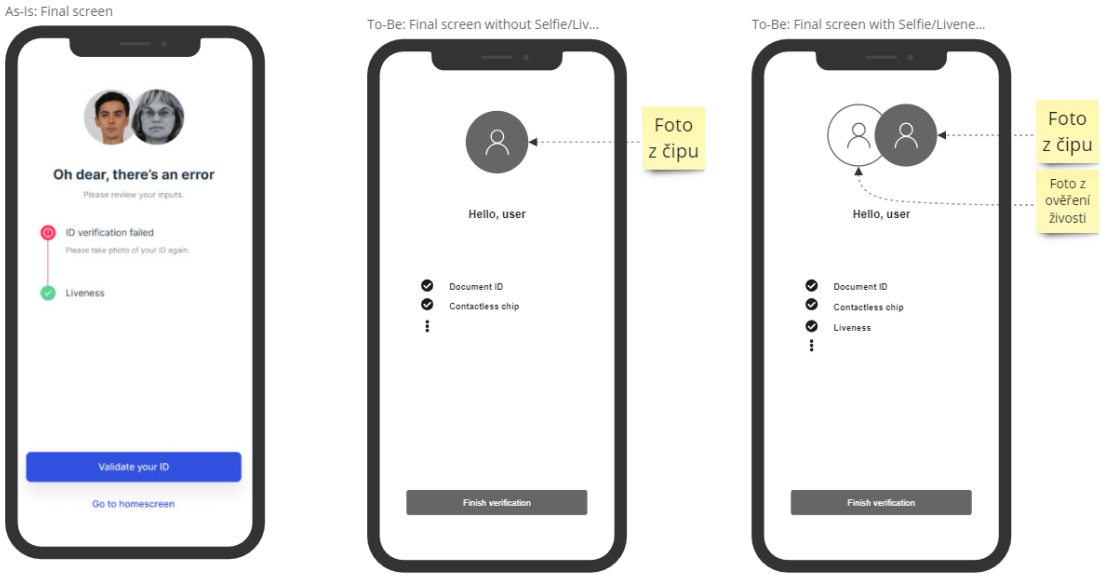
Reference: vytvořeno na základě požadavků Zobrazení dat přečtených z čipu (viz sekce č. 5.3.4).

US7: Zobrazení výsledků celé investigace

Jako uživatel mobilní DEMO aplikace chci mít přehled o každém kroku validace na finální obrazovce, aby bylo jasné, který krok se nezdařil.

Doplňující informace:

- Zdroj a množství zobrazených fotografií držitele dokladu se má řídit následujícími pravidly":
  - Pouze NFC: 1 fotografie čipu.
  - Skenování dokumentů + NFC: 1 fotografie z OCR.
  - NFC + živost: 2 fotografie (čip a živost).
  - Skenování dokumentů + NFC + Liveness: 2 fotografie (OCR a živost).
- Uživatel má možnost pokračovat dál nebo se vrátit domů v závislosti na výsledku.
- Pro rozšířený návrh komponenty a následnou implementací se má použit prvotní návrh uvedený na obrázku č. 5.19.



Obrázek 5.19 Zobrazení výsledků celé investigace

Na základě této sekce lze udělat závěr, že vytvoření uživatelských příběhů a příprava wireframů pro úpravu DEMO aplikace představují zásadní kroky k lepšímu pochopení a efektivnějšímu plánování vývoje integrace zpracování digitálních dokladů totožnosti. Diagram průběhu aplikace, který zahrnuje všechny alternativní scénáře, pak poskytuje komplexní náhled na možné interakce uživatele s aplikací. Tento diagram, uložený v elektronické příloze práce jako soubor s názvem **Screenflow.pdf**.

5.8 Testování aplikace

Týmu Trask ZenID se povedlo implementovat aplikaci na základě poskytnutého návrhu, což bylo uděláno nad rámec této práce.

Pro účely testování vyvinuté aplikace bylo vytvořeno devět testovacích scénářů, které jsou popsány v souboru "Testovací scénáře.docx"v příloze E diplomové práce. Tyto scénáře zkoumají navržené procesy a ověřují jak standardní průchod aplikací, tak i různé alternativní a chybové scénáře.

Následující tabulka č. 5.2 uvádí výjimečné situace, které byly zkoumány v jednotlivých testovacích případech.[11] První dva řádky tabulky zdůrazňují, zda testovací scénář skončil úspěchem (data z bezkontaktního čipu byla úspěšně odeslána do backendu pro další vyhodnocení), nebo neúspěchem (data z bezkontaktního čipu nebyla načtena). Všechny scénáře byly formulovány pro české dokumenty, ale mohou být rozšířené o další modely.

Testovací případy jsou pojmenovány ve formátu *TC[číslo]-[pozitivní nebo negativní případ]: [průběh procesu] ([testovaný dokument], [testované výjimky,])*.

Testování aplikace bylo provedeno týmem testerů Trask ZenID dle uvedených scénářů. Výsledky testování potvrdily, že prototyp byl řádně navržen a zohledňuje všechny relevantní aspekty procesu extrakce dat z bezkontaktního čipu.

[11] Tabulka byla vytvořena autorem.

Případ	Pouze NFC	Dokument + NFC	Dokument + NFC + Selfie	Dokument + NFC + Životnost	NFC + Selfie
Pozitivní případ	TC1 - Id	TC3 - Id	TC6 - Res	TC0 - Id, TC5 - Pas	TC7 - Id
Negativní případ	TC2 - Pas	TC4 - Res	TC6 - Res	TC8 - Id	TC8 - Id
Model dokumentu bez čipu					
NFC čtečka není aktivní	TC1 - Id				
NFC čtečka není přítomná	TC2 - Pas				
Časový limit vypršel	TC1 - Id	TC4 - Res		TC8 - Id	
Spojení s čipem bylo ztraceno		TC3 - Id			
MRZ nebyl správně načten			TC6 - Res		
Opakování se vyčerpala		TC4 - Res	TC6 - Res		
Přeskočení je povoleno	TC2 - Pas		TC6 - Res	TC8 - Id	
Přeskočení není povoleno		TC4 - Res			
Proces byl zopakován			TC6 - Res		

Tabulka 5.2 Testovací případy

5.9 Oblasti pro zlepšení

Na základě analýzy implementovaného procesu, obecných předpokladů uvedených v této kapitole a také po provedení diskuze s Trask ZenID týmem byly definované možné oblasti pro zlepšení.

V rámci posilování bezpečnostních opatření by měla být analyzována možnost implementace metody Active Authentication (AA). Tato metoda poskytuje další úroveň zabezpečení tím, že ověřuje, zda čip nebyl kompromitován. Proces AA využívá soukromý klíč uložený na čipu, který není nikdy přenášen mimo čip, a je tedy chráněn před potenciálními útoky. Ověření probíhá tak, že čip při komunikaci s čtečkou prokáže znalost soukromého klíče bez jeho odhalení, což zajišťuje, že data zůstávají bezpečná a čip nebyl duplikován [51].

Další oblastí pro zlepšení je využití volitelných datových souboru (Optional Datagroups, DGs) v rámci identifikačních procesů. Tyto soubory mohou obsahovat informace, které nejsou nezbytně nutné pro všechny případy užití, ale mohou poskytnout doplňující údaje pro specifické účely (viz obrázek č. 5.2). Pro identifikaci v bankovnictví nebo cestovních službách by bylo možné tyto datové soubory využít k ověření dodatečných údajů o uživateli, což by zlepšilo spolehlivost a přesnost verifikačního procesu.

Rovněž by měla být zkoumána implementace kontroly LDS2 pro rozšíření možností identifikace v sektoru bankovnictví nebo při cestování. Tyto struktury mohou obsahovat cestovní záznamy nebo jiné biometrické údaje, které by mohly být využity pro komplexnější ověřovací procedury, čímž by se zvýšila účinnost systémů pro ověřování klientů (KYC) v bankovnictví nebo zjednodušila kontrola na hranicích při cestování (viz také sekce č. 5.3.2).

Nakonec má být zváženo rozšíření podpory systému na doklady s kontaktními čipy, které se běžně používají na pobočkách v bankách. Tato rozšíření by umožnila pobočkám vybaveným kontaktními čtečkami sbírat a zpracovávat informace shodným způsobem jako systémy s bezkon-

taktním NFC, čímž by se celý systém stal univerzálnějším a flexibilnějším. Backend Trask ZenID by byl upraven tak, aby mohl správně integrovat a zpracovávat data získaná z těchto různých typů čipů, což by výrazně rozšířilo jeho použitelnost ve více typech aplikací.

V této kapitole byla provedena detailní analýza struktury čipů a bezpečnostních mechanismů dle směrnice ICAO 9303. Bylo rozhodnuto, že implementace systému Trask ZenID se zaměří na zpracování struktury LDS1, které bude podporováno bezpečnostními mechanismy Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE) pro přístup k čipu a Passive Authentication (PA) pro ověření integrity dat. Pro každý z těchto mechanismů byl vytvořen detailní procesní diagram, který bude sloužit jako základní dokumentace pro následnou implementaci.

Během analýzy byly definovány požadavky na budoucí systém, které byly převedeny do uživatelských příběhů a slouží jako klíčové vstupy pro další vývojové fáze. Součástí rozšíření mobilního SDK byl také návrh prototypu aplikace, který byl podpořen uživatelskými příběhy a odpovídajícím mapováním na jednotlivé požadavky definované během analýzy.

Prototyp a vyvíjená aplikace byly následně podrobeny testování s využitím vytvořených testovacích scénářů, což potvrdilo správnost navrženého prototypu a efektivitu procesu. Testování ukázalo, že aplikace splňuje stanovené cíle a očekávání v kontextu funkcionality a bezpečnosti.

V neposlední řadě byly navrženy možnosti pro budoucí rozšíření aplikace. Hlavní zaměření budoucího rozvoje zahrnuje zvážení zpracování volitelných souborů čipu a rozšíření systému o podporu kontaktních čipů, což by umožnilo aplikaci pokrýt širší spektrum použití v různých sektorech, včetně bankovnictví a cestovního ruchu. Toto rozšíření by poskytlo uživatelům větší flexibilitu a zabezpečení při ověřování totožnosti a souvisejících procesech.

Kapitola 6
Závěr

Tato diplomová práce vzešla z iniciativy vedení projektu Trask ZenID, produktu pro automatizované řešení ověřené identity zákazníků na dálku vyvíjeného společností Trask Solutions a.s. Cílem bylo rozšířit stávající systém o zpracování digitálních dokladů totožnosti, což bylo úspěšně realizováno. Práce prokázala, že navrhovaná strategie integrace digitálních dokladů je v současném kontextu vzdálené identifikace vhodná a prospěšná, jak dokládá provedená analýza využití v finančním a úvěrovém sektoru, který je pro Trask ZenID klíčový.

Součástí hodnocení byla analýza splnění Trask ZenID požadavků Evropského orgánu pro bankovnictví (EBA) a bezpečnostních prvků podle databáze PRADO. Následně vytvořený business case a rozpracování WBS projektu poskytly důkazy o proveditelnosti projektu a potenciální návratnosti investic. V rámci business case byly vytvořeny pesimistické a optimistické projektové plány pokrývající finanční stránku projektu. V obou případech se ukázalo, že i když tok peněz je záporný v prvním roce, ukazatel čisté současné hodnoty (NPV) za pět let vykazuje kladné hodnoty, což naznačuje, že budoucí hodnota příjmů a úspor generovaná projektem je vyšší než hodnota nákladů spojených s projektem. Rozdíl v plánech byl pouze v rychlosti vrácení investic.

Na základě pozitivního výsledku business case bylo rozhodnuto vytvořit i podklady pro implementaci projektu. Vzhledem k tomu byla provedena analýza ICAO 9303 s cílem prozkoumat technická omezení a vytvořit prvotní návrh integrace. Proces integrace byl zmapován do diagramu za využití BPMN 2.0. Bylo rozhodnuto, že implementace se soustředí na zpracování LDS1 za využití bezpečnostních mechanismů Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE) a Passive Authentication (PA).

V dalším kroku byl vytvořen návrh prototypu DEMO aplikace pro znázornění fungování celého procesu od začátku do konce (E2E). Testování aplikace dle testovacích scénářů potvrdilo efektivitu a správnost navrženého procesu. Na závěr byly uvedeny možnosti rozšíření systému, které spočívaly ve zpracování volitelných informací v čipu pro rozšíření identifikačního procesu a také zapojení validace kontaktních čipů.

Implementace projektu byla provedena dle stanoveného návrhu a momentálně probíhá fáze zhodnocení navrhovaných rozšíření, která by mohla dále zvýšit hodnotu a efektivitu systému.

Práce měla několik klíčových přínosů:

- Zlepšení bezpečnosti procesu ověření totožnosti s využitím digitálních dokladů.
- Rozšíření funkčnosti produktu Trask ZenID o možnosti, které zvyšují jeho konkurenceschopnost a atraktivitu pro různé sektory využívající vzdálenou identifikaci.
- Posílení důvěry uživatelů díky transparentnějšímu a ucelenějšímu zpracování osobních údajů.

Celkově lze projekt i výsledky práce považovat za úspěšné a přínosné. Výsledky práce jsou prospěšné nejen z pohledu tohoto projektu, ale i obecně v kontextu vzdálené identifikace.

Příloha A

Analýza PRADO.xlsx - popis souboru

Soubor ”Analýza PRADO.xlsx”, který je výstupem analýzy bezpečnostních prvků na dokladech totožnosti, obsahuje dva listy. První list s názvem ”All”uvádí kategorizaci bezpečnostních prvků a technik na základě analýzy glosáře PRADO. Druhý list nazvaný ”CZ”je zaměřen na detailnější analýzu bezpečnostních prvků specifických pro české dokumenty, jako jsou občanské průkazy, cestovní pasy, řidičské průkazy a povolení k pobytu. Dál je popsána struktura příslušná každé tabulce listů.

List - All. Tabulka obsažená v prvním listu elektronické přílohy obsahuje systematizovaný a kategorizovaný přehled glosáře. První sloupec uvádí kategorii bezpečnostního prvku nebo metody jeho integraci do dokladu totožnosti. V následujících třech sloupcích jsou tyto prvky dále rozděleny do sekcí a podsekcí, pokud byly identifikovány během studia glosáře. Poslední stupeň této hierarchické struktury vždy tvoří název konkretního bezpečnostního prvku. Tato struktura umožňuje snadnou orientaci a rychlý přehled bezpečnostních prvků. Pátý sloupec poskytuje překlady názvů jednotlivých sekcí a bezpečnostních prvků do češtiny, což napomáhá lepšímu porozumění a aplikaci informací pro české uživatele. Sloupec ”Light”specifikuje, jaký typ osvětlení je potřebný během zachycení, validace a zpracování bezpečnostního prvku. Sloupec ”Special HW”uvádí, zda pro provedení těchto operací je navíc vyžadován speciální hardware. Ve sloupci ”Description”je poskytnut detailní popis každého prvku, vysvětlující, jak prvek funguje a k čemu slouží, což bylo převzato z glosáře PRADO. Další sekce tabulky ukazuje přítomnost bezpečnostních prvků nebo techniky na dokladech pro Českou republiku, Slovensko a Chorvatsko. Informace byly shromážděny z PRADO a z manuální analýzy viditelných charakteristik konkrétních dokumentů. Sloupec ”ZenID detection”popisuje, zda je ověření tohoto prvku podporováno a prováděno systémem ZenID. Poslední sloupec ”Note”, poskytuje dodatečné informace, jako jsou omezení použití prvku v některých dokumentech.

List - CZ. List ”CZ”poskytuje konkrétnější informace o praktickém využití bezpečnostních prvků v českých dokumentech. První sloupec tabulky uvádí název bezpečnostního prvku. Ve dvou dalších sloupcích je uveden popis prvku dle PRADO a detailní popis jeho vizuálního či textového obsahu. Sloupec ”Example”na obou listech obsahuje fotografie bezpečnostního prvku, pořízené z rejstříku PRADO. Sloupec ”ZenID detection and verification”popisuje, zda je ověření tohoto prvku podporováno a prováděno systémem ZenID. V případě, že je podpora tohoto prvku částečná, jsou omezení nebo detailnější vysvětlení uvedeny v posledním sloupci tabulky. ”Constraints for detection”uvádí speciální světlo nebo zařízení potřebné pro zachycení a zpracování bezpečnostního prvku, což je informace převzatá z prvního listu.

Příloha B

Business case.xlsx - popis souboru

Soubor „Business case.xlsx“ obsahuje informace získané během produktové a projektové analýzy integrace zpracování digitálních dokladů totožnosti v kapitolách č.3, 4. Dokument má následující strukturu:

1. **Požadavky, metody, ZenID**: Tento list obsahuje informace o splnění požadavků kladených na proces vzdálené identifikace Evropským orgánem pro bankovnictví (EBA) a metodách použitých v rámci systému Trask ZenID pro jejich naplnění (viz také sekci č.3.7).
2. **Cenový model**: List se zaměřuje na přehled cenového modelu a způsobů licencování projektu Trask ZenID, což bylo stanoveného na základě diskuzi s vedením projektu (viz také sekci č.3.6).
3. **Harmonogram, Náklady**: Obsahuje projektový plán projektu integrace zpracování digitálních dokladů totožnosti do systému Trask ZenID a detailní přehled odhadu nákladů spojených s jednotlivými fázemi projektu.
4. **Odhad Zisk, Návratnost**: Tento list obsahuje odhady počtu uživatelů/adaptérů nového modulu, předpokládaný zisk a analýzu návratnosti investice. Tyto informace jsou klíčové pro posouzení finanční životaschopnosti a úspěchu projektu.

Příloha C

Struktura čipu

Soubor	Přítomnost na čipu	Přístup k datum	Popis	Obsah	Poznámka
EF.ATR/INFO	Podmíněný	Vždy	Ukládá informace související s Answer To Reset (ATR) a dalšími počátečními interakcemi s kartou. ATR je zpráva zasílaná chytrou kartou kompatibilní s ISO/IEC 7816 během procesu inicializace.	Informace o inicializaci karty, historické znaky, proprietární data používaná kartou, podporované protokoly, specifické vlastnosti.	Pokud je přítomen volitelný LDS2, soubor je požadován. Soubor je volitelný, pokud je přítomna pouze aplikace LDS1.
EF.DIR	Podmíněný	Vždy	Adresářový soubor, poskytuje strukturu a organizaci souborů na čipu, ukazuje přítomnost aplikací podporovaných eMRTD.	Seznam identifikátorů aplikací (AIDs) včetně sady šablon aplikací.	Pokud je přítomen volitelný LDS2, soubor je požadován. Soubor je volitelný, pokud je přítomna pouze aplikace LDS1. Pokud jsou přítomny jakékoli volitelné aplikace LDS2, EF.DIR MUSÍ být zahrnut v SecurityInfos obsažených v EF.CardSecurity.
EF.CardAccess	Podmíněný	Vždy	Bezpečnostní nastavení a pravidla řídící přístup k obsahu karty.	PACE Info, Pace Domain Parameter Info.	Požadováno, pokud je čipem podporován volitelný přístupový kontrolní systém PACE.

Pokračování na další straně

– pokračování z předchozí strany

Soubor	Přítomnost na čipu	Přístup k datum	Popis	Obsah	Poznámka
EF.CardSecurity	Podmíněný	PACE	Obsahuje bezpečnostní informace pro čip, jako jsou šifrovací klíče nebo certifikát, často ve formě zabezpečených dokumentů.	Chip Authentication Info jak je vyžadováno autentizací čipu, Chip Authentication Public Key Info jak je vyžadováno PACE-CAM / Chip Authentication, Terminal Authentication Info jak je vyžadováno terminální autentizací, Security Infos obsažené v EF.CardAccess.	Požadováno, pokud: PACE s mapováním autentizace čipu je podporováno IC, Terminální autentizace v MF je podporována IC, Autentizace čipu v MF je podporována IC.

Tabulka C.1 Obsah kořenového souboru čipu

Soubor	Přítomnost na čipu	Popis	Obsah	Poznámka
EF.SOD	Povinný	Objekt pro ověření pravosti/integrity, který umožňuje potvrdit pravost a integritu zaznamenaných údajů.	Document Security Object: digitálně podepsáno vydávajícím státem, hashovací hodnoty obsahu LDS, podpis, certifikát podepisujícího dokumentu, informace o použitém algoritmu pro hashování a podepisování dat.	Existují dvě verze objektu Document Security Object EF.SOD (V0 a V1). Doporučuje se V1. Je požadován a povolen pouze jeden EF.SOD. Navíc V1 obsahuje informace o verzích LDS a Unicode přítomných v EF.COM.
EF.COM	Povinný	Soubor, který ukládá obecné informace o aplikaci.	Informace o verzi LDS, informace o verzi Unicode, mapa datových skupin přítomných v aplikaci.	Doporučuje se, aby inspekční systémy, které spoléhají na EF.COM, byly co nejdříve upraveny tak, aby používaly SOD popsaný ve verzi LDS 1.8.

Tabulka C.2 Obsah LDS1, část 1. - Informace o aplikaci

Soubor	Zpracování ZenID	Přítomnost na čipu	Popis	Obsah	Poznámka
EF.DG1	ANO	Povinný	Určeno k odrážení celého obsahu MRZ, ať už obsahuje skutečná data nebo výplňové znaky.	MRZ Data objekt obsahuje: Kód dokumentu, Vydávající stát nebo organizace, Číslo dokumentu, Kontrolní číslice, Datum narození, Pohlaví, Datum expirace, Národnost, Volitelná data, Jméno držitele.	Struktura a velikost MRZ Data objektu závisí na typu zkoumaného dokumentu (TD1/2/3). Data uvedená ve sloupci Obsah jsou společná pro všechny typy.
EF.DG2	ANO	Povinný	Reprezentuje globálně interoperabilní biometrické údaje.	Počet záznamů biometrických kódování obličeje, Hlavička, Biometrický obraz obličeje držitele	
EF.DG3	NE	Volitelný	Dodatečný identifikační prvek — Prst(y)	Počet záznamů biometrických kódování prstů, Hlavička, Biometrické kódování dat prstů.	Pokud nejsou v době vydání eMRTD k dispozici otisky prstů, měl by DG obsahovat prázdnou šablonu.
EF.DG4	NE	Volitelný	Dodatečný identifikační prvek — Iris(y)	Počet záznamů biometrických kódování očí, Hlavička, Biometrické kódování dat očí.	Pokud nejsou v době vydání eMRTD k dispozici irisy, měl by DG obsahovat prázdnou šablonu.
EF.DG5	NE	Volitelný	Zobrazený portrét	Počet záznamů zobrazených portrétů, Reprezentace zobrazeného portrétu, Počet bajtů v reprezentaci zobrazeného portrétu, Reprezentace zobrazeného portrétu.	
EF.DG6	N/A	Vyhrazeno pro budoucí použití			

Pokračování na další straně

– pokračování z předchozí strany

Soubor	Zpracování ZenID	Přítomnost na čipu	Popis	Obsah	Poznámka
EF.DG7	NE	Volitelný	Zobrazený podpis nebo obvyklá značka	Počet zobrazených podpisů nebo obvyklých značek, Reprezentace zobrazeného podpisu nebo obvyklé značky	
EF.DG8-10	NE	Volitelný	Data, struktury a funkce		Tyto datové skupiny zatím nebyly definovány. Do té doby jsou k dispozici pro dočasné vlastní použití.
EF.DG11	NE	Volitelný	Tato datová skupina se používá pro dodatečné údaje o držiteli dokumentu	Plné jméno držitele, Další jména, Osobní číslo, Plné datum narození, Místo Narození, Adresa, Telefon, Profese, Titul, Osobní shrnutí, Důkaz o občanství, Jiné platné cestovní dokumenty, číslo cestovního dokumentu, Informace o opatrovnictví	
EF.DG12	NE	Volitelný	Tato datová skupina se používá pro dodatečné informace o dokumentu	Vydávající úřad, Datum vydání, Údaje o dalších osobách, Potvrzení/Observace, Daňové/Výjezdní požadavky, Obraz přední strany eMRTD, Obraz zadní strany MRTD, Čas personalizace, Sériové číslo zařízení na personalizaci	
EF.DG13	NE	Volitelný	Volitelné podrobnosti		

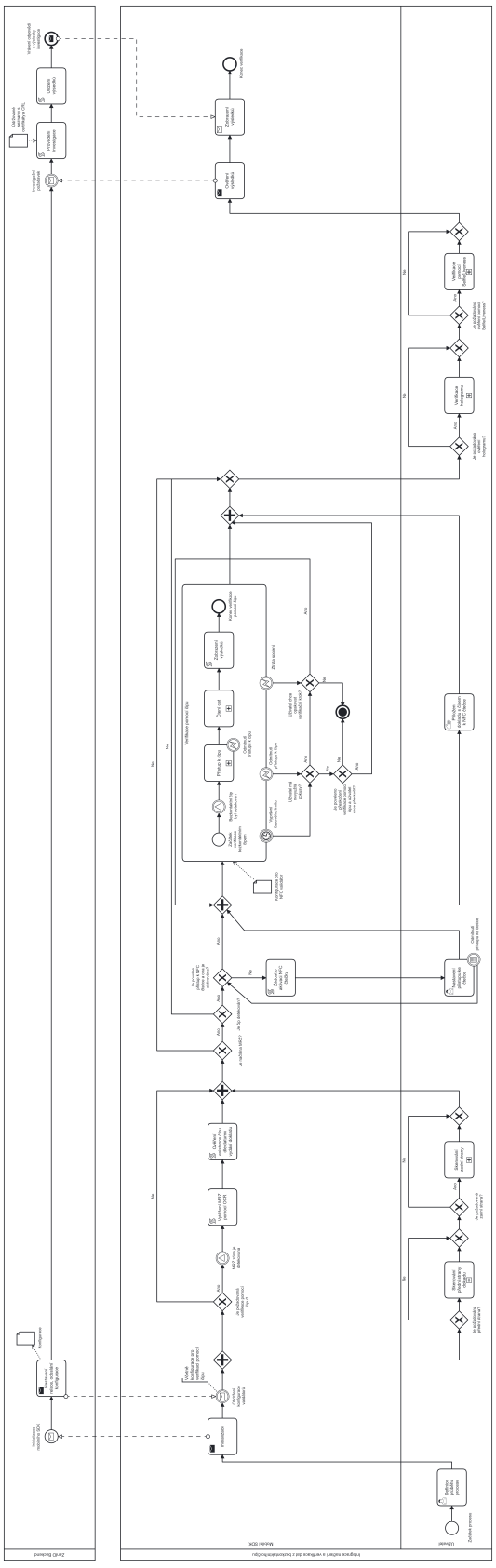
Pokračování na další straně

– pokračování z předchozí strany					
Soubor	**Zpracování ZenID**	**Přítomnost na čipu**	**Popis**	**Obsah**	**Poznámka**
EF.DG14	NE	Podmíněný	Bezpečnostní možnosti	SecurityInfos, Protokol identifikátoru objektu označuje podporovaný protokol. Otevřený typ requiredData obsahuje protokolově specifická povinná data. Otevřený typ optionalData obsahuje protokolově specifická volitelná data.	Soubor DG14 obsažený v aplikaci eMRTD je POŽADOVÁN, pokud čip eMRTD podporuje Chip Authentication nebo PACE-GM/-IM.
EF.DG15	NE	Podmíněný	Obsahuje veřejný klíč pro aktivní autentizaci	Active Authentication Public Key Info.	POŽADOVÁNO, pokud je podporována volitelná aktivní autentizace čipu
EF.DG16	NE	Volitelný	Osoba(y) k oznámení	Seznam informací pro nouzové oznámení	

Tabulka C.3 Obsah LDS1, část 2. - Informace o dokladu a jeho držiteli

Příloha D

Dokumentace procesu integrace zpracování digitálních dokladů totožnosti



Obrázek D.1 Budoucí rozšířený stav procesu identifikaci za využití mobilního SDK

ID	Název	Typ	Role	Trigger	Popis	Další kroky
1	Začátek procesu	Start Event	Uživatel		Proces začíná otevřením DEMO aplikace.	Definice průběhu procesu.
2	Definice průběhu procesu	Manual Task	Uživatel		Na úvodní stránce, včetně záložky nastavení, jsou definována kritéria procesu a typy verifikace, které budou součástí procesu, a spustí proces verifikace.	Inicializace
3	Inicializace	Send Task	Mobilní SDK		SDK se inicializuje vůči backendu a naváže spojení.	Obdržení konfigurací validatoru
4	Inicializace mobilního SDK	Receive Message	ZenID Backend	Inicializace	Backend obdrží inicializační požadavek od SDK.	Nastavení relace, odeslání konfigurace
5	Nastavení relace, odeslání konfigurace	Send Task	ZenID Backend		Jako odpověď na inicializaci backend odešle seznam profilů včetně konfigurace validatorů napříč profily.	Investigacní požadavek
6	Obdržení konfigurací validatoru	Receive Task	Mobilní SDK	Nastavení relace, odeslání konfigurace	SDK přijme backendovou konfiguraci.	Rozhodnutí o verifikaci pomocí čipu. Paralelně rozhodnutí o skenování přední strany.
7	Rozhodnutí o skenování přední strany	Exclusive Gateway	Uživatel		Na základě instrukcí od SDK uživatel provede rozhodnutí o nutnosti skenování přední strany dokladu.	Ano: Skenování přední strany dokladu. Ne: Rozhodnutí o skenování zadní strany.
8	Skenování přední strany dokladu	Subprocess	Uživatel		Uživatel provede skenování přední strany dokladu totožnosti na základě instrukcí od SDK.	Rozhodnutí o skenování zadní strany.

Pokračování na další straně

– pokračování z předchozí strany

ID	Název	Typ	Role	Trigger	Popis	Další kroky
9	Rozhodnutí o skenování zadní strany	Exclusive Gateway	Uživatel		Na základě instrukcí od SDK uživatel provede rozhodnutí o nutnosti skenování zadní strany dokladu.	Ano: Skenování zadní strany dokladu. Ne: Rozhodnutí o úspěšnosti načtení MRZ.
10	Skenování zadní strany dokladu	Subprocess	Uživatel		Uživatel provede skenování zadní strany dokladu totožnosti na základě instrukcí od SDK.	Rozhodnutí o úspěšnosti načtení MRZ.
11	Rozhodnutí o verifikaci pomocí čipu	Exclusive Gateway	Mobilní SDK		Rozhodnutí probíhá na základě vstupu obdrženého od uživatele v rámci kroku definice průběhu procesu, konkrétně validuje se volba verifikace pomocí bezkontaktního čipu.	Ano: MRZ zona je detekována Ne: Rozhodnutí o úspěšnosti načtení MRZ.
12	MRZ zona je detekována	Signal Event	Mobilní SDK	Detekce MRZ zóny MRZ čtečkou implementovanou do SDK	Pokud MRZ čtečka byla schopna detekovat MRZ, pokračuje se dál v procesu, jinak se čeká na detekci.	Vytěžení MRZ pomocí OCR
13	Vytěžení MRZ pomocí OCR	Script Task	Mobilní SDK		Pomocí technologie OCR probíhá čtení a validace dat uvedených ve strojově čitelné zóně.	Ověření existence čipu dle data vydání dokladu

Pokračování na další straně

– pokračování z předchozí strany

ID	Název	Typ	Role	Trigger	Popis	Další kroky
14	Ověření existence čipu dle data vydání dokladu	Script Task	Mobilní SDK		Na základě data vydání dokladu, které bylo vyčteno ze strojově čitelné zóny a číselníku s definovanou podporou čipu pro konkrétní modely dokladu, mobilní SDK se rozhodne o přítomnosti čipu v dokladu totožnosti.	Rozhodnutí o úspěšnosti načtení MRZ.
15	Rozhodnutí o úspěšnosti načtení MRZ.	Exclusive Gateway	Mobilní SDK		Posuzuje se na základě výsledku kroku Vytěžení MRZ pomocí OCR	Ano: Rozhodnutí o detekci čipu Ne: Rozhodnutí o verifikaci pomocí hologramu
16	Rozhodnutí o detekci čipu	Exclusive Gateway	Mobilní SDK		Posuzuje se na základě výsledku kroku Ověření existence čipu dle data vydání dokladu	Ano: Rozhodnutí o přístupu a stavu NFC čtečky Ne: Rozhodnutí o verifikaci pomocí hologramu
17	Rozhodnutí o přístupu a stavu NFC čtečky	Exclusive Gateway	Mobilní SDK		Aplikace zkouší přistoupit k NFC čtečce a udělá rozhodnutí o její dostupnosti a stavu.	Ano: Paralelně Začátek verifikace bezkontaktním čipem a Přiložení dokladu s čipem k NFC čtečce. Ne: Žádost o aktivaci NFC čtečky
18	Žádost o aktivaci NFC čtečky	Script Task	Mobilní SDK		Aplikace vyzve uživatele k poskytnutí přístupu neboli aktivaci NFC čtečky prostřednictvím systémových nastavení.	Nastavení přístup ke čtečce
19	Nastavení přístup ke čtečce	User Task	Uživatel		Uživatel provede aktualizaci systémových nastavení. Není zaručena aktivace a povolení přístupu ke čtečce.	Paralelně Začátek verifikace bezkontaktním čipem a Přiložení dokladu s čipem k NFC čtečce.

Pokračování na další straně

– pokračování z předchozí strany

ID	Název	Typ	Role	Trigger	Popis	Další kroky
20	Odmítnutí přístupu k čtečce	Conditional Boundary Event	Uživatel		Pokud uživatel zamítne přístup ke čtečce nebo deaktivuje čtečku, proces nemůže pokračovat.	Rozhodnutí o přístupu a stavu NFC čtečky
21	Přiložení dokladu s čipem k NFC čtečce	Human Task	Uživatel		Na základě instrukcí obdržených od SDK, uživatel přiloží doklad totožnosti s čipem co nejblíže k NFC čtečce pro načtení dat z bezkontaktního čipu.	Rozhodnutí o verifikaci pomocí hologramu
22	Začátek verifikace bezkontaktním čipem	Start Event	Mobilní SDK		SDK načte instrukce a konfigurace NFC validátoru pro správnou inicializaci procesu.	Bezkontaktní čip byl detekován
23	Bezkontaktní čip byl detekován	Signal Event	Mobilní SDK		Čtečka detekovala signál bezkontaktního čipu v dokladu, který byl přiložen k mobilu uživatelem	Přístup k čipu
24	Přístup k čipu	Subprocess	Mobilní SDK		Na základě mechanismu pro přístup k bezkontaktnímu čipu, který je popsán v kapitole výše, mobilní SDK se pokusí o přístup k čipu prostřednictvím PACE nebo BAC protokolu.	Čtení dat
25	Čtení dat	Subprocess	Mobilní SDK		Po navázání bezpečného kanálu spojení s bezkontaktním čipem, SDK provede načtení dat z čipu.	Zobrazení výsledku
26	Zobrazení výsledku	Script Task	Mobilní SDK		Data načtená z bezkontaktního čipu jsou zobrazena uživateli pro testovací účely	Konec verifikace pomocí čipu
27	Konec verifikace pomocí čipu	End Event	Mobilní SDK		Konec podprocesu zastřešujícího verifikaci pomocí bezkontaktního čipu	Rozhodnutí o verifikaci pomocí hologramu

Pokračování na další straně

– pokračování z předchozí strany

ID	Název	Typ	Role	Trigger	Popis	Další kroky
28	Vypršení časového limitu	Timer Boundary Event	Mobilní SDK		Vypršení časového limitu, který je dán backend validátorem	Rozhodnutí o nevyužitých pokusech
29	Odmítnutí přístupu k čipu	Error Boundary Event	Mobilní SDK		Čip odmítne pokus o navázání bezpečnostního kanálu pro výměnu zpráv	Rozhodnutí o nevyužitých pokusech
30	Ztráta spojení	Error Boundary Event	Mobilní SDK		Ztráta spojení s čipem během procesu verifikace	Rozhodnutí o opakování verifikačního kroku
31	Rozhodnutí o nevyužitých pokusech	Exclusive Gateway	Mobilní SDK		SDK provede ověření zbývajících pokusů na opakování verifikačního kroku. Omezení na pokusy je dáno konfigurací příslušného parametru backend NFC validátoru. Po každém opakování aplikace inkrementuje počet zbývajících pokusů.	Ano: Rozhodnutí o opakování verifikačního kroku Ne: Rozhodnutí o přeskoku verifikace pomocí bezkontaktního čipu
32	Rozhodnutí o opakování verifikačního kroku	Exclusive Gateway	Mobilní SDK		Aplikace vyzve uživatele k opakování verifikačního kroku. Uživatel buď odmítne opakovat nebo zkouší proces verifikace pomocí bezkontaktního čipu znovu.	Ano: Paralelně Začátek verifikace bezkontaktním čipem a Přiložení dokladu s čipem k NFC čtečce. Ne: Konec verifikace pomocí čipu
33	Rozhodnutí o přeskoku verifikace pomocí bezkontaktního čipu	Exclusive Gateway	Mobilní SDK		Na základě nastavení příslušného parametru z backendového validátoru, SDK posoudí o možnosti přeskoku verifikace pomocí bezkontaktního čipu. Pokud je přeskoku povolené, aplikace ověří u uživatele, jestli on chce tuto možnost využít.	Ano: Rozhodnutí o verifikaci pomocí hologramu. Ne: Konec verifikace pomocí čipu

Pokračování na další straně

– pokračování z předchozí strany						
ID	**Název**	**Typ**	**Role**	**Trigger**	**Popis**	**Další kroky**
34	Rozhodnutí o verifikaci pomocí hologramu	Exclusive Gateway	Uživatel		Na základě instrukcí od SDK uživatel provede rozhodnutí o nutnosti verifikace pomocí hologramu.	Ano: Verifikace hologramu. Ne: Rozhodnutí o ověření pomocí Selfie/Liveness.
35	Verifikace hologramu	Subprocess	Uživatel		Uživatel projde ověřením hologramu na dokladu totožnosti na základě instrukcí od SDK.	Rozhodnutí o ověření pomocí Selfie/Liveness.
36	Rozhodnutí o ověření pomocí Selfie/Liveness	Exclusive Gateway	Uživatel		Na základě instrukcí od SDK uživatel provede rozhodnutí o nutnosti ověření pomocí Selfie/-Liveness.	Ano: Verifikace pomocí Selfie/Liveness. Ne: Ověření výsledku.
37	Verifikace pomocí Selfie/Liveness	Subprocess	Uživatel		Uživatel projde ověřením Selfie/-Liveness na základě instrukcí od SDK.	Ověření výsledku.
38	Ověření výsledku	Send Task	Mobilní SDK		SDK odešle nasbírané evidence na backend ZenID a aktivuje proces investigace (ověření a validace obdržených evidencí)	Zobrazení výsledku
39	Investigační požadavek	Message Intermediate Catch Event	Backend ZenID	Obdržení požadavku na provedení investigací	Backend obdrží požadavek na provedení investigací, obsahující nasbírané od uživatele evidence.	Provedení investigace
40	Provedení investigace	Script Task	Backend ZenID		Na základě aktuálního nastavení validátoru, backend provede validaci evidencí, včetně Pasivní Autentikace pro ověření dat načtených z bezkontaktního čipu.	Uložení výsledku
Pokračování na další straně						

– pokračování z předchozí strany						
ID	**Název**	**Typ**	**Role**	**Trigger**	**Popis**	**Další kroky**
41	Uložení výsledku	Script task	Backend ZenID		Výsledky investigací budou bezpečně uložené do databáze a přístupné přes API nebo GUI backendu	Vrácení odpovědi s výsledky investigace
42	Vrácení odpovědi s výsledky investigace	End Task	Backend ZenID		Backend vrátí výsledky investigace příslušnému mobilnímu SDK	
43	Zobrazení výsledku	Receive Task	Mobilní SDK	Obdržení výsledku z backendu	Jakmile mobilní SDK obdrží výsledky investigace, tyto informace budou zobrazené uživateli	Konec verifikace
44	Konec verifikace	End Task	Mobilní SDK		Konec celého procesu identifikace na dálku	

Tabulka D.1 Dokumentovaný proces identifikace za využití bezkontaktního čipu

Příloha E

Číselník pro umožnění detekce bezkontaktního čipu

Země	Typ dokladu	Podpora bezkontaktního čipu
Czech Republic	ID	NFC after Issue Date 02/08/2021
Czech Republic	DL	No NFC
Czech Republic	PAS	Always
Czech Republic	GUN	No NFC
Czech Republic	RES	Always
Czech Republic	BIRTH	No NFC
European Union	VISA	No NFC
Slovakia	RES	Always
Slovakia	ID	NFC after Issue Date 01/12/2022
Slovakia	DL	No NFC
Belgium	PAS	Always
Belgium	ID	NFC after Issue Date 01/06/2020
Belarus	PAS	NFC after Issue Date 01/09/2021
Bosnia and Herzegovina	PAS	Always
Bulgaria	PAS	Always
Bulgaria	ID	No NFC
Montenegro	PAS	Always
Denmark	PAS	NFC after Issue Date 01/08/2006
Estonia	PAS	Always
Estonia	ID	No NFC
Finland	PAS	Always
Finland	ID	Unknown
France	PAS	Always
France	ID	NFC after Issue Date 03/15/2021
Croatia	PAS	Always
Croatia	ID	NFC after Issue Date 02/08/2021
Iceland	PAS	Always
Italy	ID	NFC after Issue Date 04/07/2016
Italy	PAS	Always

Pokračování na další straně

– pokračování z předchozí strany

Země	Typ dokladu	Podpora bezkontaktního čipu
Cyprus	PAS	Always
Cyprus	ID	NFC after Issue Date 02/24/2015
Lithuania	PAS	Always
Lithuania	ID	Always
Latvia	PAS	Always
Latvia	ID	Always
Luxembourg	PAS	Always
Luxembourg	ID	NFC after Issue Date 07/01/2014
Hungary	ID	Unknow
Hungary	PAS	Always
Hungary	DL	No NFC
Hungary	ADD	No NFC
Republic of North Macedonia	PAS	Always
Malta	PAS	Always
Malta	ID	No NFC
Moldova	PAS	Always
Germany	ID	NFC after Issue Date 02/08/2021
Germany	PAS	Always
Netherlands	DL	No NFC
Netherlands	PAS	Always
Netherlands	ID	Always
Norway	PAS	NFC after Issue Date 01/10/2005
Poland	ID	NFC after Issue Date 03/04/2019
Poland	PAS	Always
Poland	DL	No NFC
Portugal	PAS	Always
Portugal	ID	No NFC
Austria	ID	NFC after Issue Date 02/08/2021
Austria	PAS	Always
Austria	DL	No NFC
Romania	PAS	Always
Romania	ID	NFC after Issue Date 08/09/2021
Greece	PAS	Always
Slovenia	PAS	Always
Slovenia	ID	No NFC
United Kingdom	PAS	Always
Serbia	PAS	Always
Spain	PAS	NFC after Issue Date 14/08/2006
Spain	ID	NFC after Issue Date 01/02/2015
Sweden	PAS	Always
Sweden	ID	Always
Switzerland	PAS	Always
Ukraine	PAS	Unknown
Ukraine	ID	Always
Ukraine	DL	No NFC
Vietnam	PAS	No NFC

Tabulka E.1 Číselník pro umožnění detekce bezkontaktního čipu

Bibliografie

1. DOCUSIGN. *Identity Verification: What It Is and When to Use It*. 2023. Dostupné také z: https://www.docusign.com/blog/identity-verification. Online; přístup dne 15. září 2023.
2. OLZAK, Tom. *Chapter 11 – Identity management and access controls*. 2012. Dostupné také z: https://www.infosecinstitute.com/resources/general-security/identity-management/. Online; přístup dne 15. září 2023.
3. PSCHEROVÁ, Kateřina. *Jaká je role ČNB v oblasti prevence praní špinavých peněz a financování terorismu?* 2022. Dostupné také z: https://www.cnb.cz/cs/o_cnb/cnblog/Jaka-je-role-CNB-v-oblasti-prevence-prani-spinavych-penez-a-financovani-terorismu/. Online; přístup dne 15. září 2023.
4. EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Remote ID Proofing: Analysis of Methods to Carry Out Identity Proofing Remotely*. 2021. Report. Dostupné také z: https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing. Online; přístup dne 12. září 2024.
5. WORLD PRIVACY FORUM. *National IDs and Biometrics*. 2021. Dostupné také z: https://www.worldprivacyforum.org/2021/10/national-ids-and-biometrics/. Online; přístup dne 30. listopadu 2023.
6. EUROPEAN BANKING AUTHORITY. *Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849*. 2022. Guidelines, EBA/-GL/2022/15. European Banking Authority. Dostupné také z: https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-4. Online; přístup dne 30. listopadu 2023.
7. COUNCIL OF THE EUROPEAN UNION. *Dokumenty podle kategorie*. Council of the European Union, 2023. Dostupné také z: https://www.consilium.europa.eu/prado/cs/prado-documents/CZE/A/docs-per-category.html. Online; přístup dne 25. října 2023.
8. EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION. *Regulation (EU) No 910/2014 of the European Parliament and of the Council: On electronic identification and trust services for electronic transactions in the internal market*. 2014. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. Online; přístup dne 25. října 2023.
9. ROHN, Samantha. *Digital Customer Onboarding in Banking, Explained*. The Whatfix Blog, 2023. Dostupné také z: https://whatfix.com/blog/customer-onboarding-in-banking/. Online; přístup dne 30. listopadu 2023.

10. TRUE TAMPLIN BSc, CEPF®. *Know Your Customer (KYC)*. Finance Strategics, 2023. Dostupné také z: https://www.financestrategists.com/banking/know-your-customer-kyc/. Online; přístup dne 30. listopadu 2023.
11. SWIFT. *What is Customer Due Diligence (CDD)?* 2023. Dostupné také z: https://www.swift.com/ru/node/300736. Online; přístup dne 15. září 2023.
12. UNIT21. *TERM Enhanced Due Diligence (EDD): Meaning, Process, Requirements*. 2023. Dostupné také z: https://www.unit21.ai/fraud-aml-dictionary/enhanced-due-diligence. Online; přístup dne 15. září 2023.
13. EUROPEAN COMMISSION. *EU Trusted Lists*. 2023. Dostupné také z: https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists. Online; přístup dne 15. září 2023.
14. ČESKÁ REPUBLIKA. *Zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a fin. terorismu*. 2008. Dostupné také z: https://www.zakonyprolidi.cz/cs/2008-253%5C#cast2. Online; přístup dne 17. října 2023.
15. PSCHEROVÁ, Kateřina. *Identifikace a kontrola klientů finančních institucí jako nástroj v boji proti praní špinavých peněz*. 2020. Dostupné také z: https://www.cnb.cz/cs/o_cnb/cnblog/Identifikace-a-kontrola-klientu-financnich-instituci-jako-nastroj-v-boji-proti-prani-spinavych-penez/. Online; přístup dne 15. září 2023.
16. ČESKÁ NÁRODNÍ BANKA. *67/2018 Sb. VYHLÁŠKA o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu*. 2008. Dostupné také z: https://fau.gov.cz/files/vyhlaska-cnb-c-672018-sb-o-nekterych-pozadavcich-na-system-vnitrnich-zasad-postupu-a-kontrolnich-opatreni-prot.pdf. Online; přístup dne 15. září 2023.
17. EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Remote identity proofing: attacks countermeasures*. 2022. Report. ISBN 978-92-9204-549-4. Dostupné z DOI: 10.2824/183066. Online; přístup dne 12. září 2024.
18. KHAN, Akif. *Buyer's Guide for Identity Proofing*. 2022. Dostupné také z: https://www.gartner.com. ID G00767717, Online; přístup dne 30. října 2023.
19. PRADO. *Glosář technických pojmů souvisejících se zajišťovacími prvky a zabezpečenými doklady obecně (v abecedním pořadí)*. 2022. Dostupné také z: https://www.consilium.europa.eu/prado/cs/prado-glossary/prado-glossary.pdf. Online; přístup dne 25. října 2023.
20. CHIBA, Emi. *Hype Cycle for HR Technology*. 2023. Dostupné také z: https://www.gartner.com. ID G00785903, Online; přístup dne 30. října 2023.
21. DAON. *Identity Verification & Authentication for any customer, anywhere*. 2023. Dostupné také z: https://www.daon.com/. Online; přístup dne 13. prosince 2023.
22. JUMIO. *Don't fight identity fraud without us*. 2023. Dostupné také z: https://www.jumio.com/. Online; přístup dne 13. prosince 2023.
23. VERIDAS. *Unlock the Power of True Identity Verification*. 2023. Dostupné také z: https://veridas.com/en/. Online; přístup dne 13. prosince 2023.
24. INNOVATRICS. *Building a World of Instant Trust*. 2023. Dostupné také z: https://www.innovatrics.com/. Online; přístup dne 13. prosince 2023.
25. ZENTITY. *Get the most out of your digital channels*. 2023. Dostupné také z: https://zentity.com/. Online; přístup dne 13. prosince 2023.
26. INVERID. *Which countries have ePassports?* 2021. Dostupné také z: https://www.inverid.com/blog/countries-epassports#:~:text=Currently%20(December%202023)%2C%20172,can%20be%20read%20with%20ReadID. Online; přístup dne 13. prosince 2023.

27. EGOVERNMENTU, Odbor Hlavního architekta. *Prokazování totožnosti s využitím fyzických dokladů totožnosti: Právní úprava obecného prokazování totožnosti s využitím fyzických průkazů totožnosti*. 2023. Dostupné také z: https://archi.gov.cz/znalostni_baze:fyzicke_prokazani_totoznosti. Online; přístup dne 17. října 2023.

28. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 5: Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-340-8. Dostupné také z: https://www.icao.int/publications/Documents/9303_p5_cons_en.pdf. Online; přístup dne 12. února 2024.

29. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 6: Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-348-4. Dostupné také z: https://www.icao.int/publications/Documents/9303_p6_cons_en.pdf. Online; přístup dne 12. února 2024.

30. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-335-4. Dostupné také z: https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf. Online; přístup dne 12. února 2024.

31. DOCUSIGN. *What is a digital ID?* 2023. Dostupné také z: https://support.docusign.com/s/articles/What-is-a-digital-ID?language=en_US&rsc_301. Online; přístup dne 15. září 2023.

32. FEDERAL OFFICE FOR INFORMATION SECURITY. *Electronic Identity Documents*. 2023. Dostupné také z: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Elektronische-Ausweisdokumente/elektronische-ausweisdokumente_node.html. Online; přístup dne 17. října 2023.

33. EGOVERNMENTU, Odbor Hlavního architekta. *Slovník pojmů eGovernmentu*. 2023. Dostupné také z: https://archi.gov.cz/slovnik_egov. Online; přístup dne 17. října 2023.

34. RFID JOURNAL. *Frequently Asked Questions: What is RFID?* 2023. Dostupné také z: https://www.rfidjournal.com/faq/what-is-rfid. Online; přístup dne 22. března 2024.

35. HANYI, Norbert. *The Security of IDs Volume 2: What Travel Document RFID Chips Contain*. Adaptive Recognition, 2022. Dostupné také z: https://adaptiverecognition.com/blog/identity-industry/the-security-of-ids-volume-2-what-travel-document-rfid-chips-contain/. Online; přístup dne 22. března 2024.

36. CDW. *RFID vs. NFC: Which is Right for Your Business?* 2023. Dostupné také z: https://www.cdw.com/content/cdw/en/articles/networking/rfid-vs-nfc.html. Online; přístup dne 22. března 2024.

37. NFC FORUM. *What NFC does*. 2024. Dostupné také z: https://nfc-forum.org/learn/what-nfc-does. Online; přístup dne 22. března 2024.

38. LANZ, C. K. *What Is a Biometric Passport?* Historical Index, 2024. Dostupné také z: https://www.historicalindex.org/what-is-a-biometric-passport.htm. Online; přístup dne 14. ledna 2024.

39. FINDBIOMETRICS. *Over 60+ countries now issuing ePassports*. 2008. Dostupné také z: https://web.archive.org/web/20170406111611/http:/findbiometrics.com/over-60-countries-now-issuing-epassports-2/. Online; přístup dne 25. října 2023.

40. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Počty vyrobených občanských průkazů s čipem*. 2021. Dostupné také z: https://www.mvcr.cz/soubor/transparentnost-vs-pocty-dokladu.aspx. Online; přístup dne 20. listopadu 2023.

41. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Doc 9303: Machine Readable Travel Documents*. 2021. Report. Dostupné také z: https://www.icao.int/publications/pages/publication.aspx?docnum=9303. Online; přístup dne 12. února 2024.

42. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *2-Access to ePassport chip*. 2021. Dostupné také z: https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Document-readers.aspx. Online; přístup dne 14. ledna 2024.

43. PROJECT MANAGEMENT INSTITUTE. *Introduction to Fixed Price Contracts*. 2023. Dostupné také z: https://pmiuk.co.uk/mastering-fixed-price-contracts-benefits-key-elements-and-best-practices/. Online; přístup dne 25. října 2023.

44. ČSOB. *50. díl: Velký přehled: Daňové povinnosti a novinky v roce 2024*. 2024. Dostupné také z: https://www.pruvodcepodnikanim.cz/clanek/danove-novinky-2024/. Online; přístup dne 20. ledna 2023.

45. MONETA. *Co je čistá současná hodnota?* 2024. Dostupné také z: https://www.moneta.cz/slovnik-pojmu/detail/cista-soucasna-hodnota. Online; přístup dne 20. listopadu 2023.

46. BLUEBITE. *Android NFC Compatibility: With mixed NFC support across the Android ecosystem we break down which devices support the technology.* 2021. Dostupné také z: https://www.bluebite.com/nfc/android-nfc-compatibility. Online; přístup dne 17. října 2023.

47. GOTOTAGS. *iPhone NFC Tag Compatibility*. 2023. Dostupné také z: https://gototags.com/ios/nfc/compatibility. Online; přístup dne 17. října 2023.

48. CAN I USE. *Web NFC*. 2023. Dostupné také z: https://caniuse.com/webnfc. Online; přístup dne 17. října 2023.

49. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-381-1. Dostupné také z: https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf. Online; přístup dne 16. února 2024.

50. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-394-1. Dostupné také z: https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf. Online; přístup dne 15. února 2024.

51. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 11: Security Mechanisms for MRTDs*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-419-1. Dostupné také z: https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf. Online; přístup dne 15. února 2024.

52. INVERID. *Privacy-related security mechanisms for ePassports*. 2020. Dostupné také z: https://www.inverid.com/blog/privacy-related-security-mechanisms-for-epassports. Online; přístup dne 14. ledna 2024.

53. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Machine Readable Travel Documents Part 12: : Public Key Infrastructure for MRTDs*. Eighth. Montréal, Quebec, Canada: International Civil Aviation Organization, 2021. ISBN 978-92-9265-422-1. Dostupné také z: https://www.icao.int/publications/Documents/9303_p12_cons_en.pdf. Online; přístup dne 16. února 2024.

54. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *The ICAO Master List and ICAO Health Master List*. 2023. Dostupné také z: `https://www.icao.int/Security/FAL/PKD/Pages/ICAO-Master-List.aspx`. Online; přístup dne 17. října 2023.

55. INTERNATIONAL CIVIL AVIATION ORGANIZATION. *Pilot project - Authorizing use of data from the ICAO PKD by the Private Sector*. [B.r.]. Dostupné také z: `https://www.icao.int/Security/FAL/PKD/Pages/PKD%20Private%20sector%20pilot.aspx`. Online; přístup dne 17. října 2023.

56. BSI. *CSCA Master List*. 2023. Dostupné také z: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/CSCA/GermanMasterList.html`. Online; přístup dne 17. října 2023.

Obsah příloh

- `havrylenko_thesis` ..... zdrojová forma práce ve formátu LaTeX
- `havrylenko_thesis.pdf` ..... text práce ve formátu PDF
- `support materials` ..... podpůrné materiály
  - `Business case.xlsx` ..... soubor obsahující podklady pro business case
  - `Testovací scénáře.docx` ..... soubor obsahující testovací scénáře pro DEMO aplikaci
  - `Analýza PRADO.xlsx` ..... soubor obsahující analýzu bezpečnostních prvků dle PRADO
  - `Screenflow.pdf` ..... mapování průchodu DEMO aplikace
  - `BPMN diagrams` ..... všechny zmapované procesy ve formátu bpmn
    - `asis_level1.bpmn` ..... výstup analýzy aktuálního stavu procesu identifikace
    - `BAC.bpmn` ..... mapování procesu základního přístupového mechanismu
    - `chip_access_common_part.bpmn` .... mapování procesu předcházejícího přístupovému mechanismu
    - `PACE.bpmn` ..... mapování procesu pokročilejšího přístupového mechanismu
    - `Passive_Authentication.bpmn` ..... mapování procesu pasivního ověřování
    - `tobe_level1.bpmn` ..... výstup analýzy budoucího stavu procesu identifikace v zjednodušené notaci
    - `tobe_level2.bpmn` .. výstup pokročilejší analýzy budoucího stavu procesu identifikace