METODIKA

K PROJEKTU

„MULTIMODÁLNÍ BIOMETRICKÉ ZAŘÍZENÍ PRO OVĚŘENÍ IDENTITY OSOB NA ZÁKLADĚ OTISKŮ PRSTŮ A OBLIČEJE PŘI PŘEKRAČOVÁNÍ STÁTNÍCH HRANIC“ (BEFFIC)

Touchless Biometric Systems s.r.o.: Martin Drahanský, Radim Dvořák
Výzkumný ústav bezpečnosti práce, v. v. i.: Ondřej Kanich, Pavel Danihelka, Petr Novotný

Brno, 29. května 2024 (verze 0.8)

OBSAH

1 ÚVOD

Tato metodika vznikla jako plánovaný výsledek projektu s názvem „***Multimodální biometrické zařízení pro ověření identity osob na základě otisků prstů a obličeje při překračování státních hranic***“, s akronymem **BEFFIC** a označením poskytovatele Ministerstva vnitra České republiky **VB01000066**.

Cílem této metodiky je rozbor aktuálního stavu využití biometrických systémů při ochraně kritické infrastruktury. Sem spadají normy, legislativa, technické aspekty a další faktory, které hrají při výběru vhodného biometrického systému roli. Velký význam je třeba dbát při výběru systémů pro realizaci hraniční kontroly, kde se objevují osobní identifikační doklady vydané různými státy, tj. je třeba zajistit co nejvyšší míru kompatibility, příp. interoperability s jinými biometrickými šablonami.

Naším cílem spjatým s projektem je definování vhodného použití stacionární a mobilní verze zařízení společnosti Touchless Biometric Systems s.r.o. s obchodním označením **3D FLOW**, které vznikly rovněž v rámci stejnojmenného projektu. Tato zařízení jsou přednostně určena pro využití v policejních složkách a kritických infrastrukturách, zejména v oblasti hraniční kontroly (např. letiště, přístavy).

Zařízení 3D FLOW pokrývá mezeru na trhu, a to v podobě kompaktního zařízení, které umožňuje identifikovat či verifikovat osoby na základě otisků prstů a/nebo obličeje, a to ve spojení s biometrickými identifikačními doklady (občanský průkaz, cestovní pas aj.). Jedná se o unikátní zařízení, které zároveň využívá multispektrálního osvětlení pro detekci prezentačních útoků, přičemž tato detekce využívá i další informace ze získaného obrazu, které jednoznačně identifikují použití nástroje prezentačního útoku.

Využití této metodiky je u subjektů kritické infrastruktury (dle směrnice CER je zaváděn termín tzv. „kritické subjekty“) spatřováno zejména v pomoci s definováním možností a limitů nasazení popisovaného zařízení. Dále se jedná o pomoc s nastavením možností a limitů cíleně zvolené dislokace zařízení v rámci provozovaných objektů kritické infrastruktury na takové části provozu, u nichž je žádoucí specificky nastavit a adekvátně implementovat vyšší úroveň systému bezpečnosti. Uživatelem metodiky by měly být provozovatelé a správci kritických infrastruktur, a to zejména v oblasti letišť, přístavů a hraničních přechodů. Nicméně mobilní verze je vhodná i pro provoz cizinecké policie při kontrole osob překračujících státní hranice mimo vyznačené přechody, příp. pohybujících se na území daného státu při podezření na ilegalitu pobytu. Dalším možným použitím je využití ve forenzní medicíně pro postmortem daktyloskopování. Všechny tyto případy použití jsou popsány v kapitole 3.3.

2 CÍLOVÁ SKUPINA

Kritická infrastruktura (KI) obecně tvoří hlavní oblast, u níž je předpokládáno nejširší využití popisovaného zařízení. Uplatnitelnost zařízení je předpokládána nejen u subjektů kritické infrastruktury (tj. provozovatelů prvků KI), které jsou organizačními složkami státu, ale také u subjektů KI, které organizační složkou státu nejsou (tj. soukromé právnické osoby).

Všechny subjekty mají vykonávat zákonem stanovené povinnosti. Další zvyšování úrovně bezpečnosti v oblasti bezpečnosti nad rámec zákonem stanovených povinností poté musí být opodstatněno, odsouhlaseno a systémově zavedeno. Hlavní rozdíl v oblasti bezpečnosti u výše popsaných druhů subjektů kritické infrastruktury může být vnímán v kontextu přístupu k oblasti bezpečnosti. Subjekty náležící mezi organizační složky státu striktně dodržují zákonem stanovené povinnosti a velmi zřídka dochází k dalšímu zvyšování úrovně bezpečnosti. Oproti tomu subjekty nenáležící mezi organizační složky státu vykazují vyšší míru dalšího zvyšování úrovně bezpečnosti.

Z toho důvodu je možné předpokládat zájem o zařízení u subjektů KI, které dlouhodobě vyvíjejí snahu o další zvyšování úrovně bezpečnosti, a to bez ohledu na to, zdali se jedná o soukromé právnické osoby provozující prvek KI či nikoliv.

Ochrana prvků kritické infrastruktury (tj. ochrana kritické infrastruktury obecně) sestává z několika oblastí bezpečnosti, přičemž oblast fyzické bezpečnosti a personální bezpečnosti jsou součástí řešení bezpečnosti. Zařízení může být využito k posilování bezpečnosti zejména u prvků kritické infrastruktury, kde je nutné omezovat přístup pro vybrané osoby.

Biometrické zařízení (nejen 3D FLOW) je doporučováno k využití v částech prvků kritické infrastruktury, kde je nutno řídit přístupy, např.

- dispečink provozovatelů prvků KI;
- dohledová a bezpečnostní centra;
- datová centra a úložiště dat;
- evidování pohybu osob;
- místa bezpečnostních kontrol v objektech;
- vstup do specificky zabezpečených zón.

Částmi prvků kritické infrastruktury jsou myšleny buď vybrané objekty, jejich části či vybrané prostory. Ty je možno rozdělit do tzv. kategorií objektů (prostor) či zařadit do tříd bezpečnostních zón. Kategorie objektů, pro něž je zařízení doporučováno by měly respektovat následující rozdělení (viz tabulka 2.1).

Tabulka 2.1: Kategorie objektů KI.

Kategorie objektu	Název kategorie	Obecná charakteristika
Kat. I	Objekt s kritickým významem pro plnění základní funkce prvku KI	Nenahraditelný objekt nebo obtížně nahraditelný. Výpadek funkce objektu bude mít kritický dopad na zajištění základní funkce prvku KI.

Kat. II	Objekt se zásadním významem	Objekt obtížně nahraditelný pro zajištění poskytování základní funkce prvku KI. Poškození či vyřazení bude mít závažný dopad na zajištění základní funkce prvku KI.
Kat. III	Objekt s důležitým významem	Objekt nahraditelný pro zajištění základní funkce prvku KI jen v případě mimořádných organizačních opatření. Výpadkem funkce objektu dojde k závažným komplikacím v činnosti subjektu KI.
Kat. IV	Objekt podpůrného charakteru	Funkcí objektu je zajištění kontinuální činnosti objektů kategorie I. až III. Vyřazením funkce objektu dojde ke komplikacím v zajišťování základní funkce prvku KI nebo podpůrných činnostech.

Nasazování zařízení by mělo probíhat pro výše uvedené kategorie objektů sestupně, tj. od objektů či prostor nejvíce kritických (primárně kat. I, následně kat. II a dále). Kategorizaci objektů či prostor je možné provést pomocí několika metod analýzy kritičnosti, které mohou být specificky upraveny pro oblast kritické infrastruktury (viz další informace).

Pokud je třeba dále upřesnit nasazení biometrického zařízení pouze pro vybrané části objektů či prostor, je možné provést zařazení vymezených prostor do tzv. třídy bezpečnostních zón. Cílem je dislokovat bezpečnostní zóny v již kategorizovaném objektu. Bezpečnostní zóna je vymezená část objektu nebo prostor, v níž jsou dislokována chráněná aktiva. Bezpečnostní zóny jsou děleny následovně – viz tabulka 2.2.

Tabulka 2.2: Kategorie objektů KI.

Třída bezp. zóny	**Název třídy**	**Obecná charakteristika**
Zvlášť zabezpečená	Zvlášť chráněný prostor s kritickým významem	Striktně režimově vymezený prostor. Musí být dislokován v objektech kat. I a kat. II
Zabezpečená	Prostor se zvýšenou ochranou se zásadním významem	Vymezený prostor, který musí být dislokován v objektech kat. I až kat. III.
Chráněná	Prostor s důležitým významem pro činnost prvku KI	Prostor, v němž jsou umístěny komponenty mající významný vliv na zajištění funkcí kategorizovaných objektů.
Kontrolovaná	Kontrolovaný prostor	Prostor nemající přímý význam pro bezpečnost a kontinuální poskytování funkce prvku KI, ale jejich vyřazení může ohrozit subjekt kritické infrastruktury.

Nasazování zařízení by mělo probíhat pro výše uvedené třídy bezpečnostních zón sestupně, tj. primárně od prostor či zón zvláště zabezpečených dále přes zabezpečené atd. Upřesnění/zatřídění prostor do bezpečnostních zón je možné provést s ohledem na užívání objektu, a to podobným způsobem či metodami, jakými probíhá kategorizace objektu.

Mimo výše uvedené návrhy pro využití zařízení stacionárního charakteru může být využito také přenosné zařízení. Jeho nasazení je předpokládáno jako doplňkové či dočasné řešení v případech, kdy je nezbytné aplikovat vyšší stupeň opatření pro kontrolu přístupu/vstupu. Takovou situací může být např. zvyšování úrovně aplikovaných opatření na ochranu kritické infrastruktury při zvyšování stupně teroristického ohrožení. Právě využití přenosného zařízení za účelem zvýšení úrovně kontroly oprávněných přístupů/vstupů do vymezených prostor může být vhodným doplňkovým řešením.

2.1 Kritické infrastruktury

Objekty KI je možné rozdělit do následujících skupin:

I. Kritická infrastruktura (dle typologie NV 432/2010 Sb.):
- Dispečink výrobce elektřiny (I.A.1.d)
- Technický dispečink provozovatele přenosové soustavy (I.A.2.c);
- Technický dispečink provozovatele distribuční soustavy (I.A.3.b);
- Technický dispečink přepravní soustavy zemního plynu (I.B.1.e);
- a další poměrně velké množství objektů

II. Další typy objektů s vazbou na typologii dle NV 432/2010 Sb.)
- Technický dispečink provozovatele soustavy pro zásobování pitnou vodou (vazba na II.);
- Dispečink správy komunikací/provozu silniční sítě – celostátní, regionální, městský, oblastní (vazba na V.B.c);
- Datové centrum (nebo místo lokalizace provozovatele) vyhlašování vzniku a ukončení smogových situací a regulačních opatření (vazba na VIII.C.g);
- a další poměrně velké množství navazujících objektů

III. Měkké cíle
- Provozovatelé měkkých cílů – zázemí provozu (např. dispečink bezpečnostní služby);
- Místa bezpečnostní kontroly v objektech zvláštního významu nebo v objektech vysoké kumulace osob;
- Typ objektu: církevní objekty;
- Typ objektu: dopravní uzly;
- Typ objektu: kulturní a sportovní centrum;
- Typ objektu: obchodní centrum;
- Typ objektu: školy a školská zařízení;

- Typ objektu: veřejná správa;
- Typ objektu: zdravotnické zařízení;
- Místa bezpečnostní kontroly u dalších typů měkkých cílů (venkovní prostranství, amfiteátr, koncerty, apod.).

Cílem výpisu výše nebylo dát kompletní seznam všech možných KI, ale spíše poukázat na různé možné druhy. Vzhledem k zaměření metodiky na biometrické zařízení byla větší pozornost věnována právě výpisu měkkých cílů.

Analýza a určení konkrétních prvků KI, je na delší diskuzi a nezapadá do rozsahu této metodiky. Zmiňme tedy jen některé: metoda SKI (Švýcarská), CARVER (resp. CARVER 2), AKIS/ACIS, CISIA, AIMS, TRAGIS – bližší informace viz [08].

2.2 Provoz na letištích, v přístavech a hraničních přechodech

Je nutné si uvědomit, že při zabezpečení prostorů v rámci přeshraniční kontroly se nejedná o ochranu KI. I přesto, že letiště samozřejmě do prvků KI patří, tak samotný jeho provoz tj. standardní použití při překonávání hranic nespadá do definic KI. V tomto případě se tak spíše jedná o pomoc cizinecké a dalším složkám Policie ČR. Převážně tedy v souvislosti s nelegální migrací, hledáním nebezpečných osob (využití tzv. *biometric-enabled watchlists* viz [09] – napojení na EU policejní a podobné složky).

V případě kontroly identity osob v přeshraničním provozu je třeba myslet právě na oba typy biometrických zařízení, a to stacionární a mobilní.

U *stacionární verze biometrického zařízení* se jedná o případ, kdy je dané zařízení pevně upevněno na vstupních či prostupních místech. Pod *vstupními místy* si můžeme představit vstupy do objektů či vnitřních prostor (viz kategorie objektu a třída bezpečnostní zóny). Zde se často jedná o zaměstnance daného provozovatele (ať již státního či soukromého). V takovém případě by mělo zařízení umožňovat provádět identifikaci vůči vlastní databázi, tj. zaměstnanci jsou registrováni administrátorem organizace, uloženi v databázi a tím je jim garantován přístup. Biometrické zařízení potom buď může pracovat plně v režimu identifikace, kdy uživatel pouze prezentuje svoji biometrickou charakteristiku (např. otisk prstu či obličej), jeho identita je rozpoznána (nebo není) a je (nebo není) mu udělen přístup. Lze pracovat i s verzí, kdy zaměstnanec používá osobní zaměstnaneckou kartu, tedy před vstupem se identifikuje pomocí dané karty a poté provádí biometrický systém pouze verifikaci, tedy ověření identity. V těchto případech není nutné využití biometrických identifikačních dokladů (cestovní pasy či občanské průkazy). V tomto případě se jedná o klasické využití biometrického zařízení v podobě identifikace či verifikace osoby vůči vlastní databázi, kterou spravuje administrátor organizace (lze např. okamžitě ukončit platnost přístupu zaměstnanci, kterému byl ukončen pracovní poměr). *Prostupním místem* je potom myšlena zejména zóna tzv. biometrických elektronických bran, přes které procházejí cestující za účelem ověření jejich identity vůči biometrickému identifikačnímu dokladu (cestovní pas, občanský průkaz). V tomto případě se jedná o zajištění lokálního přístupu k biometrickým údajům uloženým v daném typu dokladu – viz kapitola 4. Zde je důležité, aby použitý biometrický systém vykazoval interoperabilitu (viz podkapitola 3.2) s ostatními biometrickými systémy dle normy, neboť jen tak je zajištěna porovnatelnost biometrických údajů osoby v biometrickém identifikačním dokladu s aktuálně načtenými údaji. Velkou výhodou je možnost přidání biometrických údajů hledaných osob do vnitřní databáze biometrického systému, kdy dochází nejen k porovnání biometrického vzorku z prezentované biometrické charakteristiky daného jedince s údaji v biometrickém

identifikačním dokladu, ale je možné provést identifikaci se všemi osobami v interní databázi. Interní databáze může obsahovat biometrické šablony (jsou-li dostupné) osob, které jsou hledané či mají zakázaný vstup do daného státu. I jakékoliv zfalšování biometrického identifikačního dokladu, ačkoliv je padělání čipu s platnými podpisy a chráněnými zónami za využití platných certifikátů certifikační autority dané země (téměř) nemožné, biometrická charakteristika prozradí identitu jedince. Zde lze samozřejmě pomýšlet na tvorbu a použití nástroje prezentačního útoku (podvrh biometrické charakteristiky), avšak k odhalení použití tohoto nástroje slouží právě zabudovaná detekce prezentačního útoku, kdy je operátorovi systému (často policista) nahlášeno podezření o použití nástroje prezentačního útoku, kdy je jedinec přesměrován na osobní fyzickou kontrolu. Tam lze potom podrobně prozkoumat otisky prstů, příp. zkontrolovat, zda jedinec nemá nasazenu masku. Tímto způsobem lze velmi významně zvýšit bezpečnost přeshraniční kontroly.

V případě *mobilní verze biometrického zařízení* se jedná v principu o totožné zařízení. Podaří-li se vytvořit stacionární verzi biometrického zařízení (byl to náš cíl) dostatečně kompaktní, aby byla přenositelná, postačuje doplnění baterie, aby bylo zařízení nezávislé na externím přívodu napájení. V takovém případě je zařízení přenosné a lze jej použít kdekoliv v terénu, tj. je možné kontrolovat cestující např. na letištní ploše (v případě nouzového přistání), přímo na palubě lodi (např. propuknutí onemocnění u výletních lodí) či kdekoliv v terénu, kdy je třeba ověřit identitu osoby vůči biometrickému identifikačnímu dokladu. V případě kontroly jedince vůči hledaným osobám (obecně osobám zájmu) je třeba buď mít přístup k internetu (kvůli kontrole vůči aktuální verzi osob zájmu) nebo si před odchodem do terénu tuto databázi aktualizovat e vnitřní paměti zařízení.

Naše zařízení 3D FLOW (viz kapitola 5) všechny tyto výše uvedené požadavky splňuje. Toto námi zkonstruované zařízení lze použít jako docházkový, přístupový či biometrický kontrolní systém pro všechny výše uvedené kombinace. V rámci naší společnosti máme i nabídku cloudového řešení, kdy je třeba zajistit on-line provoz zařízení.

2.3 Postmortem daktyloskopování

Zvláštním příkladem použití námi zkonstruovaného zařízení 3D FLOW (viz kapitola 5) je postmortem daktyloskopování. Toto probíhá dosud na ústavech soudního lékařství kontaktní metodou, kdy je třeba styk pokožky zesnulého jedince s podložkou, na kterou se otiskuje reliéf kůže bříška prstu (příp. celé palmární části ruky). V některých případech je kůže jedince ve špatné kondici, kdy může dojít jakýmkoliv stykem s jiným předmětem k deformaci či nenávratnému poškození papilárního terénu. K tomuto účelu je výhodné využít bezkontaktního způsobu snímání otisků prstů, což naše zařízení umožňuje (mobilní verze s velkou výhodou předčí stacionární verzi díky manipulovatelnosti u zesnulého jedince). Zde je třeba myslet na vypnutí detekce prezentačního útoku, neboť neživá tkáň vykazuje atributy, které detektor prezentačního útoku vyhodnotí jako použití nástroje prezentačního útoku. Deaktivováním detekce prezentačního útoku dojde k nasnímání otisků prstů. Pro tento účel jsme vytvořili i verzi zařízení, která umožňuje multispektrální osvětlení povrchu kůže, což může sehrát velmi významnou roli např. u zvrásnělé kůže, kdy pod infračerveným světlem získáme poměrně značné množství informace o podkožní vrstvě, která obsahuje základ tvorby papilárních linií. Další podrobnosti, byť došlo k měsíčnímu testování zařízení na rozličných ústavech soudního lékařství, přesahují rámec tohoto metodického dokumentu.

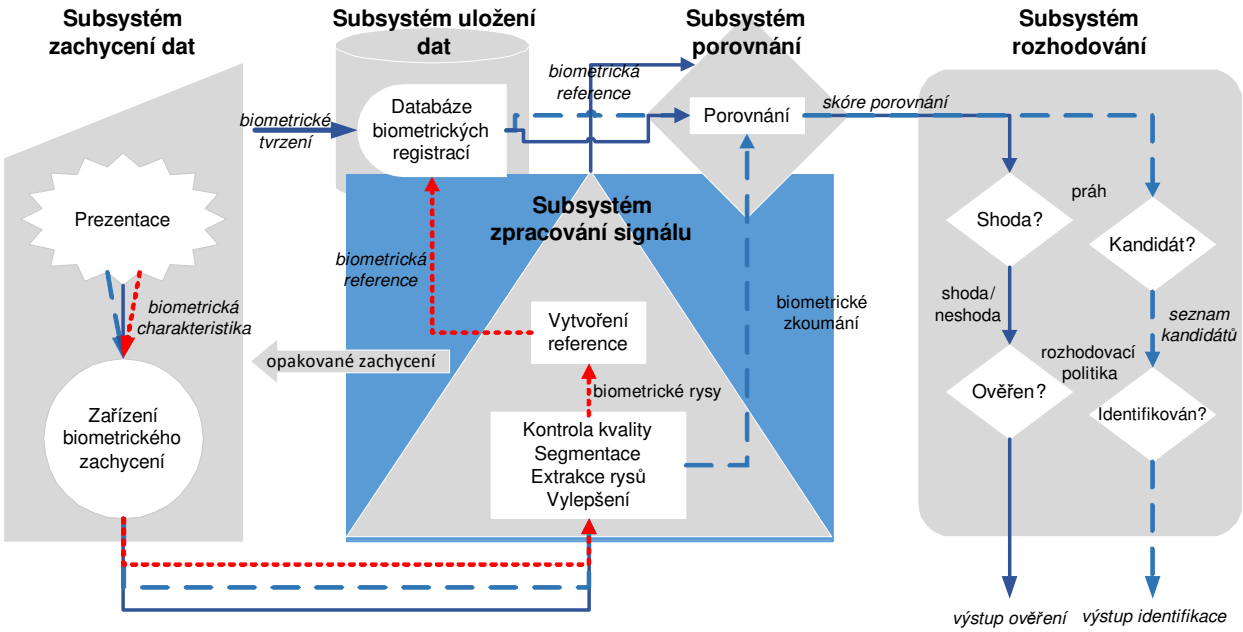
3 NORMY A LEGISLATIVA PRO BIOMETRICKÉ SYSTÉMY

Cílem této kapitoly není podat dokonalý a podrobný výklad o všech možnostech, úskalích a detailech biometrie, ale spíše zdůraznit prvky důležité pro použití biometrie pro zabezpečení objektů či prostor. Přesnější informace mohou být nalezeny v brožuře pro obyvatele ohledně biometrických systémů [01], dále v normách ČSN (příp. dosud nepřeložených biometrických norem ISO/IEC; např. [12]) týkajících se jak výkonnosti, tak obecně fungování biometrických systémů – viz podkapitola 3.2.

Na úvod zde budou zmíněny základní informace ohledně biometrického systému a používaných (nebo naopak velmi nedoporučovaných) biometrických charakteristik. Na to navazuje podkapitola věnující se biometrické výkonnosti a možnosti, jak zvýšit, snížit nebo si ověřit výkonnost biometrických systémů. Poslední dvě podkapitoly se věnují obecněji normám, které se týkají výše uvedených bodů, technických údajům a parametrům biometrických snímačů a prvkům ochrany osobních údajů (hlavně biometrických údajů) dle GDPR.

3.1 Biometrické systémy

Biometrický systém [09] zajišťuje automatizované rozpoznávání lidských jedinců na základě jejich charakteristických *anatomických* a *behaviorálních rysů*. Obecný biometrický systém je schematicky znázorněn na obrázku 3.1 (obrázek převzat z normy [02]). Na samotném začátku je zařízení biometrického zachycení snímající prezentovanou biometrickou charakteristiku. Ta může být snímána s vědomím nebo bez vědomí uživatele. Získaná data (biometrický vzorek) putují do modulu subsystému zpracování signálu, kde se provádí kontrola kvality, segmentace, extrakce rysů, příp. vylepšení dat. Zároveň se zde vytvoří reference (šablona), která vstupuje při registraci do subsystému uložení dat, při požadavku na porovnání potom přímo do subsystému porovnání, který si zároveň vyžádá biometrickou referenci ze subsystému uložení dat, příp. přístup ke všem referencím. Tato šablona se následně porovná se šablonou uloženou v databázi. Výsledkem je míra shody obou šablon (skóre porovnání), která putuje do aplikace (např. zámku pro otevření dveří). Subsystém porovnání provádí buď porovnání 1:1 (reference vůči referenci; verifikace) či 1:M (reference vůči všem referencím v subsystému uložení dat; identifikace), přičemž jako výsledek předává buď 1 skóre porovnání (verifikace) či seznam skór porovnání (identifikace). Subsystém rozhodování potom provede rozhodnutí s ohledem na požadavek, tj. verifikaci či identifikaci. Takový obecný biometrický systém může pracovat s jakýmkoliv vstupním signálem, avšak ve zcela majoritní skupině biometrických systémů se jedná o obrazová či videosekvenční data. Dalším důležitým aspektem je použití systému detekce prezentačního útoku, který není v daném obrázku zohledněn (viz podkapitola 3.2).



Obrázek 3.1: Obecný biometrický systém [02].

Různé *biometrické charakteristiky* [10] mají rozličné vlastnosti (jedinečnost, míru stárnutí, měřitelnost, apod.) a díky nim se potom více či méně hodí pro dané využití. Biometrický systém vyvažuje tři základní vlastnosti: jedná se o přesnost (porovnání dvou šablon), škálovatelnost (kolik šablon je schopen odlišit) a pohodlí (jak snadné je systém využít). Biometrický systém, který vykazuje maximální přesnost, škálovatelnost a pohodlí, neexistuje. Velmi často jsou tyto požadavky protichůdné.

Pro modelové využití na ochranu KI vyžadujeme: co nejvyšší přesnost (nejdůležitější parametr – viz podkapitola 3.2, týkající se biometrické výkonnosti); dostatečnou škálovatelnost pro očekávaný počet osob (který bude z pohledu biometrických systémů poměrně nízký, např. stovky uživatelů) a na pohodlí téměř nemáme požadavky (nevadí, pokud je systém složitější, pokud plní předchozí funkce).

Pro modelové využití na letištích či v přístavech (příp. dalších přeshraničních činnostech) je situace trochu jiná. Bavíme-li se o přepravě osob, potom vyžadujeme: vysokou škálovatelnost (teoreticky musí obsáhnout všechny jedince na naší planetě); nabízet poměrně velké pohodlí použití (není možné každou osobu školit na dané zařízení, zařízení musí pracovat na první pokus, a to co nejtransparentněji); co nejvyšší přesnost při dodržení předchozích parametrů. Ačkoliv to může vypadat protichůdně, pokud zařízení nepojme dostatečný počet osob, je irelevantní, že je přesné, pokud bude složité a veřejnost ho nebude chtít využívat, tak nesplní očekávanou funkcionalitu.

Má-li biometrický systém splnit oba účely, je vhodné, aby obsahoval přísnější režim pro KI (s důrazem na přesnost) a následně volnější režim pro přeshraniční kontrolu (s důrazem na snadnost použití i přesnost). Biometrické charakteristiky je třeba volit tak, aby splnily kritéria obou variant. Níže je uveden přehled vhodných biometrických charakteristik, méně vhodných a zcela nevhodných.

Vhodné biometrické charakteristiky [11]: *otisky prstů* (součástí mezinárodních biometrických identifikačních dokladů), *obličej* (součástí mezinárodních biometrických identifikačních dokladů), *duhovka oka* (součástí mezinárodních biometrických identifikačních dokladů), dlaň (cévní řečiště či otisk).

Méně vhodné biometrické charakteristiky: *sítnice oka* (nepříjemná pro uživatele a obtížně získatelná), *termogram* (není dostatečně rychlá a přesná zároveň), *chůze* (komplikovanější snímání a nižší rozlišovací schopnost).

Nevhodné biometrické charakteristiky: *geometrie ruky* (nízká rozlišovací schopnost a škálovatelnost), *dentální obraz* (komplikované snímání a nevhodnost pro opakování), *podpis* (nízká škálovatelnost; přesný pouze při behaviorálním snímání s využitím dynamických vlastností), *tvar ucha* (nepřesný a komplikované snímání), *struktura nehtu* (nepřesná), *DNA* (komplikované až nereálné snímání), *hlas* (nepřesný a malá škálovatelnost), *mimika obličeje* (nízká přesnost a škálovatelnost, avšak velmi vhodná pro detekci prezentačního útoku), *dynamika stisku kláves* (komplikované snímání a pro přeshraniční kontrolu zcela nevhodné), *pohyby rtů* (nízká přesnost a škálovatelnost).

Samozřejmě platí, že i vhodné (námi doporučené) biometrické charakteristiky mají své silnější a slabší stránky. Tato diskuse však přesahuje rámec tohoto metodického dokumentu. Podrobnosti k výhodám a nevýhodám jednotlivých biometrických charakteristik lze nalézt např. v [09][11][12].

3.2 Normy – biometrická výkonnost

Nejprve se podívejme na samotný pojem *biometrická výkonnost*. Pod tímto slovním spojením se skrývá způsob vyjádření spolehlivosti, přesnosti, opakovatelnosti a mnoha dalších vlastností biometrických systémů, včetně požadavků na časovou a výpočetní náročnost. Obecná biometrická výkonnost je popsána zejména v řadě norem ISO/IEC 19795 (v českém překladu vyšly některé z nich, např. [02]) – tuto normu lze tedy brát jako úplný základ, nicméně různé zmínky lze nalézt i v dalších normách, např. ISO/IEC 30107 (řada se týká detekce prezentačního útoku), ISO/IEC 24745 (ochrana biometrických informací) či velmi důležitý harmonizovaný biometrický slovník ISO/IEC 2382-37. Níže si uvedeme pár významných pojmů v oblasti biometrické výkonnosti, přičemž je zde primárně využito výše uvedených zdrojů.

3.2.1 Míra selhání snímání

Míra selhání snímání (**FTA** – *Fail To Acquire*; používá se i **FTC** – *Fail To Capture* ve stejném významu) je podíl verifikací či pokusů, u kterých systém selže při snímání či lokalizaci vzorku s dostatečnou kvalitou. Míra selhání snímání zahrnuje:

- pokusy, kde systém není schopen lokalizovat biometrický vzorek, přestože je prezentován,
- pokusy, u nichž selže segmentace, a
- pokusy, ve kterých nesplňuje nalezený vzorek práh kontroly kvality samotného snímače.

Míra selhání snímání by měla být určena jako podíl (nebo vážený podíl) zaznamenaných pokusů oprávněných uživatelů (a pokud možno každý on-line pokus útočníka s nulovým úsilím), které nemohly být dokončeny z důvodu selhání při prezentaci (není nasnímán žádný obraz), segmentaci či kontroly kvality.

Míra selhání snímání závisí na prazích pro kvalitu vzorku, stejně jako povolená doba trvání snímání vzorku či povolený počet prezentací. Tato nastavení by měla být obsažena ve zprávě současně s pozorovanou mírou selhání snímání. Tato míra tak primárně ukazuje kvalitu použitého senzoru.

Pokusy, kdy nebyl nasnímán či zpracován vzorek nebo nesplnil prahy kvality, nejsou zpracovány algoritmem porovnání a negenerují skóre porovnání. Taková selhání snímání by měla být vyňata z výpočtu chybových měr chybné shody a chybné neshody, ale měly by být zahrnuty v kalkulaci měr chybného přijetí a chybného odmítnutí. Míry selhání snímání, chybné shody a chybné neshody by měly být spočteny za stejných nastavení prahu akceptace kvality.

3.2.2 Míra selhání registrace

Míra selhání registrace (**FTE** – *Fail To Enroll*; významově téměř totožný je i název **FTX** – *Fail To eXtract*) je podíl populace, pro kterou systém selže při kompletaci procesu registrace. Míra selhání registrace zahrnuje takové jedince:

- z jejichž nasnímaného biometrického vzorku není možné extrahovat rysy používané daným systémem,
- kteří nejsou schopni vyprodukovat vzorek s dostatečnou kvalitou při registraci (což zahrnuje i ty kteří selžou vlivem nezkušenosti s používáním daného zařízení), a
- kteří nemohou spolehlivě vyprodukovat rozhodnutí shody s jejich nedávno vytvořenou šablonou během pokusů o potvrzení použitelnosti registrace.

Míra selhání registrace u cílové populace by měla být určena jako podíl (nebo vážený podíl) skupiny testu, kteří nemohli být registrováni za předem definované registrační politiky.

Míra selhání registrace závisí na registrační politice, která řídí práh kvality vzorku pro registraci, práh rozhodnutí pro potvrzení použitelnosti registrace (tedy úspěšnost extrakce rysů používaným systémem) a počet pokusů nebo času přípustných pro registraci v registrační transakci. Politika registrace by měla být popsána společně s pozorovanou mírou selhání registrace.

Podobně jako u předchozí míry by pokusy uživatelů neschopných registrovat se do systému neměly přispívat k míře selhání snímání nebo chybovým mírám porovnání.

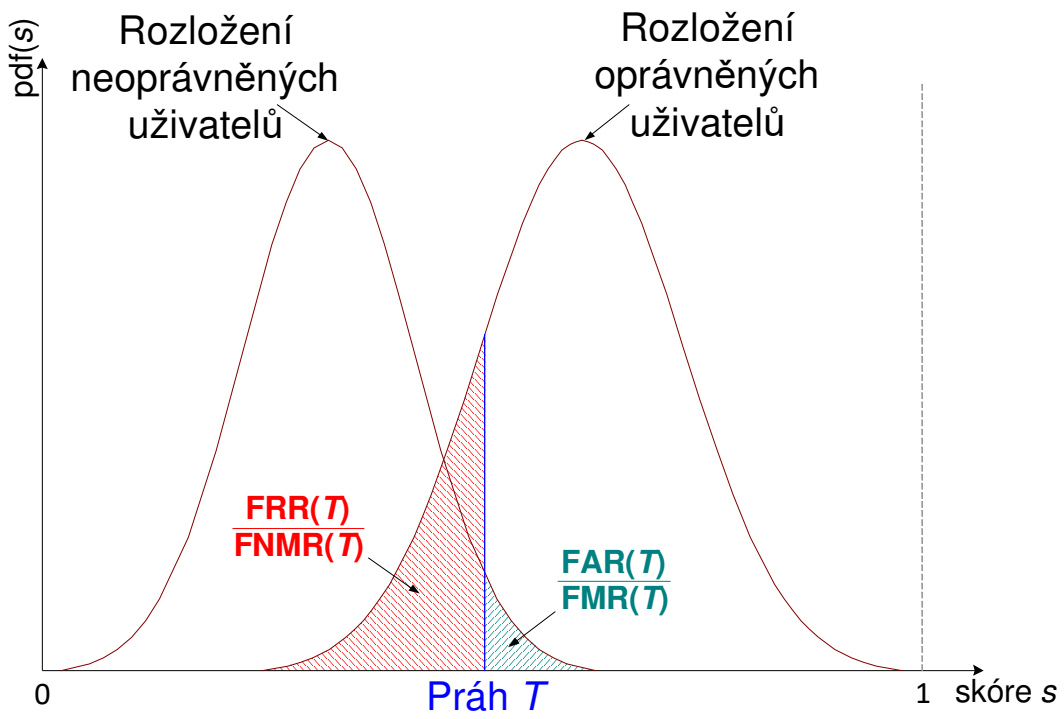
3.2.3 Míra chybné neshody

Míra chybné neshody je podíl vzorků získaných z pokusů oprávněných uživatelů, které jsou chybně deklarovány jako neshodné se šablonou stejné vlastnosti od stejného uživatele, jenž poskytl vzorek.

Míra chybné neshody by měla být odhadnuta jako podíl (nebo vážený podíl) zaznamenaných pokusů oprávněných uživatelů, kteří prošli podsystémem porovnání, u kterých skóre vyprodukované podobnosti leželo pod prahem rozhodnutí.

3.2.4 Míra chybného zamítnutí

Míra chybného zamítnutí (**FRR** – *False Rejection Rate*; odpovídá přibližně **FNMR** – *False Non-Match Rate* – viz obrázek 3.2) je podíl oprávněných verifikačních transakcí, které byly chybně zamítnuty. Transakce se může skládat z jednoho nebo více oprávněných pokusů v závislosti na rozhodovací politice.



Obrázek 3.2: Rozložení oprávněných a neoprávněných uživatelů s chybovými mírami.

Míra chybného zamítnutí se stanovuje jako podíl (nebo vážený podíl) zaznamenaných oprávněných transakcí, které byly chybně zamítnuty. Mezi chybně zamítnuté transakce se zahrnují jak transakce zamítnuté z důvodu selhání snímání, tak i transakce zamítnuté z důvodu chybného porovnání.

Míra chybného zamítnutí závisí na rozhodovací politice, na hodnotě prahu rozhodnutí o shodě a na hodnotě prahu kvality vzorku. Hodnota míry chybného zamítnutí se zaznamená s těmito detaily spolu s mírou chybného přijetí stanovenou za stejných podmínek (nebo bude zobrazena graficky v křivkách ROC (*Reciever Operating Curve*) či DET (*Detection Error Trade-off*) viz dále, spolu s mírou chybného přijetí stanovenou při stejných prahových hodnotách).

3.2.5 Míra chybného přijetí

Míra chybného přijetí (**FAR** – *False Acceptance Rate*; odpovídá přibližně **FMR** – *False Match Rate* – viz obrázek 3.2) je očekávaný podíl neoprávněných transakcí provedených s nulovým úsilím útočníka, které jsou chybně přijaty. Transakce se může skládat z jednoho nebo více neoprávněných pokusů v závislosti na rozhodovací politice.

Míra chybného přijetí se stanovuje jako podíl (nebo vážený podíl) zaznamenaných transakcí provedených s nulovým úsilím útočníka, které byly chybně přijaty.

Míra chybného přijetí závisí na rozhodovací politice, na hodnotě prahu rozhodnutí o shodě a na hodnotě prahu kvality vzorku. Hodnota míry chybného přijetí se zaznamená s těmito detaily spolu s mírou chybného zamítnutí stanovenou za stejných podmínek (nebo bude zobrazena graficky v křivkách ROC či DET spolu s mírou chybného zamítnutí stanovenou při stejných prahových hodnotách).

3.2.6 Míra oprávněného přijetí

Míra oprávněného přijetí (**GAR** – *Genuine Acceptance Rate*; odpovídá přibližně **TMR** – *True Match Rate*) je doplněk k míře FRR (resp. FNMR), tedy vyjadřuje podíl oprávněných verifikačních transakcí, které byly správně potvrzeny. Všechna výše zmíněná pravidla pro tyto míry tak platí i pro tento doplněk.

3.2.7 Míra oprávněného zamítnutí

Míra oprávněného zamítnutí (**IRR** – *Impostor Rejection Rate*; odpovídá přibližně **TNMR** – *True Non-Match Rate*) je doplněk k míře FAR (resp. FMR), tedy vyjadřuje podíl neoprávněných verifikačních transakcí, které byly správně zamítnuty. Všechna výše zmíněná pravidla pro tyto míry tak platí i pro tento doplněk.

3.2.8 Míra vyrovnání chyb

Místo, kde se na obrázku 3.2 protnou rozložení opravněných a neoprávněných uživatelů, se nazývá míra vyrovnání chyb (**EER** – *Equal Error Rate*). Pokud je práh T nastaven na tuto hodnotu, pak platí, že míra chybného přijetí a míra chybného odmítnutí dosahují stejné hodnoty.

Mezi výrobci systémů se pak vžil přenesený význam, a to je přímo hodnota FAR (a FRR) pro práh nastavený na EER. Toto označení není přesné, ale bývá využíváno, a proto je zde zmíněno. Pomocí této hodnoty je pak možné systémy vůči sobě porovnávat. Nicméně je třeba vzít vždy v úvahu, že nastavení prahu na EER není vždy žádoucí a vhodné. Velmi záleží na očekávaném využití systému.

Výkonnost shody a/nebo rozhodování biometrického systému přes rozmezí rozhodovacího prahu by měla být znázorněna graficky buď ROC (*Receiver Operating Curve*) nebo DET křivkami, ne však oběma.

Měřítko osy (znázornění minima a maxima a použití logaritmického měřítka) by mělo být zvoleno tak, aby byly výsledky zřetelné a jasně interpretovatelné, a měly by být konzistentní u různých grafů v celé zprávě. Je-li nutné změnit měřítko, aby byla zajištěna zřetelnost, měla by být uvedena poznámka poukazující na změnu měřítka.

K porovnání výkonu různých systémů jsou vhodnější, než základní míry chyb, chyby rozhodovací DET nebo ROC (míra chybného zamítnutí versus míra chybného přijetí), které ukazují kombinovaný efekt chyb shody, selhání snímání obrazu, chyby rozdělení dat dle třídy a selhání registrace.

3.2.9 Křivka detekce chyb porovnání/operační charakteristiky příjemce

Křivka detekce chyb porovnání (*Detection Error Trade-off*, **DET**) se konstruuje za využití dosažených skóre shody oprávněných uživatelů a útočníků získaných porovnáním příznaků z jednotlivých pokusů a jednotlivých registračních šablon. Skóre shody každého pokusu bude zaznamenáno. Výsledky pokusů oprávněných uživatelů budou seřazeny. S výsledky pokusů útočníků bude naloženo stejně. Hodnoty ležící daleko mimo meze by měly být prozkoumány, aby byla zjištěna případná chyba klasifikace. Odstranění jakýchkoliv výsledků z testu by mělo být plně dokumentováno a povede k externímu posouzení výsledků testu.

Křivky DET (nebo ROC) jsou stanoveny jako akumulace seřazených skór oprávněných uživatelů a útočníků. Výsledky nabývají různých možných hodnot, proto je křivka DET (nebo ROC) znázorněna parametricky tak, že každý bod (x, y) reprezentuje míru chybné shody a chybné neshody, využívaje výsledek shody jako rozhodovacího prahu.

Míra chybné shody je podíl výsledků shody útočníků rovných nebo větších než je aktuální hodnota rozhodovacího prahu a míra chybné neshody je podíl výsledků shody oprávněných uživatelů menších, než je hodnota rozhodovacího prahu. Křivky by měly být znázorněny s mírou chybné shody na ose x a s mírou chybné neshody na ose y. Osy znázorňující míry chyb mohou využít logaritmického měřítka.

Křivky DET (nebo ROC) mohou být podobným způsobem také použity ke znázornění vztahu mezi mírou chybného přijetí a mírou chybného zamítnutí. Míra chybného přijetí a míra chybného zamítnutí bude záviset na míře chybné shody, míře chybné neshody a na selhání snímání způsobem závislým na rozhodovací politice. Transakce s více pokusy mohou vyžadovat vytvoření nového výsledku transakce založeného na podobnosti výsledků dílčích pokusů (např. rozhodovací politika založená na výběru maximální hodnoty výsledků shody ze tří pokusů). Podobně lze křivky DET (nebo ROC) použít ke znázornění vztahu mezi mírami chyby identifikace.

Křivky DET mohou být použity ke znázornění míry chyby shody (míra chybné neshody v závislosti na míře chybné shody), míry chyby rozhodnutí (míra chybného zamítnutí v závislosti na míře chybného přijetí) a míry chyby identifikace nad otevřenou množinou (míra chybně negativní identifikace v závislosti na míře chybně pozitivní identifikace).

Je možné použít logaritmické měřítko k rozprostření jednotlivých průběhů, aby bylo dosaženo jasnějšího znázornění výsledků. V případě použití logaritmického měřítka je možné nulovou míru chyby pozorovanou v N případech znázornit jako hodnotu $0{,}5/N$ nebo jako minimum daného měřítka, je-li větší než tato hodnota.

Křivky ROC jsou tradiční metodou shrnutí výkonnosti neúplné diagnostiky, detekce a systémů rozpoznávání vzorů. Křivky ROC nejsou závislé na prahu, což umožňuje porovnání výkonu rozdílných systémů za podobných podmínek nebo jednoho systému za různých podmínek. Křivky ROC mohou být použity ke znázornění výkonu algoritmu testování shody (1-míra chybné neshody v závislosti na míře chybné shody), výkonu koncového verifikačního systému (1-míra chybného zamítnutí v závislosti na míře chybného přijetí), ale i výkonu systému identifikace nad otevřenou množinou (míra (správné) identifikace v závislosti na míře chybně pozitivní chyby identifikace).

Existují různé souhrny bezpečnostních požadavků, které odpovídají třídám bezpečnosti biometrických řešení, např. Google/Android (viz [03]) nebo FIDO (viz [04]). Dle těchto doporučení se pohybují např. hodnoty FRR až u 10 %, zatímco FAR u hodnoty $2{\cdot}10^{-5}$. Zde se však jedná primárně o mobilní zařízení.

V současné době existuje pouze jedna úroveň certifikace pro biometrické požadavky (úroveň certifikace 1) dle FIDO [05] – viz text níže. Proto se všechny požadavky zmíněné v následujícím textu vztahují na tuto úroveň. Biometrický certifikační program FIDO používá k měření biometrického výkonu chybného odmítnutí (FRR) a míru chybného přijetí (FAR).

Míra chybného odmítnutí **FRR** musí splňovat to, že její hodnota bude menší než 3:100 pro horní hranici 80% intervalu spolehlivosti. FRR se měří na úrovni transakce. Skutečně dosažené FRR musí být dokumentováno laboratoří. Prahová hodnota musí být během testování pevně stanovena a neměnná. Nastavuje ji prodejce a musí odpovídat deklarované hodnotě FAR, která má být testována. Počet pokusů transakce je omezen na 5. Zdokumentovány musejí být všechny chyby (hlavně FTA), na které se při testování narazilo.

Míra chybného přijetí **FAR** musí splňovat požadavek, že její hodnota bude menší než 1:10 000 pro horní hranici 80% intervalu spolehlivosti. FAR se měří na úrovni transakce. Míra chybného přijetí je očekávaný podíl neoprávněných transakcí s nulovým úsilím, které budou (nesprávně) přijaty. Transakce může sestávat z jednoho nebo více neoprávněných pokusů v závislosti na zásadách rozhodování. Míra chybného přijetí musí být odhadnuta jako podíl (nebo vážený poměr) zaznamenaných neoprávněných transakcí s nulovým úsilím, které byly (nesprávně) přijaty. FAR bude záviset na zásadách rozhodování, prahu porovnání a prahu pro kvalitu vzorku. Hodnota FAR tak musí být publikována včetně těchto detailů současně s hodnotami FRR (případně mohou být obě zobrazeny v ROC nebo DET křivce). Prah musí být zvolen stejně jako u FRR. Stejně jako u FRR jsou i zde platná omezení na počet pokusů. U této metriky však nesmí být do výpočtu zahrnuty pokusy končící FTA.

Dále jsou uvedena pravidla týkající se **využití nástrojů prezentačního útoku** (PAI). 5 ze 6 zvolených PAI úrovně A (primitivní útoky, viz tabulka 5.1) musí dosáhnout méně než 20% IAPMR. K tomu navíc všechny PAI úrovně A musí dosáhnout méně než 50% IAPMR. Dále 3 ze 4 zvolených PAI úrovně B musí dosáhnout méně než 20% IAPMR a všechny tyto PAI musejí dosáhnout méně než 50%. Přesné hodnoty IAPMR musejí být dokumentovány laboratoří. Práh musí být pevně zvolen prodejcem (a odpovídat prahu pro FAR/FRR). Na transakci útoku nesmí být povoleno více než pět pokusů. Pro PAI by měl být použit maximální počet pokusů transakce nebo dokud není porovnán (což má za následek chybu). FTA se v tomto případě nepočítá za chybu, neboť některé systémy reagují na detekci PAI pomocí FTA.

Z bezpečnostních důvodů by poskytnuté šablony k registraci a ověřovací transakce měly být **chráněny** jako důvěrné a autentizace dat by měla být chráněná pomocí kryptografických algoritmů uvedených v seznamu povolených kryptografií FIDO. Laboratoř musí hlásit FIDO proces používaný k zajištění konzistence a bezpečnosti testovaného zařízení.

3.3 Legislativa (GDPR)

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů), ve zkratce **GDPR** (*General Data Protection Regulation*), představuje právní rámec ochrany osobních údajů v evropském prostoru, které od 25. května 2018 přímo stanovuje pravidla pro zpracování osobních údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak Obecné nařízení od 25. května 2018 nahradilo zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Charakteristická pro Obecné nařízení je jeho univerzální použitelnost ve všech státech Evropské unie (a Islandu, Norska a Lichtenštejnska) a tudíž i sjednocující účinek, jelikož jednotná pravidla pro zpracování osobních údajů platí v každém státě EU a třech dále vyjmenovaných. V ČR dále platí zákon č. 110/2019 Sb., o zpracování osobních údajů.

V České republice se aspekty osobních údajů zabývá Úřad pro ochranu osobních údajů[1], pod jehož kompetenci spadají biometrické identifikační dokumenty, pochopi-

[1] https://uoou.gov.cz/

telně včetně biometrických údajů, které jsou považovány za osobní údaj (a to v jakékoliv podobě umožňující reidentifikaci osoby). Na evropské úrovni se zabývá problematikou ochrany osobních údajů Evropská komise[2] (EC – *European Comission*).

U elektronických zařízení je třeba dbát na jejich bezpečnost, což zajišťuje revize konstrukce daného zařízení (platnost v každé zemi EU je jiná), v ČR ideálně dle zákona č. 250/2021 Sb., o bezpečnosti práce v souvislosti s provozem vyhrazených technických zařízení a o změně souvisejících zákonů (podrobnosti viz [06]). Touto problematikou se zabývá rovněž nařízení č. 190/2022 Sb., o vyhrazených technických elektrických zařízeních a požadavcích na zajištění jejich bezpečnosti. Částečně pokrývá bezpečnost daného zařízení i certifikace CE[3], která se týká nově zaváděných zařízení na trh, a to nejen po elektrické stránce, ale i mechanické bezpečnosti.

V případě bezpečnostních požadavků na dané zařízení je třeba zhodnotit, pro jaké prostory a za jakým účelem má být zařízení použito. Zde lze v ČR vycházet např. ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dohled nad tímto zákonem má na starosti Národní bezpečnostní úřad[4] a Národní úřad pro kybernetickou a informační bezpečnost[5].

Dodržování norem, a to zejména ČSN, příp. neexistuje-li lokalizace do českého jazyka, potom ISO/IEC, příp. ANSI, je víceméně dobrovolné. Významným benefitem však je zajištění interoperability mezi dalšími systémy, což je např. pro provoz přeshraničních kontrol nezbytné.

Dále existuje definice datového formátu[6] biometrických identifikačních dokladů dle Mezinárodní organizace pro civilní letectví (ICAO). Podrobnější popis je k nalezení v kapitole 4.

3.4 Legislativa – rozbor k zařízení 3D FLOW

Právní rozbor v této podkapitole navazuje na předchozí výzkumnou činnost v oblasti vztahu biometrických údajů a ochrany osobních údajů [13].

V předchozím textu byl v rámci této metodiky představen systém založený na zpracování biometrických osobních údajů, konkrétně zařízení TBS 3D FLOW, a možností jeho využití při ochraně specifických cílových prostředí, které může představovat např. některá z kritických informačních infrastruktur ve smyslu zákona o krizovém řízení[7], nebo další prostředí jako např. provoz letiště, přístavy a hraniční přechody; zcela specifické je využití zařízení pro účely postmortem daktyloskopování.

Výše popsané zařízení TBS 3D FLOW je založeno na zpracování biometrických osobních údajů, při němž dochází ke shromažďování, zaznamenávání, uspořádání, zaznamenávání, uchovávání či jinému zpracování osobních údajů[8]. Obecně platí, že technologie biometrických zařízení jsou založeny na zpracování biometrických údajů jako osobních údajů, které umožňují pravděpodobnostní identifikaci a autentizaci osoby.

[2] https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en
[3] https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1415011214675&uri=CELEX:32008D0768
[4] https://www.nbu.cz/
[5] https://nukib.gov.cz/
[6] https://www.icao.int/publications/documents/9303_p9_cons_en.pdf
[7] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů
[8] Čl. 4 odst. 1 GDPR

Tato zařízení umožňují s vysokou pravděpodobností určit, že osoba je tou, za níž se vydává, což přispívá k bezpečnosti osob a dalších hodnot v cílovém prostředí, které takovou ochranu vyžaduje. Na procesy zpracování osobních údajů se vztahuje právní rámec ochrany osobních údajů. Ačkoliv veřejnost většinou předpokládá, že se na zpracování osobních údajů vztahuje obecné nařízení na ochranu osobních údajů, tento předpoklad neplatí vždy. Určení příslušné právní úpravy závisí na účelu zpracování osobních údajů, případně na subjektu, který údaje zpracovává. Podle toho se v členských státech EU uplatní buď nařízení 2016/679/EU, známé jako obecné nařízení o ochraně osobních údajů či GDPR (dále GDPR)[9], nebo směrnice 2016/618/EU, které je nazývána jako trestněprávní směrnice nebo směrnice pro vymáhání práva (dále trestněprávní směrnice)[10], která byla navržena za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. Zatímco obecné nařízení je přímo účinné, s případnými výjimkami, pokud jde o ustanovení, která odkazují na vnitrostátní úpravu, směrnice 2016/680 byla do právního řádu ČR převedena zákonem č. 110/2019 Sb., o zpracování osobních údajů, který jednak provádí trestněprávní směrnici, jednak v omezeném rozsahu upravuje některé otázky na základě zmocnění v obecném nařízení ve vztahu k některým dílčím oblastem, jak bylo výše uvedeno.

Ochranu osobních údajů je kromě toho třeba chápat i v kontextu základních práv, protože právo na osobní údaje a právo na soukromí jsou hodnoty, jimž poskytuje ochranu ústavní rámec, tj. Listina základních práv EU či obdobný katalog základních práv v ČR. To prakticky znamená specifickou, vyšší či silnější úroveň ochrany než v případě běžných zákonů. V tomto ohledu obecné nařízení výslovně uvádí, že zohledňuje základní právo na ochranu osobních údajů podle čl. 8 Listiny základních práv EU (dále Listina), rovněž však další základní práva, s nimiž musí být právo na ochranu osobních údajů v souladu na základě principu proporcionality[11]. V praxi se nastavení uvedené zvýšené ochrany uplatňuje prostřednictvím článku 52 odst. 1 Listiny základních práv EU, *podle nějž každé omezení výkonu práv a svobod uznaných Listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.* V tomto případě se jedná o abstraktní požadavky, které jsou do praxe převáděny prostřednicím aplikace požadavků článku 52 a GDPR, přičemž k jejich interpretaci lze použít metodické pokyny Sboru pro ochranu osobních údajů či soudní judikaturu, především Soudního dvora EU.

Obecné nařízení na ochranu osobních údajů a trestněprávní směrnice jsou založeny na tom, že zpracování osobních údajů musí být v souladu s obecnými zásadami obecného nařízení, mezi něž patří zákonnost, korektnost a férovost zpracování osobních údajů, účelové určení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost a odpovědnost správce[12]. V tomto kontextu je třeba zdůraznit především klíčové postavení principu odpovědnosti správce, který je plně odpovědný za nastavení

[9] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

[10] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV

[11] Bod 5 a 6 Preambule GDPR

[12] Články 5 a 6 GDPR a článek 4 trestněprávní směrnice

souladu s požadavky ochrany osobních údajů. Prakticky to znamená, že správce musí vědět, jaké právní předpisy ochrany osobních údajů se na něj vztahují, jaké zpracování a za jakým účelem provádí. Na každé konkrétní zpracování osobních údajů musí správce aplikovat zásady ochrany osobních údajů. Výchozí právní rámec může představovat buď obecné nařízení na ochranu osobních údajů, nebo tzv. trestněprávní směrnice provedená zákonem č. 110/2019 Sb., o ochraně osobních údajů. Obecně lze uvést, že požadavky stanovené obecným nařízením jsou přísnější a detailnější než požadavky trestněprávní směrnice. Obě normy přitom z hlediska obsahu upravují stejné otázky, kdy definují, co se rozumí zpracováním osobních údajů, a stanoví pravidla (zásady), které je přitom potřebné dodržovat. Ačkoli jsou definice pojmů a používaných institutů v obou předpisech shodné, nastavení požadovaných podmínek ve vztahu k nim se liší.

V této metodice popsané zařízení TBS 3D FLOW je založeno na zpracování biometrických osobních údajů, které jsou definovány shodně jak v článku 2016/679/EU, tak v článku 2016/680/EU jako *osobní údaje vyplývající z konkrétního technického zpracování, týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje*. V obou případech jsou také biometrické údaje považovány za zvláštní kategorii osobních údajů, jejichž zpracování je zakázáno, pokud neexistuje výjimka, která se na zpracování vztahuje. Výjimky jsou stanoveny v čl. 9 odst. 2, pokud jde o obecné nařízení[13], a v čl. 10 pokud jde o trestněprávní směrnici. Jak již bylo uvedeno výše, je úkolem správce, aby před zahájením zpracování pečlivě posoudil, v jakém režimu dojde ke zpracování osobních údajů, za jakým účelem a na základě jakého právního důvodu. Poté aplikuje i další zásady zpracování osobních údajů.

Pokud by se jednalo o kontext trestněprávní směrnice, základní rámec stanoví článek 3 odst. 13 směrnice 2016/680/EU, který definuje pojem biometrický údaj, článek 4 zásady vztahující se ke zpracování osobních údajů, článek 8 zákonnost zpracování, článek 10 zpracování zvláštních kategorií osobních údajů a možné výjimky a článek 11 automatizované individuální posuzování. Obdobně obecné nařízení o ochraně osobních údajů upravuje v článku 4 odst. 14 pojem biometrický údaj, v článku 5 a 6 zásady zpracování, v článku 9 zvláštní kategorie osobních údajů a možné výjimky.

K interpretaci a aplikaci obtížných otázek ochrany osobních údajů přijímá Sbor pro ochranu osobních údajů (*European Data Protection Board*, EDPB), který je tvořený zástupci dozorových úřadů členských zemí, doporučení obvykle označované jako pokyny či stanoviska (*guidelines*, *opinions*). Ačkoli tyto dokumenty nejsou právně závazné, pro praxi mohou být velmi užitečné; jejich cílem je poskytnout pomoc správcům, zpracovatelům či subjektům údajům. Konkrétně ve vztahu k problematice biometrických údajů se z poslední doby uplatní zejména pokyny 5/2022 o použití technologie *facial recognition* v oblasti prosazování práva z 12. 5. 2022, které byly aktualizovány

[13] Článek 9 Zpracování zvláštních kategorií osobních údajů v odstavci 1 zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Odstavec 2 stanoví výjimky, kdy se odstavec 1 nepoužije. Například odstavec 2 písm. g) jako výjimku uvádí zpracování e nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektů údajů.

26. 4. 2023[14]. Byť se tyto pokyny vztahují specificky na zpracování *facial recognition*, z velké části se uplatní i ve vztahu k biometrickým údajům obecně, jak to uvádí i samotné pokyny.

Výše uvedené pokyny 5/2022 obsahují definici technologie *facial recognition*, upřesňují přehled požadavků trestněprávní směrnice, charakter základního práva a způsob jeho limitace, požadavky vztahující se k právnímu základu, aplikaci požadavku nezbytnosti a proporcionality, způsob plnění informační povinnosti, uplatňování práv subjektů údajů, logování, posouzení vlivu a další otázky. Pokyny jsou v řadě otázek velmi konkrétní, takže správce údajů s jejich pomocí může vyřešit řadu sporných či obtížných otázek. Zvlášť je třeba upozornit na to, že pokyny věnují pozornost otázce posouzení vlivu[15], jehož vypracování je v případě zpracování biometrických údajů zpravidla povinné.

Institut posouzení vlivu na ochranu osobních údajů (*Data Protection Impact Assessment*, DPIA) je před použitím technologie *facial recognition* povinným požadavkem zejména při použití nových technologií, neboť s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování je pravděpodobné, že povede k vysokému riziku pro práva a svobody fyzických osob, které jsou předmětem zpracování[16]. Nadto používání technologie *facial recognition* obvykle zahrnuje systematické automatizované zpracování zvláštních kategorií údajů, které rovněž vyžaduje zvážení posouzení vlivu na ochranu osobních údajů. Posouzení by mělo obsahovat alespoň obecný popis plánovaného zpracování operací, posouzení jejich nezbytnosti a přiměřenosti ve vztahu ke konkrétnímu účelu či účelům zpracování, posouzení rizik pro práva a svobody subjektů údajů, opatření, která by měla být přijata za účelem zajištění souladu se zákonem, předpokládaná opatření k řešení rizik, záruky, bezpečnostní opatření a mechanismy k zajištění ochrany osobních údajů a jejich ochrany. Bližší informace k posouzení vlivu lze nalézt v pokynech WP 29 o posouzení vlivu na ochranu osobních údajů[17]. Zpracování posouzení vlivu správci významně pomůže při nastavení a dokumentaci procesů ochrany osobních údajů jak pro účely vnitřních procesů v jeho organizaci, tak ve vztahu k dozorovému úřadu a subjektům údajů.

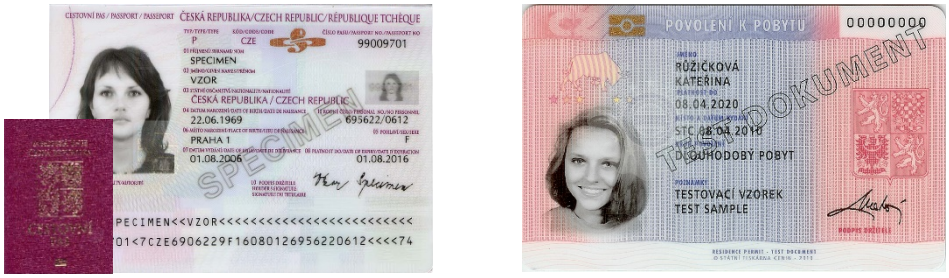
[14] *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*
[15] Článek 35 GDPR, případně článek 27 trestněprávní směrnice.
[16] Článek 35 odst. 1, 2 a 3 GDPR
[17] Pokyny pracovní skupiny *Article 29 Working Party* (WP 248 rev.01) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* ze dne 4. 4. 2017, revidované 4. 10. 2017; pracovní skupina WP 29 předcházela Sbor pro ochranu osobních údajů.

4 BIOMETRICKÉ IDENTIFIKAČNÍ DOKLADY

V této kapitole jsou uvedena základní fakta k biometrickým identifikačním dokladům. Většina těchto podkladů pochází ze zdroje Státní tiskárny cenin[18] a dalších zdrojů, zejména ICAO.

4.1 Struktura biometrického dokladu

V České republice jsou v současnosti vydávány tři typy elektronických biometrických dokladů: (a) *cestovní doklady*, (b) *občanské průkazy* (od srpna 2021 s bezkontaktním čipem, obsahujícím ICAO aplikaci) a (c) *povolení k pobytu* pro příslušníky cizích zemí (dále jen PkP).



Obrázek 4.1: Vzory cestovního pasu a povolení k pobytu v ČR (zdroj STC).

Elektronický biometrický doklad je takový doklad, který je vybaven elektronickým nosičem biometrických dat, na kterém jsou, kromě jiných údajů, uložena vlastní biometrická data. V případě cestovních dokladů a PkP je nosičem biometrických dat bezkontaktní elektronický čip (dále jen čip). U českých cestovních dokladů a PkP je čip umístěn spolu s vinutou měděnou anténou uvnitř polykarbonátové datové stránky dokladu. U dokladů vydávaných v České republice jsou do čipu ukládány dva biometrické údaje, obraz obličeje a otisky prstů držitele dokladu.

Výroba cestovních dokladů a PkP se řídí mezinárodními legislativními, technickými a bezpečnostními standardy, které předepisují způsob, jakým mají být doklady vyráběny a definují požadavky na ukládání elektronických dat (včetně biometrických) do čipu a způsob jejich zabezpečení proti neoprávněnému přístupu. Mezi základní dokumenty patří např.:

- Nařízení rady č. 2252/2004, o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy;
- Rozhodnutí Komise K(2006) 2909, kterým se stanoví technické specifikace norem pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy;
- Nařízení Rady (ES) č. 1030/2002, kterým se stanoví jednotný vzor povolení pro státní příslušníky třetích zemí, ve znění nařízení Rady (ES) č. 380/2008;

[18] https://stc.cz/

- Rozhodnutí Komise K(2009) 3770, kterým se upravují technické specifikace pro jednotný vzor povolení k pobytu pro státní příslušníky třetích zemí;
- ICAO dokument 9303, část 1, strojově čitelné cestovní pasy s biometrickými prvky, 6. vydání, 2006;
- ICAO dokument 9303, část 3, strojově čitelné úřední cestovní doklady velikosti ID1 a ID2, 3. vydání, 2008;
- ICAO TR – Doplňkové řízení přístupu (SAC) pro strojově čitelné doklady, verze 1.01;
- Common Criteria, verze 3.1 – soubor bezpečnostních požadavků na bezpečnostní funkce IT systémů, výchozí dokument pro bezpečnostní certifikaci biometrických dokladů;
- Evropská certifikační politika EUCP 2.0 pro infrastrukturu rozšířeného přístupu pro pasy a cestovní dokumenty vydávané členskými státy.

Za vydávání biometrických dokladů jsou v ČR odpovědné Ministerstvo vnitra ČR (vydává cestovní doklady, cizinecký cestovní doklad, uprchlický cestovní doklad a PkP) a Ministerstvo zahraničních věcí ČR (vydává diplomatický a služební cestovní doklad).

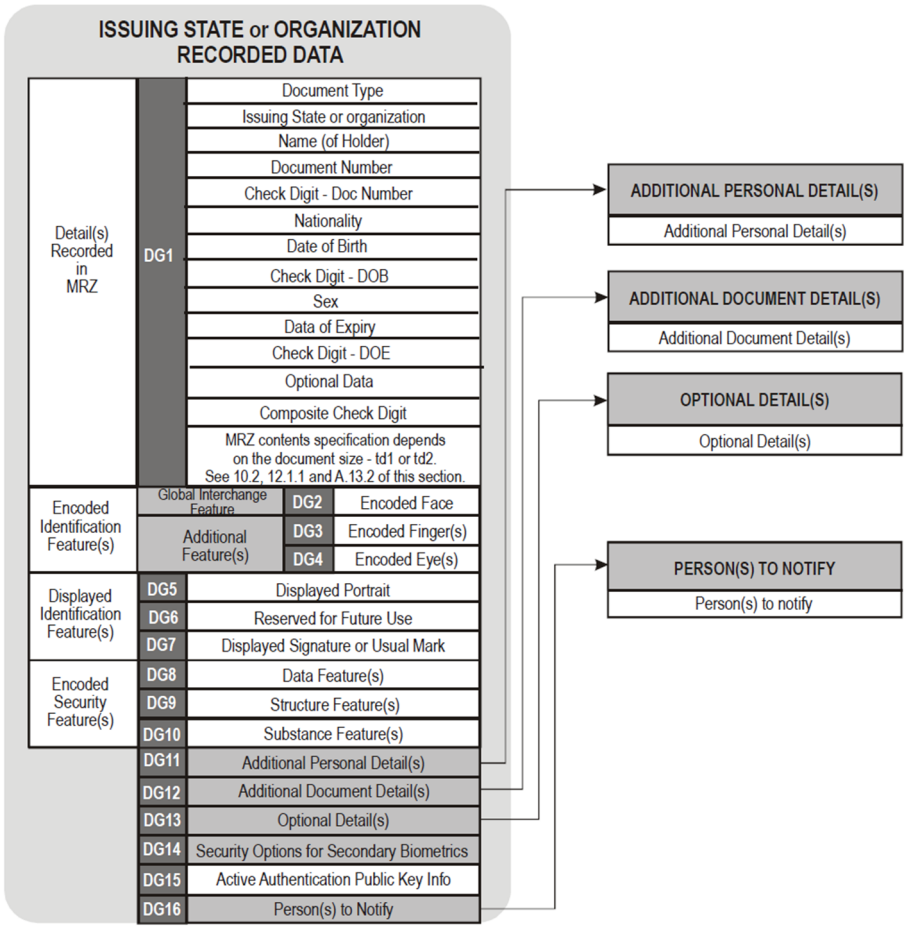
Struktura dat ukládaných do čipu je popsána v dokumentu ICAO 9303. Cílem je zajistit jednotný způsob ukládání a zabezpečení dat v čipu tak, aby byla zajištěna mezinárodní interoperabilita biometrických cestovních dokladů.

V čipu jsou data uložena a zabezpečena ve speciální aplikaci, tzv. *ICAO aplikaci*. Tato aplikace je společná pro cestovní doklady i PkP. Data jsou v čipu uložena strukturovaně, v tzv. logické datové struktuře (LDS). LDS verze 1.7 je rozdělena do šestnácti datových skupin a je definována dle obrázku 4.2.

Data uložená v LDS můžeme rozdělit do tří hlavních kategorií. První kategorií jsou data s požadavkem na nízké zabezpečení. Jedná se o data, která jsou vizuálně zobrazena přímo na datové stránce, jako např. jméno a příjmení držitele dokladu, datum narození, apod. Tato data jsou v čipu uložena v datové skupině DG1. Do této kategorie ovšem patří i první biometrický prvek, obraz obličeje držitele dokladu, který je uložen v datové skupině DG2. Na zabezpečení těchto dat v čipu nejsou kladeny vysoké požadavky, pro jejich ochranu se využívá tzv. základního řízení přístupu – BAC (*Basic Access Control*). Od 1. 1. 2015, se v souladu s rozhodnutím Komise K(2011) 5478 resp. K(2011) 5499, zavádí pro ochranu dat první kategorie mechanismus tzv. doplňkového řízení přístupu – SAC (*Supplemental Access Control*).

Do druhé kategorie patří data s požadavkem na vysoké zabezpečení a jedná se o otisky prstů držitele dokladu. Otisky prstů jsou uloženy v datové skupině DG3 a jsou zabezpečeny tzv. rozšířeným řízením přístupu – EAC (*Extended Access Control*). Do této kategorie patří technicky také obraz oční duhovky, v LDS je pro tato data vyhrazena datová skupina DG4, v českých dokladech se však prozatím nepoužívá.

Třetí kategorií dat ukládaných do čipu jsou tzv. „provozní“ data. Jedná se o různé elektronické klíče, certifikáty, kontrolní a ověřovací data, která tvoří kostru zabezpečení přístupu k datům na čipu.



Obrázek 4.2: Datová struktura čipu biometrického identifikačního dokladu (zdroj STC).

Všechna data uložená v čipu jsou, kromě výše zmíněných mechanismů uvedených v předchozí kapitole, chráněna ještě některými dalšími kryptografickými mechanismy a algoritmy. Pro úplnost uvedeme stručný přehled všech základních kryptografických algoritmů a mechanismů použitých v českých biometrických dokladech:

- PA – Pasivní autentizace, ochrana integrity dat v čipu;
- AA – Aktivní autentizace, ochrana čipu proti kopírování;
- BAC – Základní řízení přístupu, ochrana přístupu k datům první kategorie;
- SAC (od 1. 1. 2015) – Doplňkové řízení přístupu, ochrana přístupu k datům první kategorie;
- EAC – Rozšířené řízení přístupu, ochrana přístupu k datům druhé kategorie, sestává z mechanismů TA (*Terminálová Autentizace*) a CA (*Čipová Autentizace*).

Čip s využitím uvedených mechanismů chrání data, která jsou na něm uložená před neoprávněným čtením. Sám rozhoduje o tom, komu a jaká data poskytne. Čip od systémů, které žádají o přístup k datům, nazývejme je *inspekčními systémy*, žádá poskytnutí důkazu o oprávnění inspekčního systému k datům přistupovat. Pokud se inspekčnímu systému nepodaří prokázat své oprávnění ke čtení dat, čip nebude ochoten data poskytnout a odmítne inspekčnímu systému spolupráci. Důležitým pojmem je rovněž infrastruktura veřejných klíčů (PKI – *Public Key Infrastructure*), jejíž popis však již přesahuje rámec a rozsah tohoto dokumentu.

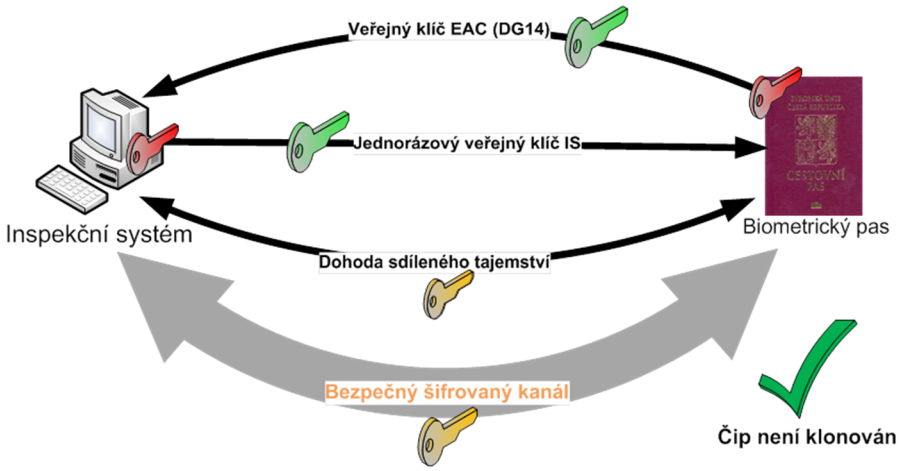
4.2 Způsob práce s biometrickým dokladem

Uživatel cestovního dokladu nebo PkP musí nejprve přiložit doklad ke čtecímu zařízení. Při čtení dat z čipu inspekčním systémem je nejprve opticky přečtena strojově čitelná zóna dokladu (MRZ), ze které jsou odvozeny symetrické klíče pro BAC. Posléze je proveden mechanizmus BAC a z dokladu je možné přečíst údaje první kategorie – osobní údaje a fotografii obličeje.

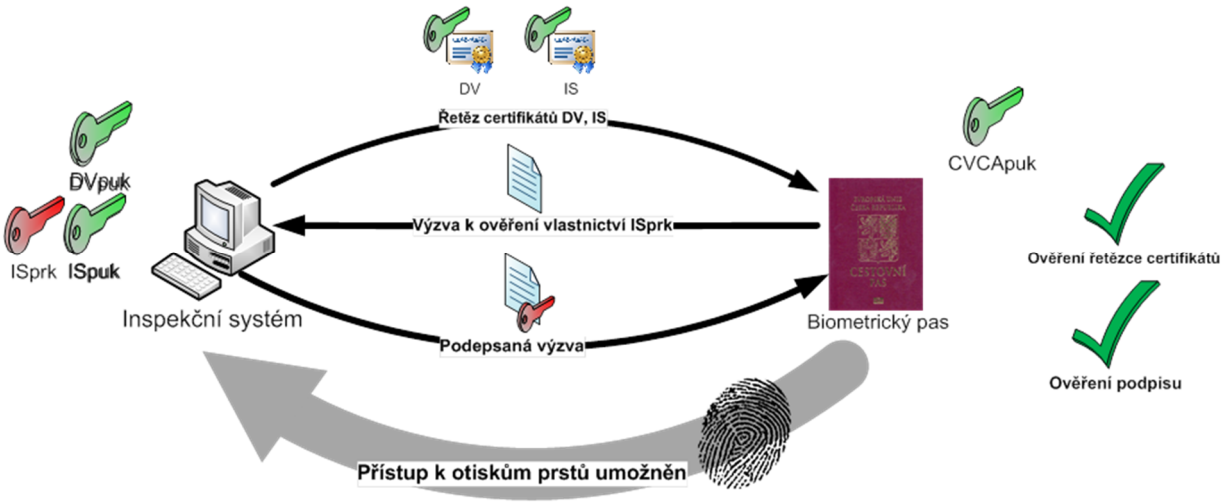
V případě, že čip i inspekční systém podporují algoritmus SAC, není algoritmus BAC v tomto případě realizován, a je použit rovnou silnější mechanismus SAC.

Dále následuje provedení mechanismu EAC, a to v pořadí nejprve čipová autentizace a posléze terminálová autentizace. Procesy při realizaci CA a TA jsou znázorněny na následujících schematických procesních diagramech – viz obrázky 4.3 a 4.4.

Po úspěšném provedení EAC získává inspekční systém přístup k otiskům prstů a veškerá komunikace mezi čipem a inspekčním systémem probíhá bezpečným šifrovaným kanálem.



Obrázek 4.3: Čipová autentizace (zdroj STC).



Obrázek 4.3: Terminálová autentizace (zdroj STC).

5 POPIS ZAŘÍZENÍ TBS 3D FLOW

V rámci výše zmíněného projektu se zkratkou BEFFIC bylo vytvořeno zařízení s obchodním názvem 3D FLOW, u nějž existuje jak stacionární, tak i mobilní verze, pokrývající přesně portfolio potřeb popsaných v podkapitole 2.2. V následujících podkapitolách jsou uvedeny základní údaje, které se zčásti opírají o udělený užitný vzor [07], který je nyní rozšiřován na mezinárodní patent.

5.1 Hardware

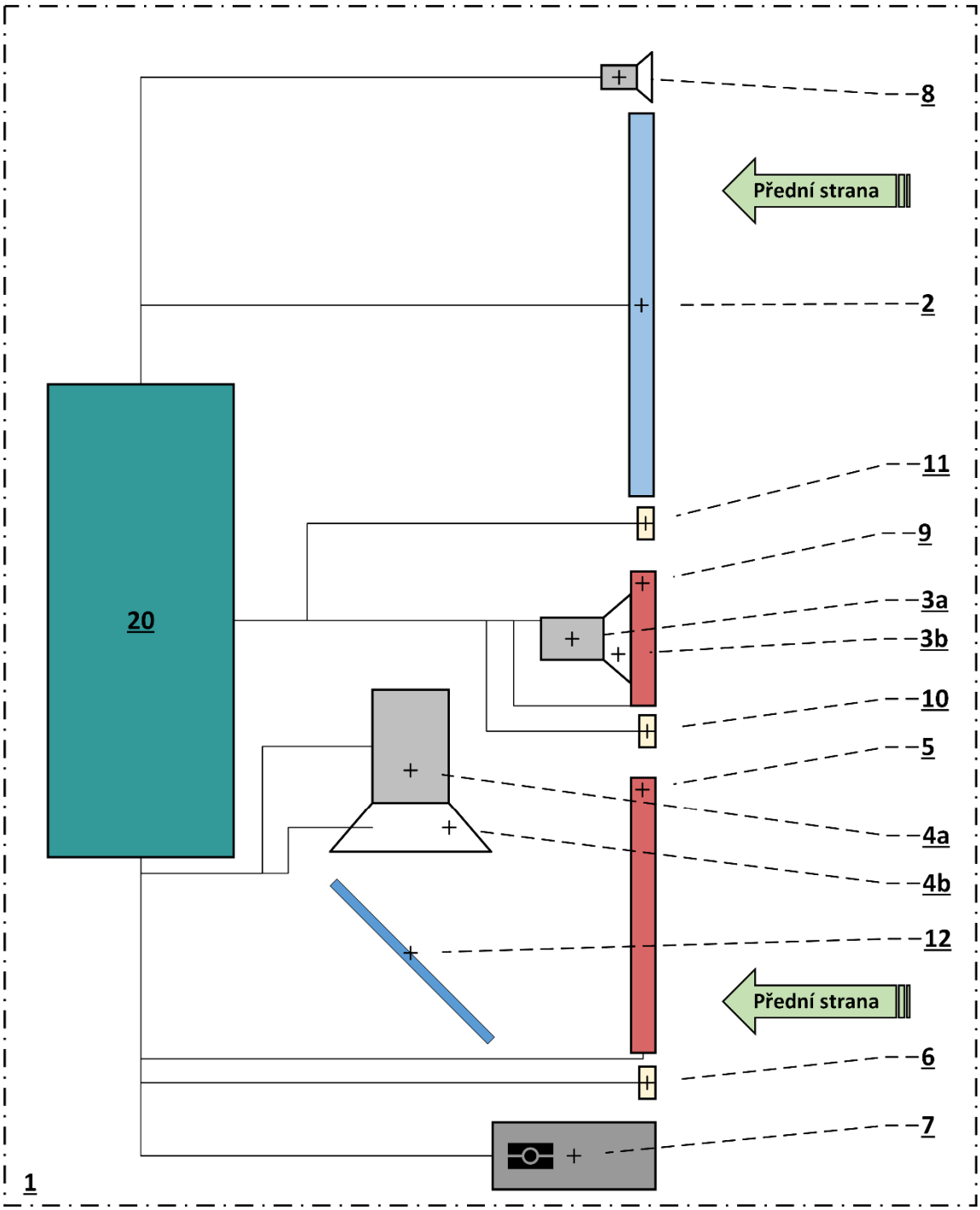
Finální verze stacionárního zařízení 3D FLOW je zobrazena na obrázku 5.1. Zde je patrný kovový housing, na čelní straně je vidět dotykový displej, osvětlovací modul (modrá barva) s otvorem pro zrcadlo a kamerovou jednotku (uvnitř zařízení), přičemž v mezilehlém prostoru mezi displejem a osvětlovacím modulem je umístěna zabudovaná kamera na snímání obličeje ve 2D.

Obrázek 5.1: Jednotka 3D FLOW.

Příkladné provedení zařízení 1 (3D FLOW) zobrazené na obrázku 5.2 zahrnuje řídicí jednotku 20, která je určena k přijímání a zpracovávání biometrických údajů uživatelů a k řízení níže uvedených připojených komponent.

Dále toto biometrické zařízení 1 (3D FLOW) zahrnuje první kamerovou jednotku 4, která obsahuje první obrazový snímač 4a a první čočku 4b. Kamerová jednotka 4 je přednostně umístěna ve spodní části zařízení pod displejem 2. První čočka 4b je přednostně tekutá čočka, ale může se jednat i o čočku pevnou, resp. čočku s motorickým typem přeostřování.

Dále je biometrické zařízení 1 (3D FLOW) opatřeno prvním senzorem 6 přiblížení, který je určen pro zjištění vzdálenosti dlaně uživatele od první kamerové jednotky 4 a pro předání změřené vzdálenosti řídicí jednotce 20. Na základě této vzdálenosti je tak první kamerové jednotce 4, resp. první čočce 4b, vydán signál, na jehož základě dojde k automatickému zaostření na dlaň, resp. prsty uživatele a pořízení snímku alespoň jednoho prstu.



Obrázek 5.2: Schematické složení zařízení 3D FLOW.

První senzor 6 přiblížení a první kamerová jednotka 4, resp. první čočka 4b, jsou v tomto provedení s výhodou umístěny v jedné rovině tak, aby změřená vzdálenost byla skutečnou vzdáleností ruky od první čočky 4b.

V blízkosti první kamerové jednotky 4 je navíc umístěna první osvětlovací jednotka 5, např. v podobě soustavy bodových světel, rozmístěných v kruhu se vzájemným úhlovým rozestupem okolo první čočky 4b, přičemž uvedená první osvětlovací jednotka 5 je určena pro osvětlení ruky uživatele tak, aby mohl být pořízen dostatečně světlý a zřetelný snímek, případně sada snímků s různou hloubkou ostrosti.

Při používání biometrického zařízení 1 (3D FLOW) může být výhodné, když se uživateli dá pokyn, aby nejprve ukázal na první kamerovou jednotku 4 svou otevřenou dlaň přibližně kolmo na optickou osu první kamerové jednotky 4, přičemž se získá první snímek, případně první sada snímků s různou hloubkou ostrosti, a aby následně dlaní otáčel kolem osy odpovídající distálnímu směru dlaně, tedy v podstatě kolem osy nataženého prostředníčku, na jednu stranu, přičemž se získá druhý snímek, případně druhá sada snímků s různou hloubkou ostrosti, a druhou stranu, přičemž se získá třetí snímek, případně třetí sada snímků s různou hloubkou ostrosti.

Popisované první provedení obsahuje i druhou kamerovou jednotku 3, která zahrnuje druhý obrazový snímač 3a a druhou čočku 3b. Druhá čočka 3b je přednostně tekutá čočka obdobně jako první čočka 4b, avšak může se jednat i o pevnou čočku, resp. čočku s motorickým typem přeostřování. Konstrukce druhé kamerové jednotky 3 je tedy analogická konstrukci první kamerové jednotky 4.

Dále je biometrické zařízení 1 (3D FLOW) opatřeno druhým senzorem 10 přiblížení, který je určen pro zjištění vzdálenosti obličeje uživatele od druhé kamerové jednotky 3 a pro předání změřené vzdálenosti řídicí jednotce 20. Na základě této vzdálenosti je tak druhé kamerové jednotce 3, resp. druhé čočce 3b, vydán signál, na jehož základě dojde k automatickému zaostření na obličej a pořízení snímku obličeje.

Druhý senzor 10 přiblížení a druhá kamerová jednotka 3, resp. druhá čočka 3b, jsou v tomto provedení opět s výhodou umístěny v jedné rovině.

Druhá kamerová jednotka 3 je určena pro obličejovou identifikaci/verifikaci, a proto je umístěna výše než první kamerová jednotka 4, např. mezi první kamerovou jednotkou 4 a displejem 2.

Okolo druhé kamerové jednotky 3 pak může být umístěna druhá osvětlovací jednotka 9, např. v podobě soustavy bodových světel, rozmístěných v kruhu se vzájemným úhlovým rozestupem okolo druhé čočky 3b.

Druhá kamerová jednotka 3 s příslušným druhým senzorem 10 přiblížení a druhou osvětlovací jednotkou 9 je volitelná a nemusí být nutně součástí biometrického zařízení 1.

První provedení dále zahrnuje i čtečku 7 biometrických identifikačních dokladů, zejména radiofrekvenčních údajů z čipu na dokladu. Za tímto účelem čtečka 7 biometrických identifikačních dokladů zahrnuje RFID/NFC čtečku. Pro snímání MRZ dokladu je určena první kamerová jednotka 4. Čtečka 7 biometrických identifikačních dokladů je volitelná a nemusí být nutně součástí biometrického zařízení 1.

Výše zmíněný displej 2 může být buď dotykový nebo bezdotykový. Pokud je displej 2 bezdotykový, zahrnuje zařízení 1 navíc sestavu 11 doplňkových senzorů přiblížení. Sestava 11 doplňkových senzorů přiblížení pak slouží pro zajištění detekce přítomnosti prstu ve specifickém prostoru před displejem 2, přičemž umožňuje kontrolu displeje 2 ze vzdálenosti několika centimetrů až nižší desítky centimetrů.

Dále první příkladné provedení biometrického zařízení 1 zahrnuje 3D kameru 8, s výhodou uspořádanou ve vrchní části zařízení 1, jejímž účelem je přesné polohování ruky pro zachycení otisku prstu a/nebo obličeje pro obličejovou identifikaci/verifikaci, včetně detekce vhodné polohy a vzdálenosti. 3D kamera také může být s výhodou využita pro biometrické rozpoznání ve 3D, zejména obličeje/hlavy a prostorové geometrie ruky. 3D kamera 8 je volitelná a nemusí být nutně součástí zařízení 1.

Jednotlivé součásti biometrického zařízení 1, konkrétně 3D kamera 8, displej 2, senzory 6, 10 přiblížení, sestava 11 doplňkových senzorů přiblížení, osvětlovací jednotky 5, 9, obrazové snímače 3a, 4a a čočky 3b, 4b kamerových jednotek 3, 4 jsou přímo nebo nepřímo signálově propojeny s řídicí jednotkou 20.

Výsledek identifikace/verifikace je zobrazen na displeji 2, tj. např. při úspěšné identifikaci se zobrazí identita, zatímco v opačném případě se zobrazí informace o neúspěšné identifikaci. Výsledek je také zařízením 1 odeslán přes API, například pro otevření brány.

Pro druhou kamerovou jednotku 3 probíhá postup analogicky, přičemž je pořízen i snímek obličeje, za současného osvětlení druhou osvětlovací jednotkou 9, a tedy je v řídicí jednotce 20 provedeno vyhodnocení dvou biometrických údajů – obrazů otisku prstu a obličeje.

Pokud je zařízení 1 opatřeno i čtečkou 7 biometrických identifikačních dokladů, uživatel umístí biometrický identifikační doklad před první kamerovou jednotku 4, podobně jako ruku. První kamerová jednotka 4 poté pořídí snímek přední strany na biometrickém identifikačním dokladu. Z tohoto snímku je rozpoznána za pomocí optického rozpoznávání znaků strojově čitelná oblast, která obsahuje klíč k veřejně přístupným údajům v čipu (tj. osobní data uživatele a snímek obličeje).

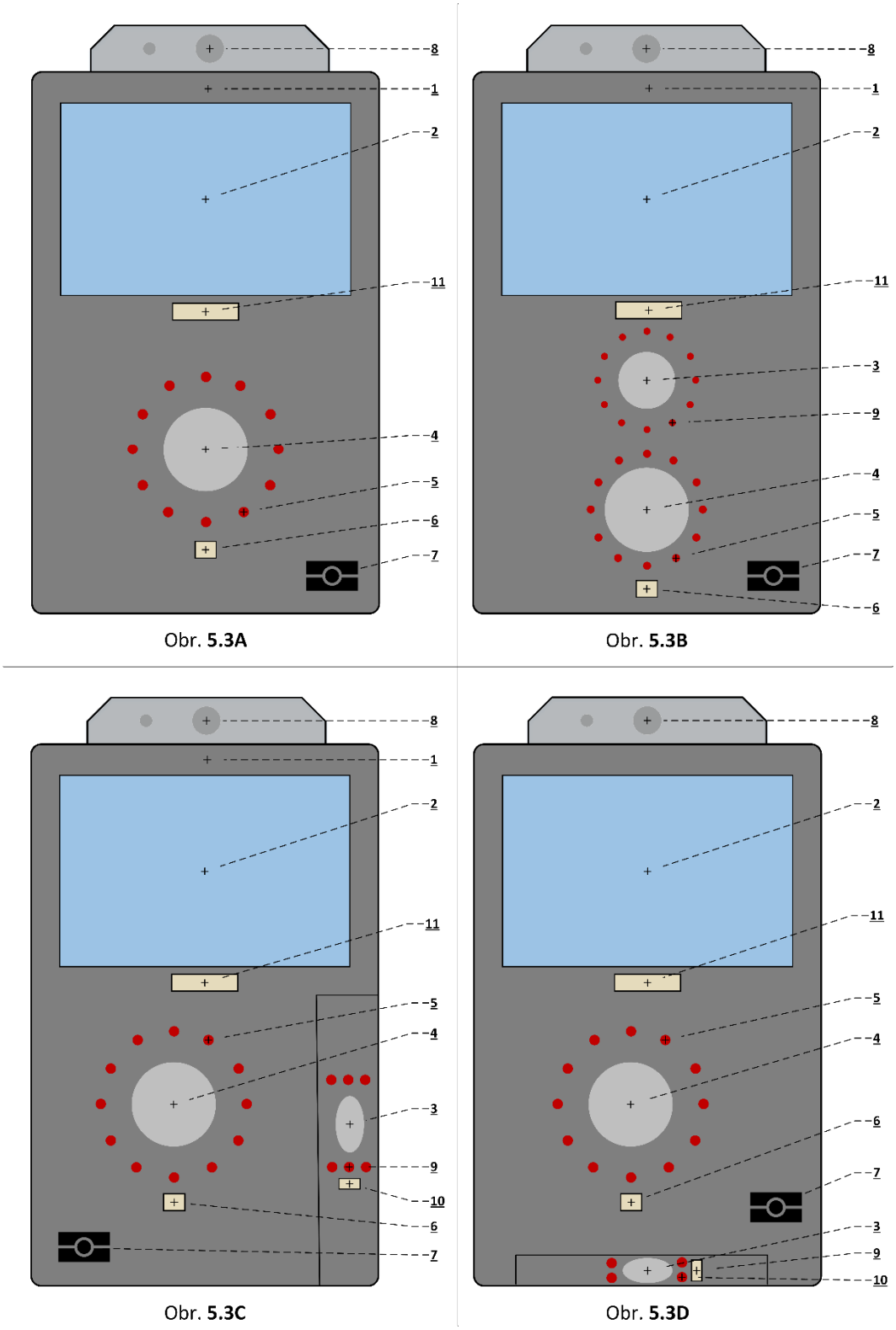
Následně uživatel doklad přiloží ke čtečce 7 dokumentů, vybavené RFID/NFC čtečkou, která přečtené údaje odešle do řídicí jednotky 20, která srovná tyto údaje z biometrického identifikačního dokladu s biometrickými údaji zjištěnými ze snímků pořízených výše uvedeným způsobem.

Pokud je zařízení 1 opatřeno 3D kamerou 8, uvedená 3D kamera 8 vytváří trojrozměrný obraz obličeje uživatele a/nebo jeho ruky, přičemž tento obraz je následně odeslán do řídicí jednotky 20. Řídicí jednotka 20 tak obdobně jako u snímků, pořízených první kamerovou jednotkou 4 a/nebo druhou kamerovou jednotkou 3, provede vyhodnocení snímku, tj. identifikaci/verifikaci uživatele.

Bezkontaktní multimodální biometrické zařízení v souladu s předkládaným technickým řešením může využívat multispektrální princip detekce prezentačních útoků na otisky prstů s využitím osvětlení dlaně/prstu různými vlnovými délkami od ultrafialového spektra přes viditelné záření až po infračervené spektrum, nebo snímáním krevního řečiště, viditelného v infračerveném spektru.

Obrázky 5.3A až 5.3D znázorňují různé příklady konfigurace jednotlivých součástí na zařízení, které se liší přítomností, případně umístěním druhé kamerové jednotky 3. Varianta z obrázku 5.3A neobsahuje druhou kamerovou jednotku 3 – v této variantě se tedy nepočítá s obličejovou identifikací/verifikací. Obrázek 5.3B znázorňuje čelní pohled na zařízení podle schématu na obrázku 5.2. Varianta znázorněná na obrázku 5.3C vychází z varianty z obrázku 5.3B s tím rozdílem, že druhá kamerová jednotka 3 není umístěna nad první kamerovou jednotkou 4, ale vedle ní. Varianta z obrázku 5.3D rovněž vychází z varianty z obrázku 5.3B s tím rozdílem, že druhá kamerová jednotka 4 není umístěna nad první kamerovou jednotkou 4, ale pod ní. Ve variantě znázorněné na obrázku 5.3D je tak první kamerová jednotka 4 určena pro obličejovou identifikaci, zatímco druhá kamerová jednotka 3 je určena pro snímání otisků prstů a směřuje směrem k zemi.

První obrazový snímač 4a a/nebo druhý obrazový snímač 3a jsou přednostně typu CCD nebo CMOS.



Obrázek 5.3: Konfigurační možnosti zařízení 3D FLOW.

Základní deska v zařízení má tyto parametry:

- procesor: NXP® i.MX 8M Plus, 1.6 GHz
- paměť: 4 GB
- rozhraní vnitřní: audio, tamper switch, proxboard, RFID, 5×USB, SD karta, micro-HDMI, $MIPI_{DSI}$, $MIPI_{CSI}$
- rozhraní vnější: Gigabit ethernet s PoE, 2×USB 3, relé, RS485, RS232, 2×GP_{Out}, 2×GP_{In}, Wiegand out, Power in

Jak již bylo zmíněno dříve, zařízení obsahuje kamerové jednotky, jejichž specifikace překračuje rámec tohoto dokumentu, navíc, jelikož se jedná o vlastní kamerovou jednotku, je součástí ochrany obchodního tajemství. Každopádně rozlišení dosahuje minimálně HD, a to jak kamera na otisky prstů, tak i na obličej.

Stacionární verze se od mobilní odlišuje především v integrované baterii a lehce odlehčeném korpusu.

5.2 Software

Uvnitř zařízení běží standardní engine TBS, který slouží k propojení veškerých hardwarových komponent, umožňuje připojení a využití externích knihoven (zejména od společnosti Innovatrics[19]) a zobrazení výsledků, resp. interakci s uživateli. Samozřejmostí je integrace interní databáze a možnost využití cloudových služeb.

Pro biometrická rozpoznání (obličej a otisky prstů) je využito knihoven společnosti Innovatrics. Fotografie obličeje, která je uložena v biometrickém identifikačním dokladu, je velmi podobná obličeji, který nasnímá kamera zařízení 3D FLOW, takže není třeba provádět žádné úpravy.

U otisků prstů je však situace odlišná. Otisk prstu, který je uložen v biometrickém identifikačním dokladu, je obvykle nasnímán kontaktním způsobem. Kromě deformace kůže, která je způsobena stykem kůže s podložkou, je navíc i odlišné šedotónové rozložení samotného otisku prstu. Kvůli tomu je třeba provést úpravu námi nasnímaného otisku prstu, aby byl co nejpodobnější barevným rozložením a reprezentací papilárních linií standardnímu typu otisku prstu, který je definován ICAO, příp. kvalitou dle NIST IR 7151, resp. nejnovější metodikou testování kvality otisků prstů NFIQ. V těchto úpravách se maximálně vyhýbáme strojovému učení, neboť to může libovolně modifikovat i strukturu běhu papilárních linií, čímž mohou vzniknout nové vzory (a markanty), které mohou snížit podobnost sounáležících otisků prstů, a naopak zvýšit podobnost odlišných otisků prstů. V tomto případě si tedy zakládáme na klasických metodách zpracování obrazu.

Nicméně k detekci samotných prstů, neboť kamera nasnímá horní palmární část ruky, kde se nachází 1 a více prstů (dle skrčených prstů či absentujících), využíváme strojového učení, protože to funguje skvěle, nehledě na změnu pozadí, příp. osvětlení.

Zabudovaná detekce prezentačního útoku je založena na strojovém učení, avšak samotná funkčnost je obchodním tajemstvím společnosti, proto zde není dále rozebrána.

[19] https://www.innovatrics.com/

Každopádně zde odlišujme detekci prezentačního útoku obličeje, kde využíváme poskytnutou funkcionalitu PAD přímo externím dodavatelem, společností Innovatrics. U otisků prstů je to naše vlastní řešení, orientované na bezkontaktní snímání.

Softwarové řešení samozřejmě chrání biometrické reference (šablony) proti manipulaci a neoprávněnému vyčtení. Zařízení 3D FLOW je tedy konformní s požadavky ochrany osobních údajů v biometrickém zařízení.

5.3 Příklady použití

Jak již bylo zmíněno výše, jelikož existují dvě verze zařízení 3D FLOW, a to stacionární a mobilní, u obou verzí se nachází dva režimy přísný („*strict*") a volnější („*relaxed*").

U **stacionární verze** se jedná především o využití pro docházkové systémy, řízení přístupu a/nebo vstupu. Instalace je vhodná od běžných objektů až po kritické infrastruktury. Správná výška montáže zařízení je odvislá od průměrné výšky osob v okruhu uživatelů. Je doporučeno zařízení namontovat v nižší výšce, neboť i vyšší uživatel se může lehce zohnout a prezentovat svoje otisky prstů a obličej, zatímco člověk nízkého vzrůstu bude mít problémy se snímáním obličeje, neboť povyskočení nebude časově dostatečné na kvalitní nasnímání obličeje. Důležitým faktem je, že v okamžiku, kdy se objeví požadavek na využití biometrických identifikačních dokladů, je třeba, aby mělo zařízení přidělen platný certifikát nadřazenou certifikační autoritou, tudíž mělo přístup do oblasti DG3, kde je uložen otisk prstu. Bez tohoto certifikátu je možné vyčíst z čipu pouze oblasti DG1 a DG2 (obličej). Je očekávatelné, že pro plně civilní využití bude obtížné takový certifikát získat (viz následující odstavec).

U **mobilní verze** se jedná zejména o využití policií, armádou a celní správou k ověření identity jedince. V takovém případě si již daná organizace zajistí pro dané zařízení nadřazený certifikát, aby zařízení mohlo vyčítat z čipu i jiné bloky, než pouze DG1 a DG2. Využití pro civilní účely v tomto případě nedává příliš smysl.

Přísný režim („*strict*") odpovídá modelové situaci popsané v kapitole 3.1 na ochranu KI. Jedná se o režim s přísněji nastavenými prahy přijetí (jak pro obličej, tak pro otisky prstů). Cílem je tedy vyšší přesnost za cenu nižšího uživatelského komfortu. Aktivace režimu je zřejmá z červeného tónu pozadí na displeji zařízení v klidovém režimu. Naopak **volnější režim** („*relaxed*") odpovídá modelové situaci přeshraniční kontroly. Prahy jsou nastaveny o cca 10 % nižší. Tím se dosáhne vyšší a rychlejší propustnost zařízením (tedy zvýšení uživatelské přívětivosti), ale za cenu snížení přesnosti. Tento režim je rozpoznatelný modrým tónem pozadí v klidovém režimu. Operátor podle typu využití vidí, zda je zařízení nastaveno ve správném režimu.

6 ZÁVĚR

V této metodice jsou rozebrány oblasti kritických infrastruktur, základní funkčnost biometrických systémů a doporučení týkající se volby biometrické charakteristiky. Následuje ověřování výkonnosti biometrických systémů a k tomu přidružená legislativa a ochrana osobních (biometrických) údajů. Dále jsou v základu popsány biometrické identifikační doklady. Na závěr je uveden popis námi (v rámci projektu BEFFIC) zkonstruovaného zařízení 3D FLOW, a to včetně rozpadu na stacionární a mobilní verzi zařízení.

7 POUŽITÉ ZKRATKY

AA	aktivní autentizace (*Active Authentization*)
ANSI	americký národní standardizační institut (*American National Standards Institute*)
API	rozhraní pro programování aplikací (*Application Programming Interface*)
BAC	základní řízení přístupu (*Basic Access Control*)
BEFFIC	Multimodální biometrické zařízení pro ověření identity osob na základě otisků prstů a obličeje při překračování státních hranic (*Multimodal **bi**ometric d**e**vice for veri**f**ying the identity of persons on the basis of **f**ingerpr**i**nts and fa**c**es when crossing state borders*)
CA	čipová autentizace (*chip authentization*)
CCD	zařízení s vázanými náboji (typ kamery – *Charge-Coupled Device*)
CE	certifikát shody (*Certification of Conformity*)
CMOS	doplňkový polovodič na bázi kovu a oxidu (*Complementary Metal-Oxid Semiconductor*)
ČR	Česká Republika
ČSN	česká technická norma
DET	vyrovnání chyb detekce (*Detection Trade-off*)
DG	datová skupina (*Data Group*)
DPIA	posouzení vlivu na ochranu osobních údajů (*Data Protection Impact Assessment*)
EAC	rozšířené řízení přístupu (*Extended Access Control*)
EC	Evropská komise (*European Commission*)
EDPB	Evropský sbor pro ochranu osobních údajů (*European Data Protection Board*)
EER	míra vyrovnání chyb (*Equal Error Rate*)
EU	Evropská unie
EUCP	evropská certifikační politika (*European Union Common Policies*)
FAR	míra chybného přijetí (*False Accept Rate*)
FIDO	rychlá identita on-line (*Fast Identity Online*)
FMR	míra chybné shody (*False Match Rate*)
FNMR	míra chybné neshody (*False Non-Match Rate*)
FRR	míra chybného odmítnutí (*False Reject Rate*)
FTA	míra selhání snímání (*Fail To Acquire*)
FTC	míra selhání snímání (*Fail To Capture*)
FTE	míra selhání registrace (*Fail To Enroll*)
FTX	míra selhání registrace (*Fail To eXtract*)

GAR	míra oprávněného přijetí (*Genuine Acceptance Rate*)
GDPR	Obecné nařízení o ochraně osobních údajů (*General Data Protection Regulation*)
HD	video s vysokým rozlišením (*High Definition*)
HDMI	multimediální rozhraní s vysokým rozlišením (*High Definition Multimedia Interface*)
IAPMR	míra shody útočné prezentace podvodníkem (*Impostor Attack Presentation Match Rate*)
ICAO	Mezinárodní organizace pro civilní letectví (*International Civil Aviation Organization*)IEC mezinárodní elektronická komise (*International Electrotechnical Commission*)
IRR	míra oprávněného zamítnutí (*Impostor Rejection Rate*)
ISO	mezinárodní organizace pro standardizaci (*International Organization for Standardization*)
KI	kritická infrastruktura (*critical infrastructure*)
LDS	logická datová struktura (*Logic Data Structure*)
MRZ	strojově čitelná zóna (*Machine Readable Zone*)
NFC	blízkopolní komunikace (*Near Field Communication*)
NFIQ	obrazová kvalita otisku prstu dle NIST (*NIST Fingerprint Image Quality*)
NIST	Národní institut standardů a technologie (*National Institute of Standards and Technology*)
NV	nařízení vlády
PA	pasivní autentizace (*passive authentication*)PAD detekce prezentačního útoku (*Presentation Attack Detection*)
PAI	nástroj prezentačního útoku (*Presentation Attack Instrument*)
PKI	infrastruktura veřejných klíčů (*Public Key Infrastructure*)
PkP	povolení k pobytu
PoE	napájení po síťovém kabelu (*Power Over Ethernet*)
RFID	identifikace na rádiové frekvenci (*Radio Frequency Identification*)
ROC	provozní křivka přijímače (*Receiver Operating Curve*)
SAC	doplňkové řízení přístupu (*Supplemental Access Control*)
STC	státní tiskárna cenin
TA	terminálová autentizace (*Terminal Authentication*)
TBS	Touchless Biometric Systems s.r.o.
TMR	míra oprávněného přijetí (*True Match Rate*)
TNMR	míra oprávněného zamítnutí (*True Non-Match Rate*)
TR	technická zpráva (*Technical Report*)

8 LITERATURA

[01] KANICH Ondřej, PETROVÁ Kafková Marcela, KRAUSOVÁ Alžběta, DOSEDĚL Tomáš, DRAHANSKÝ Martin a MATEJKA Ján. *Brožura pro obyvatele - biometrické systémy*. Brno, 2021, https://www.fit.vut.cz/research/publication-file/12670/Brozura%20pro%20obyvatele.pdf.

[02] ČSN ISO/IEC 19795-1: *Informační technologie – Testování biometrické výkonnosti a podávání zpráv – Část 1: Principy a rámec*; 2023.

[03] https://source.android.com/docs/security/features/biometric/measure

[04] https://fidoalliance.org/certification/biometric-component-certification/

[05] FIDO Biometrics Requirements, on-line: https://fidoalliance.org/specs/biometric/Biometrics-Requirements-v1.0-wd-20190606.html.

[06] Odborná způsobilost v elektrotechnice od 1. 7. 2022, https://zsbozp.vubp.cz/odborna-zpusobilost-v-elektrotechnice-od-1-7-2022.

[07] Bezkontaktní multimodální biometrické zařízení, užitný vzor, ÚPV-37555, https://isdv.upv.gov.cz/doc/FullFiles/UtilityModels/FullDocuments/FDUM0037/uv037555.pdf.

[08] NOVOTNÝ, Petr. *Určování regionálních subjektů a prvků kritické infrastruktury*. Disertační práce. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2017. Dostupné z: http://hdl.handle.net/10084/120157. [cit. 2024-03-19].

[09] DRAHANSKÝ, Martin: *Hand-Based Biometrics: Methods and Technology*, IET 2018, s. 430, ISBN 978-1-78561-224-4.

[10] DRAHANSKÝ, Martin; ORSÁG, Filip; DOLEŽEL, Michal; a kol. *Biometrie*. Computer Press a.s., 2011, s. 294. ISBN 978-80-254-8979-6

[11] JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. *Handbook of Biometrics*. Springer, 2008, s. 556, ISBN 978-0-387-71040-2.

[12] ČSN ISO/IEC 30107-3: *Informační technologie - Detekce biometrického prezentačního útoku - Část 3: Testování a podávání zpráv*, 2019.

[13] MATEJKA, Ján, MATOCHOVÁ Soňa, PROKEŠ Josef. *Analýza biometrických údajů v kontextu obecného nařízení o ochraně osobních údajů*. Acta Informatica Pragensia, 2019, 8.2: 88-111.