Dodatok č. 3 k zmluve o dielo
č. SE-OVO-13-050/2010

Ministerstvo vnútra Slovenskej republiky

Sídlo:	Pribinova 2, 812 72 Bratislava, Slovenská republika
Osoba oprávnená konať:	**Ing. Denisa Saková, PhD.,** vedúca služobného úradu Ministerstva vnútra Slovenskej republiky, na základe plnomocenstva č.p.: KVSU-2012/000692-001
IČO:	00151866
Identifikačné číslo pre DPH:	SK 2020571520
Bankové spojenie:	Štátna pokladnica
Číslo účtu:	7000180023/8180

(ďalej tiež len **„objednávateľ**“)

na strane jednej

a

Hewlett-Packard Slovakia, s.r.o.

Sídlo:	Galvaniho 7, 820 02 Bratislava
Zastúpená:	**Ing. Martin Kubala,** generálny riaditeľ a konateľ
IČO:	357 853 06
Identifikačné číslo pre DPH:	SK2020213393
Bankové spojenie:	Všeobecná úverová banka, a.s.
Číslo účtu:	1464046853/0200
zapísaná v Obchodnom registri	Okresného súdu Bratislava I, oddiel: Sro, vložka č.: 21438/B

(ďalej tiež len **„zhotoviteľ“**)

na strane druhej

uzatvorili dňa 4.6.2010 zmluvu o dielo č. SE-13-050/OVO-2010 v znení jej Dodatku č. 1 zo dňa 23.6.2010 a Dodatku č. 2 zo dňa 18.5.2011 (ďalej tiež len ako „Zmluva“). Zmluvné strany, konajúc v zmysle článku 26 a súvisiacich ustanovení Zmluvy, sa dohodli na tomto Dodatku č. 3 k Zmluve, ktorým Zmluvu menia v súlade s nasledujúcim:

1 ZMENA ZMLUVY

1.1 Doposiaľ dohodnuté znenie bodu 9.5 Zmluvy sa v celom rozsahu nahrádza nasledovným znením:

„9.5 Príslušný Dokument sa považuje za riadne vykonaný vypracovaním v súlade s písomne dohodnutým popisom takého Dokumentu, čo bude potvrdené podpisom Akceptačného protokolu Predsedom Riadiaceho výboru objednávateľa a kontaktnou osobou zhotoviteľa.“.

1.2 Doposiaľ dohodnuté znenie bodu 10.11 Zmluvy sa v celom rozsahu nahrádza nasledovným znením:

“10.11 Akceptačné testy sa však budú považovať za úspešne vykonané a dôjde k obojstrannému podpisu Akceptačného protokolu Predsedom Riadiaceho výboru objednávateľa a kontaktnou osobou zhotoviteľa, ak v zmysle zápisnice o Akceptačnom teste alebo zápisnice o opakovanom Akceptačnom teste boli Vady odstránené aspoň v rozsahu, ako je uvedené v čl. 10.9. Podpis Akceptačného protokolu potvrdzuje, že Dielo alebo jeho príslušná časť bola riadne vykonaná; zhotoviteľ je však povinný odstrániť všetky Vady uvedené v zápisnici o Akceptačnom teste alebo v zápisnici o opakovanom Akceptačnom teste najneskôr v lehotách podľa bodu 10.7 tejto Zmluvy.”.

1.3 Doposiaľ dohodnuté znenie bodu 10.14.1 Zmluvy sa v celom rozsahu nahrádza nasledovným znením:

„10.14.1 O dodaní vyššie uvedených častí Diela do Miesta implementácie budú spísané osobitné preberacie protokoly, ktoré podpíšu Predseda Riadiaceho výboru objednávateľa a kontaktná osoba zhotoviteľa. O čase dodania je povinný zhotoviteľ písomne informovať objednávateľa najmenej tri (3) pracovné dni vopred.“.

1.4 Doposiaľ dohodnuté znenie bodu 11.2 Zmluvy sa v celom rozsahu nahrádza nasledovným znením:

„11.2 O uskutočnení každého školenia bude podpísaný Akceptačný protokol, ktorý podpíše Predseda Riadiaceho výboru objednávateľa a kontaktná osoba zhotoviteľa. Prílohou Akceptačného protokolu bude prezenčná listina podpísaná zamestnancami objednávateľa, ktorí sa školenia zúčastnili. O čase konania príslušného školenia podľa Prílohy č.1 tejto Zmluvy je povinný zhotoviteľ písomne informovať objednávateľa najmenej päť (5) pracovných dní vopred. Ak objednávateľ bezdôvodne odmietne podpísať Akceptačný protokol o čas, po ktorý bude objednávateľ v omeškaní s podpísaním Akceptačného protokolu sa predlžujú lehoty pre vykonanie Školenia (časti č. 11, 24, 34, 48, 65, 76, 87, 106 a 117 Diela).“.

1.5 Doposiaľ dohodnuté znenie bodu 21.6 sa v celom rozsahu nahrádza nasledovným znením:

„21.6 Zmluvné strany vytvoria Riadiaci výbor zložený zo zástupcov Zhotoviteľa a Objednávateľa, predsedom Riadiaceho výboru bude zástupca Objednávateľa a podpredsedom Riadiaceho výboru bude zástupca Zhotoviteľa. Zasadania Riadiaceho výboru sa zúčastňujú kontaktné osoby uvedené v bodoch 4.6 , 5.6 a 5.7. Zasadania Riadiaceho výboru sa budú riadiť Štatútom Riadiaceho výboru, ktorý si Riadiaci výbor schváli na svojom prvom zasadaní. Zasadanie Riadiaceho výboru bude zvolané jednou zo zmluvných strán podľa potreby. Ak nebude dohodnuté inak, žiadosť o zasadnutie Riadiaceho výboru bude doručená na korešpondenčnú adresu príslušnej zmluvnej strany najneskôr 14 dní pred požadovaným termínom zasadania Riadiaceho výboru. Z každého zasadnutia Riadiaceho výboru bude vyhotovená zápisnica, ktorá bude dokumentovať priebeh Riadiaceho výboru a prijaté rozhodnutia. Zápisnica bude vypracovaná zhotoviteľom a doručená objednávateľovi najneskôr do troch (3) pracovných dní od dátumu zasadnutia Riadiaceho výboru. Zápisnica bude podpísaná predsedom a podpredsedom Riadiaceho výboru. Ak objednávateľ nevznesie námietku alebo pripomienku k zápisnici do troch (3) pracovných dní od jej obdržania, uplynutím tejto lehoty sa bude obsah zápisnice považovať za akceptovaný zo strany objednávateľa. Zápisnica na pripomienkovanie sa považuje za doručenú, ak bude zaslaná elektronickou poštou na kontaktnú osobu objednávateľa a záložný dokument bude zaslaný faxom. Akceptovaná zápisnica sa posiela elektronicky a poštou. Uznesenia Riadiacej komisie sú nadradené uzneseniam z porád podľa bodu 21.4.“.

1.6 Doposiaľ dohodnuté znenie bodu 24 sa v celom rozsahu nahrádza nasledovným znením:

“Táto Zmluva sa uzatvára na dobu určitú v trvaní 40 mesiacov a nadobúda platnosť a účinnosť dňom jej podpísania obidvoma zmluvnými stranami.“.

1.7 Doposiaľ dohodnuté znenie Prílohy č. 1 Zmluvy sa v celom rozsahu nahrádza znením Prílohy č. 1 tohto dodatku.

1.8 Doposiaľ dohodnuté znenie Prílohy č. 2 Zmluvy sa v celom rozsahu nahrádza znením Prílohy č. 2 tohto dodatku.

2 OSTATNÉ USTANOVENIA

2.1 Tento dodatok je vyhotovený v štyroch (4) rovnopisoch, z ktorých dva (2) dostane každá zo zmluvných strán. Neoddeliteľnou súčasťou tohto dodatku sú Príloha č. 1 a Príloha č. 2. Ostatné ustanovenia Zmluvy, ktoré nie sú ustanoveniami dodatku dotknuté, zostávajú v platnosti nezmenené.

2.2 Tento dodatok nadobúda platnosť dňom jeho podpisu obidvoma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv, ktorý vedie Úrad vlády SR, v súlade so zákonom č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, a ktorými sa menia a dopĺňajú niektoré zákony. Dodatok zverejní objednávateľ.

V Bratislave dňa .....28.08.2012.....

Za Zhotoviteľa

Hewlett-Packard Slovakia, s.r.o.

_____

Ing. Martin Kubala

Generálny riaditeľ a konateľ

V Bratislave dňa .....28.08.2012.....

Za Objednávateľa

Ministerstvo vnútra Slovenskej republiky

_____

Ing. Denisa Saková, PhD.

Vedúca služobného úradu Ministerstva vnútra

Príloha č. 1 – Popis funkčnosti

Obsah

Časť I. Rozšírenie technického riešenia Personalizačného systému v Národnom personalizačnom centre Ministerstva vnútra Slovenskej republiky o personalizáciu elektronických eID kariet a vybudovanie technického riešenia pre Záložné personalizačné centrum pre personalizáciu dokladov v pôsobnosti MV na báze hrubého polykarbonátu podľa normy ISO 7810

1. Súlad riešenia s relevantnými normami

Návrh rozšírenia technického riešenia Personalizačného systému v Národnom personalizačnom centre MV o personalizáciu elektronických EID kariet a vybudovanie technického riešenia pre Záložné personalizačné centrum pre doklady v pôsobnosti MV na báze hrubého polykarbonátu podľa normy ISO 7810 bude v súlade s nasledovnými normami a predpismi:

[1] Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)Version 2.01
[2] ID cards: CEN TC224 WG15
[3] European Citizen Card + ISO 24727 Middleware are the grounds for mass-deployment of eID Cards
[4] ICAO, Machine Readable Travel Documents - Part 1: Machine Readable Passport, Specifications for electronically enabled passports with biometric identification capabilities, ICAO Doc 9303, 2006
[5] ICAO, Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents, Specifications for electronically enabled official travel documents with biometric identification capabilities, ICAO Doc 9303, 2008
[6] ISO 7816 parts 1, 2, 3, 4, 5, 6, 8 & 9
[7] ISO14443 type-A and type B
[8] Global Platform, Card Specification, Version 2.1.1, March 2003
[9] ICAO, Machine Readable Travel Documents – Technical report – Development of Logical data structure – LDS, Revision 1.7
[10] EU Technical Guideline TR 03110 - "Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control", V1. 11, 2008)“

2. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej v prílohe B1 - Opis predmetu zákazky časť I: „Rozšírenie technického riešenia Personalizačného systému v Národnom personalizačnom centre Ministerstva vnútra Slovenskej republiky o personalizáciu elektronických eID kariet a vybudovanie technického riešenia pre Záložné personalizačné centrum pre personalizáciu dokladov v pôsobnosti MV na báze hrubého polykarbonátu podľa normy ISO 7810“.

3. Predmet Technického riešenia

Predmetom technického riešenia je rozšírenie Personalizačného systému pre Národné personalizačné centrum Ministerstva vnútra Slovenskej republiky (ďalej len „NPC“) o personalizáciu elektronických identifikačných kariet (eID) z hrubého polykarbonátu s kontaktným čipom a vybudovanie technického riešenia pre Záložné personalizačné centrum (ďalej len „ZPC“) pre personalizáciu dokladov v pôsobnosti MV na báze hrubého polykarbonátu podľa normy ISO 7810 (ďalej len „ID-1 doklady“).

Rozširenie Technického riešenia bude pokrývať hlavne nasledovné oblasti:

- Rozšírenie APV pre riadenie personalizácie a logistiky výroby pre nové typy dokladov eID a eDoPP s kontaktným čipom.
- Rozšírenie APV pre personalizáciu kontaktného čipu pre nové typy dokladov eID a eDoPP.

- Rozšírenie APV Inšpekčného systému pre nové typy dokladov eID a eDoPP pre NPC, Jednotné pracoviská a Kiosky.
- Dodávka personalizačnej technológie a technickej IT infraštruktúry pre ZPC:
  - Dodávka 3 personalizačných zariadení ID-1 dokladov so SW vybavením a prislušenstvom.
  - Dodávka 2 čitacích zariadení pre podporu skartácie dokladov ID-1 so SW vybavením a príslušenstvom.
- IT infraštruktúra ZPC (servery, PC, Tlačiarne, HSM moduly, čitačky čiarových kódov, čitačky kontaktných čipov,....).
- PKI infraštruktúra (CVCA/DVCA).
- Aktualizácia pracovných rolí a procedúr pre Personalizačné centrum (NPC, ZPC).
- Aktualizovaný bezpečnostný zámer, analýzu a smernicu (ZPC, NPC).
- Dokumentácia a školenia.

4. Popis navrhovaného riešenia

V súčasnosti vydáva SR občianský preukaz formátu ID-1 karty na báze hrubého polykarbonatu bez čipu a doklad povolenie na pobyb formátu ID-1 karty na báze hrubého polykarbonátu bez čipu a obidva doklady sú vizuálne personalizované v NPC.

4.1. Účel navrhovaného riešenia

Účelom navrhovaného riešenia je vytvorenie jednotného prostriedku pre identifikáciu a autentifikáciu fyzických osôb v rámci prostredia eGovernmentu, eHealth a postupne aj v iných oblastiach verejných aj súkromných služieb. To znamená, že je potrebné rozšíriť existujúci OP vo formáte ID-1 o elektronický čip. Elektronický čip bude bezpečným prostriedkom pre uloženie identity občana SR (osobné údaje občana) v elektronickej forme a rovnako pre uloženie kvalifikovaného certifikátu na vytváranie zaručeného elektronického podpisu (ZEP). Takto vznikne kvalitatívne nový jednotný doklad totožnosti občana SR (eID), ktorý bude zároveň slúžiť na identifikáciu a autentifikáciu fyzických osôb v rámci rozvíjajúceho sa segmentu služieb eGoverment, ale aj súkromných služieb (ebanking, ...).

Personalizácia ID-1 dokladov vydávaných v rezorte MV bude rozdelená medzi obe personalizačné centrá NPC a Záložné centrum. V prípade potreby (napr. v prípade výpadku jedného z personalizačných centier) bude možné personalizáciu ID-1 dokladov presmerovať len na jedno z nich.

Doklad DoPP bude rozšírený o kontaktný čip a bude poskytovať indentickú funkcionalitu pre cudzincov s pobybom na území SR ako eID pre občanov SR.

4.2. Prínosy navrhovaného riešenia

Navrhované technické riešenie je v súlade s cieľom projektu na vytvorenie elektronickej identifikačnej karty (elektronického OP) ako prostriedku na zrýchlenie administratívnych úkonov pre občanov, zlepšenie prístupnosti služieb štátu občanom ako aj vytvoreniu transparentného elektronického styku a konkrétnejšie:

- pre občana vytvoriť elektronický OP (eID) ako nástroj zefektívnenia komunikácie so štátnou správou a súkromným sektorom,
- pre cudzincov s pobytom na území SR vytvoriť elektronický DoPP ako nástroj zefektívnenia komunikácie so štátnou správou a súkromným sektorom
- elektronický OP a DoPP budú postavené na najnovších technológiách pre oblasť identifikačných dokladov,
- elektronický OP v súlade s európskou legislatívou a požiadavkami tak, aby bol postupne migrovateľný na jednotný elektronický doklad (ECC) občanov EÚ.
- vybudovanie záložnej kapacity NPC prostredníctvom Záložného personalizačného centra (ZPC) pre doklady formátu ID-1 v pôsobnosti MV SR a tým zabezpečiť kontinuálnu prevádzku v prípade nepredvídateľných a havarijných stavoch v NPC.
- zvýšenie kapacity NPC pomocou záložného Personalizačného systému, ktorý umožní bezpečne personalizovať všetky doklady formátu ID-1 v pôsobnosti MV SR.

5. Procesný model

Procesný model pre personalizaciu v súčasnosti vydávaných dokladov ID-1 v NPC bude aktualizovaný pre zavedenie nových typov dokladov: elektronického OP a elektronického DoPP a proces personalizácie bude vykonávaný v nasledovných krokoch:

1 - Prijatie a kontrola údajov na výrobu/personalizáciu dokladu

Objednávky sú generované systémom IS SA agenda OP (resp. IS ECU) a prichádzajú overené oproti údajom v IS SA (resp. IS ECU) a iným relevantným údajom z príslušných agend, pričom toto overovanie zabezpečuje IS SA (resp. IS ECU). Systém musí prijať objednávku cez API a odoslať ju na ďalšie spracovanie. V tomto kroku príjme systém údaje zo žiadosti o vydanie dokladu v elektronickej forme pre jednotlivé schválené obyčajné alebo expresné žiadosti (označené príznakom v žiadosti). Pozn. Expresné žiadosti sú relevantné len v prípade dokladu eID. Prijaté údaje zo žiadosti musia obsahovať všetky údaje potrebné na personalizáciu dokladu.

Každá prijatá žiadosť je tiež kontrolovaná na jedinečnosť a úplnosť - na základe definovaného vzoru sa kontroluje prítomnosť polí (údajov). Na základe týchto kontrol je rozhodnuté o akceptovaní resp. neakceptovaní žiadosti. O výsledku operácie kontroly je informovaný IS SA (resp. IS ECU) prostredníctvom rozhrania a dohodnutého protokolu. Údaje zo žiadosti sú v tomto kroku uložené do produkčnej databázy.

2 - Generovanie výrobných dávok

Akceptovaná objednávka je predmetom spracovania v systéme. Akceptované objednávky sú triedené a zoskupované do výrobných dávok (VD) podľa preddefinovaných kritérií. K dodávaným kritériám triedenia patria doba dodávky dokladu, lokalita (JP), doba prijatia objednávky.

Pri prijatí žiadosti je tiež identifikovaný typ žiadosti dokladu, t.j. či sa jedná bežnú alebo expresnú žiadosť (typ žiadosti bude rozlíšený pomocou príznaku uvedeného v žiadosti). Typ žiadosti nebude možné zmeniť v rámci personalizačného systému. Expresné žiadosti budú spracovávané prednostne v samostatných VD (platí len pre doklad eID). Ľubovoľnú vybranú bežnú žiadosť bude možné vyrobiť prednostne.

Po zaradení údajov zo žiadosti do databázy sú generované výrobné dávky. Výrobné dávky sú počas pracovnej zmeny pripravované prípravárom v pravidelných intervaloch, resp. podľa potreby a počtu nespracovaných čakajúcich objednávok. Zároveň je vygenerovaný a vytlačený Zoznam dokladov VD a príslušné etikety na balíčky dokladov, ktoré sú v nasledujúcom kroku odovzdávané spolu s čistopismi pre VD výrobárovi. Zoznam dokladov je používaný pre administratívne a overovacie účely, napr. pri kontrole kvality.

Výstupom toho kroku sú vygenerované výrobné dávky, ktoré sú následne pripravené na personalizáciu na personalizačnom zariadení.

3 – Príprava personalizačných údajov na personalizáciu

V tomto kroku prechádzajú výrobné dávky, resp. obsiahnuté údaje zo žiadosti spracované procesom prípravy na personalizáciu, ktorého cieľom je pripraviť údaje na spracovanie v personalizačných zariadeniach (pomocou technológie laserového gravírovania). V tomto kroku nie sú spracovávané jednotlivé objednávky samostatne (údaje o jednotlivých žiadostiach), ale spracúvajú sa údaje zoskupené dohromady do výrobných dávok. Na konci tohto kroku sú údaje pripravené na prenos do personalizačného zariadenia a následne sú takto pripravené údaje prenesené na ďalšie spracovanie (personalizovanie) do personalizačných výrobných liniek.

Zároveň sa v tomto kroku rozhodne o tom, na ktorom personalizačnom zariadení sa bude daná VD personalizovať. Rozhodnutie sa štandardne vykoná automaticky, ale supervízor má možnosť o prideľovaní VD rozhodovať aj manuálne.

Výstupom toho kroku sú výrobné dávky pripravené na personalizačných zariadeniach na personalizáciu.

4a – Personalizácia dokladu metódou laserového gravírovania

Čistopisy dokladov sú personalizované na personalizačnom zariadení technológiou laserového gravírovania. Vstupom do personalizačného zariadenia sú čistopisy dokladov. APV vedie evidenciu všetkých použitých čistopisov dokladov, ktoré sa objavili na vstupe personalizačných zariadení.

Výstupom toho kroku sú vizuálne personalizované doklady.

4b - Zápis údajov do kontaktného čipu

Pri personalizovaní dokladu subsystém ePerson pripraví údaje na zápis do pamäte čipu a odovzdá ich modulu personalizačného zariadenia zodpovedného za zápis do čipu. Tento modul následne overí autenticitu čipu (pomocou tzv. transportného kľúča) a čip odomkne na zápis, vytvorí dátovú štruktúru (pre osobné údaje držiteľa, v prípade dokladu eID taktiež aj pre aplikáciu a údaje na realizáciu ZEP, údaje o karte a autorizačné údaje, iný dátový priestor napr. pre eHealth, zapíše všetky pripravené údaje do čipu (zaintegrovaného do materiálu dokladu), po úspešnom zápise údajov čip uzamkne. To znamená, že čip bude zablokovaný na zápis a jeho obsah už môže byť následne zmenený len na základe dohodnutého autentifikačného mechanizmu.

Rozdelenie zodpovednosti za inicializáciu, pre-personalizáciu a samotnú personalizáciu bude zadefinované medzi dodávateľom čistopisov eID a eDoPP a zhotoviteľom personalizačného systému tak, aby boli zohľadnené bezpečnostné požiadavky, požiadavky na efektívne využívanie personalizačných zariadení a tiež návrh štruktúry čipu (aplikácie, súborový systém, ...). To znamená, že časť aktivít bude vykonávaná ešte dodávateľom čistopisov a časť aktivít bude vykonávaná v rámci tohto kroku v Personalizačnom centre.

Výstupom toho kroku sú personalizované doklady s uzamknutým personalizovaným čipom pripraveným na zápis certifikátov pre ZEP a AC a prípadne ďalších certifikátov na pracoviskách RA.

Krok 5 - Kontrola kvality personalizovaných dokladov

Po ukončení personalizácie dokladu je výrobárom skontrolovaná kvalita personalizácie (kvalita laserového gravírovania). Kvalita laserového gravírovania je najskôr kontrolovaná/nastavovaná personalizačným zariadením priamo počas personalizácie (sú nastavované parametre zameranie laserového lúča). Následne výrobár vykonaná vizuálnu kontrolu kvality personalizácie. Každý doklad prechádza štandardnou kontrolou kvality po ukončení jeho personalizácie, ktorú vykonáva výrobár. Všetky personalizované doklady sú kontrolované vizuálne a počas kontroly sú vyhodnotené najmä nasledovné parametre:

- hustota gravírovania,
- pozícia jednotlivých gravírovaných položiek polykarbonátovej ID-1 karty,
- nečistoty na polykarbonátovej karte.

Potom výrobár vykonáva detailnú kontrolu kvality vybraných personalizovaných dokladov voči schváleným tzv. referenčným modelom: pre prvý, stredný a ostatný doklad každej výrobnej dávky a vyplní protokol o kvalite.

Následne kontrolór overí správnosť zapísaných údajov do čipu. Táto kontrola overí správnosť údajov zapísaných do čipu voči pôvodným personalizačným údajom, ako aj správnosť údajov opticky personalizovaných (laserovým gravírovaním) voči údajom zapísaným do čipu. Okrem toho sa počas tejto kontroly overí aj integrita údajov (pomocou tzv. pasívnej autentifikácie) a tiež aj autenticita čipu a teda aj údajov do neho zapísaných (pomocou tzv. aktívnej autentifikácie, príp. iného obdobného bezpečnostného mechanizmu). Týmto sa overí schopnosť čipu správne reagovať na tieto kontroly aj neskôr pri následných kontrolách dokladu. Systém umožní v prípade potreby pripojiť viacej externých čítacích zariadení a tým zvýšiť kapacitu kontrolnej činnosti.

Identifikované nepresnosti a vady sa evidujú ako nepodarky a majú za následok znehodnotenie takýchto dokladov a ich následné skartovanie (čo je taktiež zaevidované v systéme). Ak kvalita personalizácie dokladov nedosahuje požadovaný štandard, tak budú na personalizačnom zariadení vykonané potrebné nastavenia a zároveň sa pre nepodarky inicializuje opravná personalizácia (tzv. remake procedúra).

Proces spracovania všetkých žiadostí (objednávky) tak, ako sú postupne (v jednotlivých krokoch) spracovávané a personalizované, je logovaný.

Výstupom toho kroku sú výrobárom a kontrolórom skontrolované personalizované doklady pripravené na distribúciu, zároveň je IS SA informovaný o balíčkoch dokladov, ktoré boli odvzdané na distribúciu v rámci Personalizačného centra.

Krok 6a Podpora distribúcie

Pre doklady, ktoré majú byť distribuované na pracoviská JP bude proces výroby ukončený prípravou balíčkov.

Poznámka: v terminológii JP sa pre túto entitu používa pojem balík.

Balíček (označený čiarovým kódom) obsahuje definovaný počet personalizovaných dokladov určených pre jedno JP, štandardne sa bude jednať o 10ks dokladov. Obsah balíka je posielaný elektronicky do IS SA, resp. IS ECU. Z balíčkov sú následne pripravované balíky hotových dokladov pre jednotlivé JP. Následná distribúcia balíkov je predmetom kuriérnej služby. V rámci distribúcie hotových dokladov (štadnardne sa uskutočňuje 1x denne počas personalizačného procesu okolo 13:00) sú personalizované doklady zabalené do balíkov na expedíciu a systém pripraví sprievodné dokumenty pre jednotlivé balíky, ktoré sú zaslané v papierovej forme spolu s personalizovanými dokladmi na príslušné JP.

.

Všetky balíky sú nakoniec uložené do prepraviek (pre každú prepravku je generovaná sprievodná dokumentácia – zoznam balení), ktoré sú kuriérnou službou distribuované na podateľne, z ktorých sú potom balíky, distribuované ďalej na JP, pokiaľ je to potrebné.

Výstupom toho kroku sú personalizované doklady zabalené do balíkov a prepraviek odovzdané kuriérnej službe na distribúciu.

6. Funkčný model

Navrhovaný systém bude rozšírený pre zavedenie nových typov dokladov eID a eDoPP o nasledovné kľúčové subsystémy:

- Subsystém pre riadenie personalizácie a logistiky výroby dokladov pre nové typy dokladov eID a eDoPP.
- Subsystém pre personalizáciu kontaktného čipu dokladov eID a eDoPP
- Inšpekčný subsystém

6.1. Subsystém pre riadenie personalizácie a logistiky výroby pre nové typy dokladov eID a eDoPP

Existujúci subsystém pre riadenie personalizácie a logistiky výroby ID-1 dokladov bude podporovať logistické funkcie a automatizovať kľúčové činnosti a procesy správy výroby ID-1 dokladov existujúcich typov a bude rozšírený o podporu nových typov dokladov eID a elektronického DoPP. Subsystém sprístupní používateľské rozhranie pre vykonávanie činností jednotlivých používateľských rolí. Ďalej zabezpečí komunikačné rozhrania pre externé systémy ako napr. Informačný Systém MVSR generujúci skupinové objednávky na výrobu dokladov a prijímajúci aktualizácie o stave výroby dokladov. Funkcie subsystému budú rozdelené do nasledovnych skupín (alebo subsytémov):

Rozhranie na ostatné systémy

Subsystém rozhraní na ostatné systémy poskytne komunikačné rozhranie pre automatizovaný príjem objednávok na personalizáciu ID-1 dokladov z agiend evidujúcich jednotlivé typy dokladov. Bude vykonávať kontrolu na úplnosť (prítomnost údajov v jednotlivých poliach) a informovanie o zmenách stavu prijatej žiadosti podľa postupu jej spracovania v subsystémoch výroby a expedície. Ďalej poskytne komunikačné rozhranie na automatizovaný príjem zoznamov dokladov odoslaných na skartáciu a informovanie o zmenách stavov v procese skartácie prijatých dokladov.

Logistika

Subsystém logistika zabezpečí evidenciu dodávateľov čistopisov, plánovaných a uskutočnených dodávok, prijímanie dodávok, kontrolu dodávok na vady čistopisov dokladov. Medzi podporované funkčnosti patrí:

- vedenie evidencie dodávateľov čistopisov dokladov,
- vedenie evidencie dodávok čistopisov dokladov,
- podpora pri kontrole dodávky, či dodávka nemá vadu, zaevidovanie jednotlivých kontrolovaných čistopisov, evidencia výsledkov kontrol dodávok a jednotlivých čistopisov a možnosť vygenerovať protokol o výsledku kontroly.

Subsystém logistika zabezpečuje aj reklamáciu čistopisov-nepodarkov. Reklamácia čistopisov–nepodarkov obsahuje komponenty pre vytvorenie podkladov pre dodávateľa čistopisov na opätovnú dodávku chybne vyrobených čistopisov. Medzi podporované funkčnosti patrí:

- priradenie označenia chyby (z katalógu/tabuľky chýb) k čistopisu v evidencii, ak bol čistopis označený za nepodarok (katalóg/tabuľku chýb vytvára používateľ),
- príprava reklamačných balíčkov,
- generovanie tlačových reportov o reklamácii.

Ďalej subsystém logistika podporí procesy skartácie dokladov v personalizačnom centre automatizovaným príjmom zoznamov dokladov určených na skartáciu, podporou kontroly voči fyzicky doručeným dokladom a generovaním sprievodnej dokumentácie skartácie. Medzi podporované funkčnosti patrí:

- automatizovaný príjem zoznamu dokladov určených na skartaciu,
- kontrola voči fyzickému stavu prijatých dokladov + podpora automatizovaného čítania čísiel na fyzických dokladch určených na skartáciu,
- príprava a odoslanie na skartáciu,
- generovanie tlačových reportov a potvrdení o vykonaní skartacie pre nadradené systémy.

Sklad

Subsystém sklad zabezpečí vedenie evidencie čistopisov a nepodarkov, inventarizáciu skladu, pohyby čistopisov a nepodarkov medzi skladmi a konsolidáciu boxov čistopisov. Medzi podporované funkčnosti patrí:

- vedenie evidencie dodaných čistopisov, personalizovaných čistopisov, nepodarkov, reklamovaných čistopisov,
- možnosť vykonať inventúru čistopisov, personalizovaných čistopisov, reklamovaných čistopisov, nepodarkov a skartovaných kariet,
- generovanie a tlač reportov,
- presun čistopisov a nepodarkov medzi skladmi čistopisov v NPC a ZPC.

Evidencia balíkov a boxov čistopisov je na baze čiarových kódov.

Medzisklad - obsahuje komponenty pre správu, evidenciu a inventarizáciu medziskladu. Medzi podporované funkčnosti patrí:

- príjem čistopisov do medziskladu,
- inventarizácia medziskladu,
- presuny čistopisov a nepodarkov do výroby a späť,
- generovanie a tlač reportov,
- Konsolidácia – obsahuje komponenty pre okamžité zistenie stavu a počtov dokladov vo vybranom boxe.

Výroba

Subsystém výroby obsahuje komponenty pre definovanie a správu pracovných zmien (otvorenie zmeny, pracovné role, zmenová uzávierka) personalizácie dokladov. Medzi podporované funkčnosti patrí:

- otvorenie a konfigurácia zmeny,
- možnosť vygenerovať vždy po skončení zmeny kontrolný výkaz počtu vydaných čistopisov zo skladu, voči počtu personalizovaných čistopisov odovzdaných na expedíciu, vrátených čistopisov a nepodarkov do skladu.

Subsystém výroba taktiež obsahuje komponenty pre plánovanie výroby, vyhľadávanie žiadostí na výrobu dokladov, generovanie, uvoľňovanie a správu výrobných dávok určených na personalizáciu, priradenie výrobnej dávky na technologické zariadenie ručné alebo s možnosťou automatického prednastavenia poľa typu dokladu k technologickému zariadeniu.

Load balancing – obsahuje komponenty pre automatické striedavé priraďovanie dávok ku viacerim technologickým zariadeniam.

Generovanie opravných výrobných dávok (revýroba nepodarkov) a komponenty pre konverziu údajov do formátu potrebného pre technologické zariadenie a komponenty komunikačného rozhrania na technologické zariadenie.

Medzi podporované funkčnosti patrí:

- možnosť nastavenia veľkosti dávok a možnosť operatívne zmeniť veľkosť dávok počas zmeny (resp. subdávok),
- zobrazenie aktuálneho stavu výberu pri tvorbe dávok,
- automatické vygenerovanie dávok podľa preddefinovaných kritérií,
- manuálne vygenerovanie dávok operátorom,
- zrušenie vygenerovanej dávky/dávok (manuálnych aj automatických),
- okamžité zaradenie expresnej žiadosti/žiadostí na personalizáciu v samostatnej dávke/dávkach,
- prehľady nevybavených objednávok celkovo a podľa jednotlivých jednotných pracovísk,
- prípravu údajov a dávok na personalizáciu vzorových dokladov (specimenov),
- vyhľadávanie hotových dokladov a história stavov dokladov,

- automatické aj manuálne určenie technologického zariadenia a odoslanie dávky na personalizáciu,
- zobrazenie dávok odoslaných na personalizáciu,
- revýroba nepodarkov vrátených z výroby alebo kontroly kvality,
- samostatné odovzdanie urýchlenej žiadosti do expedície počas trvania zmeny,
- personalizácia vzorových dokladov (specimenov),
- generovanie informácií o stave personalizácie čistopisu,
- overenie-kalibrácia personalizačného zariadenia,
- konverzia dát pre personalizačné zariadenia.

Subsystém prípravy výroby bude generovať výkazy o produkcii bez osobných údajov. Subsystém prípravy výroby obsahuje komponenty pre export žiadostí o externú personalizáciu zo systému a zápis na prenosné médium, import hlásení o externej personalizácii z prenosného média.

Expedícia

Subsystém expedícia zabezpečí kontrolu kvality personalizovaných dokladov so zaintegrovanou kontrolou údajov na čipe dokladu na autentičnosť a integritu. Subsystém kontrola a expedícia bude podporovať generovanie a tlač sprievodnej dokumentácie, reportov a odovzdanie dokladov kurierovi.

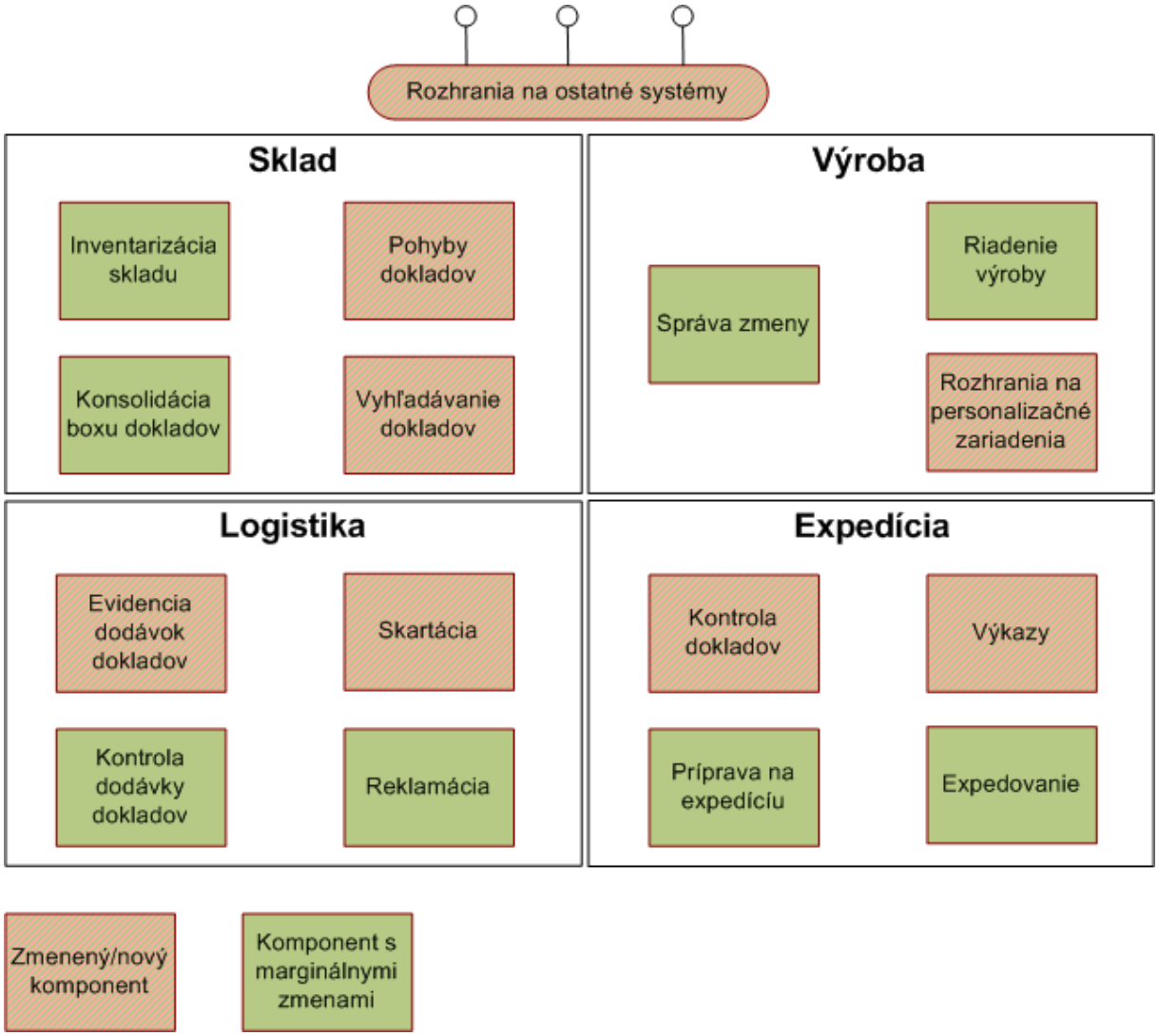
Medzi podporované funkčnosti patrí:

- kontrola kvality dokladov vrátane kontroly údajov na čipe dokladu OoE I, eID a eDoPP,
- evidencia expedovaných personalizovaných dokladov v jednotlivých balíkoch,
- generovanie a tlač sprievodných dokladov pre distribúciu balíkov s personalizovanými dokladmi,
- generovanie a tlač nálepiek na balíky,
- triedenie a samostatné balenie podľa druhov dokladov a charakteru žiadosti (bežné – urýchlené) s označovaním aký charakter majú doklady v balíku.

Administratívne funkcie

Tieto funkcie slúžia administrátorovi systému na, tvorbu štatistických reportov a na modifikáciu hodnôt a konfiguračných parametrov systému:

- údržba číselníkov (dodávatelia, kuriéri, materiál,..),
- evidencia stavov dokladov, objednávok a čistopisov, štatistiky a reporty,
- konfigurácia parametrov (zmien preddefinovaných hodnôt parametrov súvisiacich rozhraniami na externé systémy a parametrov pre objednávku, dodávku, skartačný zoznam a pod.),
- zavedenie nového typu dokladu do systému,
- pridanie personalizačného zariadenia do systému.



Obrázok č.1. Funkčná architektúra subsystému pre riadenie personalizácie a logistiky výroby ID-1 dokladov

6.2. Sybsystém pre personalizáciu kontakneho čipu dokladu (ePerso)

6.2.1 LDS pre eID a eDoPP

LDS pre eID a elektronický DoPP obsahuje:

- Údaje o doklade (napr. číslo dokladu , dátum vydania, koniec platnosti , vydavateľ a pod.). Osobné údaje (napr. meno, priezvisko, tituly, adresu trvalého bydliska, miesto a dátum narodenia). Osobne údaje budú uložené v LDS a jej dátových skupinách DG1 až DG18 v súlade s normou [1].
- Autentifikačný objekt ako PIN na ochranu osobných údajov držiteľa dokladu.
- Autentifikačné objekty ako kľúčové páry pre implementáciu prístupu k vyššie uvedeným osobným údajom pred neoprávneným čítaním a zápisom pomocou bezpečnostných mechanizmov postavených na PKI infraštruktúre a pomocou mechanizmu rozšírenej kontroly prístupu – EAC v súlade s normou [1] alebo obdobného mechanizmu v súlade s bezpečnostnými mechanizmami platformy operačného systému kontaktného čipu na eID doklade . Osobné údaje a autentizačné objekty budú uložené na čipe eID v súlade s normou ISO/IEC 7816 – 4.

Na kontaktnom čipe bude vyhradený dátovo adresný priestor na:

- Certifikát(y) (a príslušné kľúčové páry) pre identifikáciu a autentifikáciu držiteľa eID karty (zapisované na

pracoviskách RA),

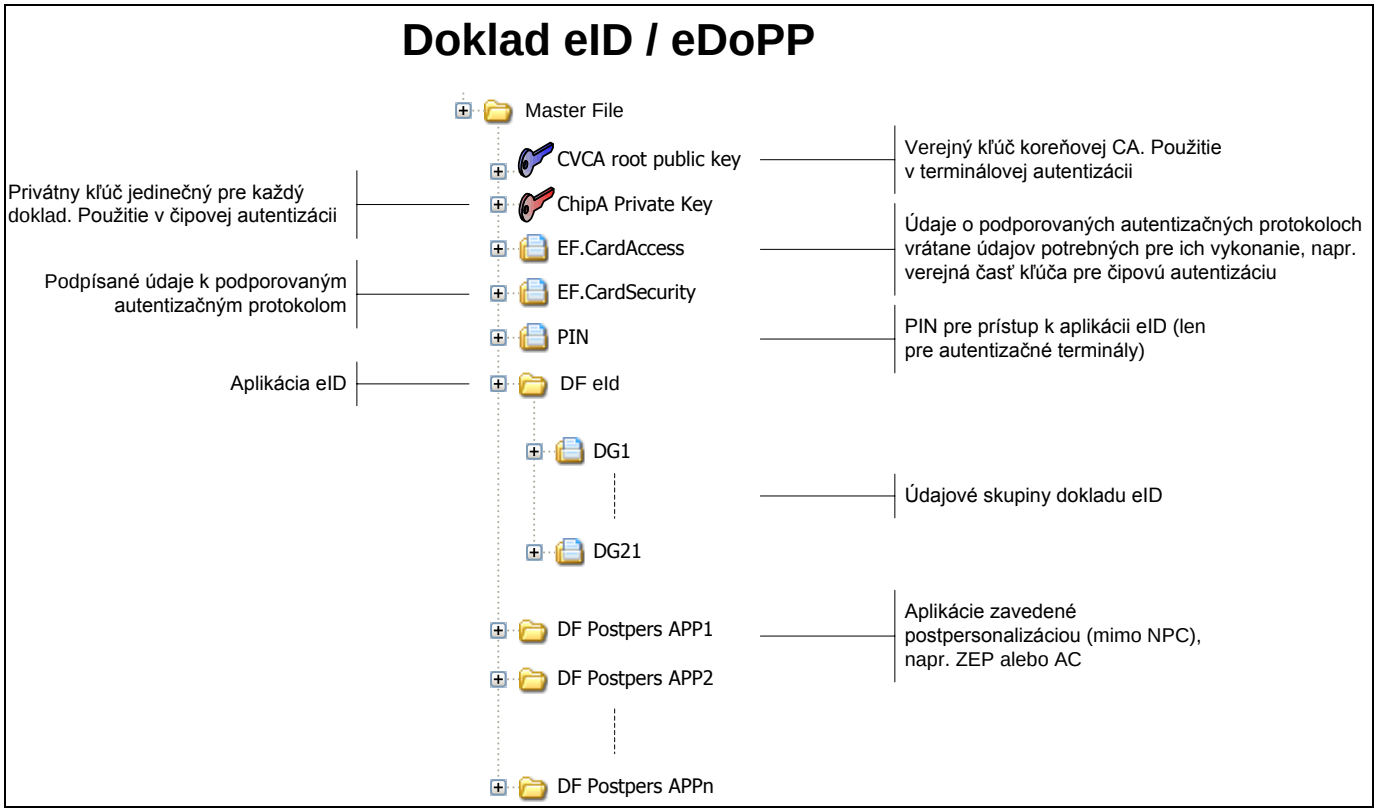
- Certifikát(y) (a príslušné kľúčové páry) pre vyhotovovanie ZEP (zapisované na pracoviskách RA)
- dátovo-adresný priestor pre iný, budúci účel (napr. základné údaje o sociálnom poistení, zdravotnom poistení, pre určenie jednoznačnej príslušnosti k zdravotnej poisťovni a iné).

Dátová skupina	Obsah	FID	SFID	R/W (čítanie, zápis)
DG1	Typ dokumentu	0x0101	0x01	R
DG2	Štát, ktorý doklad vydal	0x0102	0x02	R
DG3	Platnosť do	0x0103	0x03	R
DG4	Meno	0x0104	0x04	R
DG5	Priezvisko	0x0105	0x05	R
DG6	Meno podľa náboženstva alebo umelecké meno	0x0106	0x06	R
DG7	Akademický titul	0x0107	0x07	R
DG8	Dátum narodenia	0x0108	0x08	R
DG9	Miesto narodenia	0x0109	0x09	R
DG10	Štátna príslušnosť	0x010A	0x0A	R
DG11	Pohlavie	0x010B	0x0B	R
DG12	Voliteľné údaje (pre čítanie)	0x010C	0x0C	R
DG13	--	0x010D	0x0D	R
DG14	--	0x010E	0x0E	R
DG15	--	0x010F	0x0F	R
DG16	--	0x0111	0x11	R/W
DG17	Miesto trvalého pobytu	0x0112	0x12	R/W
DG18	Kód komunity	0x0113	0x13	R/W
DG19	Prechodný pobyt 1	0x0114	0x14	R/W
DG20	Prechodný pobyt 2	0x0115	0x15	R/W
DG21	Voliteľné údaje (pre čítanie aj zápis)	0x0116	0x16	R/W

Tabuľka 1: LDS na čipe pre eID a eDoPP

6.2.2 Súborová štruktúra na čipe pre doklady eID a eDoPP

Súborová štruktúra na čipe dokladu bude podľa ISO 7816 nasledovná:



Obrázok č. 2. Súborová štruktúra ISO/IEC 7816 – 4 na čipe eID a eDoPP

Definitívne stanovenie obsahu logickej dátovej štruktury LDS (DG1 až DG18) a špecifikácia súborovej štruktúry pre eID a eDoPP bude predmetom analytickej fazy dodávky projektu.

Doklad (eID, eDoPP) je rozdelený do logických priestorov – adresárov (DF):

- Koreňový adresár MF obsahuje údaje pre čipovú, terminálovú a používateľskú (PIN kód) autentizáciu
- Adresár DF eID obsahuje osobné údaje o občanovi
- Adresáre DF Postpers APP1 .. APPn slúžia pre uloženie kartových aplikácií pre ZEP, autentizáciu (AC) a šifrovanie. Tieto certifikáty sa nezavádzajú v Personalizačnom centre a preto sú mimo rozsah tejto ponuky.

Doklad obsahuje údaje:

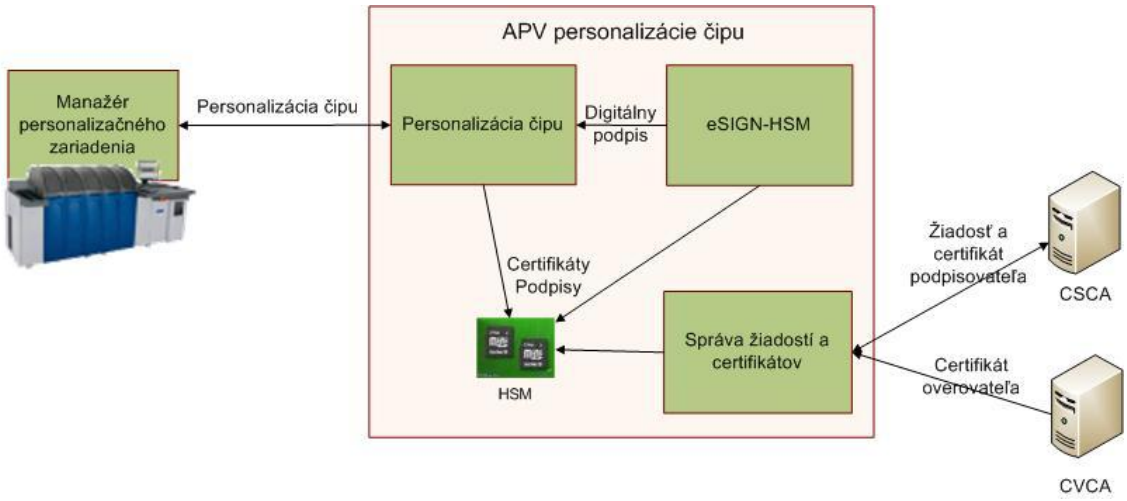
Údaj	Popis	Využitie pre
CVCA root public key	Verejný kľúč koreňovej CVCA	Terminálová autentizácia
CA Private Key	Privátny kľúč čipu	Čipová autentizácia
EFCardAccess, EFCardSecurity	Card Security Object SOC obsahuje informácie o podporovaných protokoloch (čipová a terminálová autentizácia). O.i. obsahuje aj verejný kľúč čipu pre čipovú autentizáciu	Pasívna autentizácia, Terminálová autentizácia
PIN	PIN pre prístup k údajom	Vyčítanie údajov
DG1-DG21	Údaje o držiteľovi dokladu	Uloženie údajov

Subsystém ePerso bude zodpovedný za zápis údajov do kontaktného čipu pre eID a pre elektronické povolenie na pobyt (eDoPP):

Subsystém ePerso je zodpovedný:

- Príprava dát pre personalizáciu
  - prevzatie a spracovanie z Manažéra personalizačného zariadenia (Syntera)
  - spracovanie pre personalizáciu a podpis dát pre pasívnu autentizáciu (PA) certifikátom podpisovateľa (DS) – rozhranie na komponent eSIGN-HSM

- Generovanie kľúčového páru pre čipovú autentizáciu – rozhranie HSM
- Zavedenie dátovej štruktúry do čipu:
  - odomknutie čipu pomocou transportných kľúčov,
  - zavedenie aplikácie eId pre elektronický občiansky preukaz
- Finalizácia personalizácie čipu – uzamknutie čipu – ďalší zápis možný len po autentizácii oprávnenej entity
- Vyhodnotenie výsledku personalizácie
  - kontrola personalizácie – rozhranie na komponent pre vyčítanie a kontrolu
  - poskytnutie výsledku – rozhranie na komponent Manažér personalizačného zariadenia (Syntera)



Obrázok č. 3. Komponentová architektúra ePerso subsystému

6.3. Inšpekčný subsystém

V navrhovanom riešení a jeho nižšie popísaných subsystémoch budú implementované nasledovné princípy autentifikácie:

6.3.1 Základné princípy autentifikácie pre prístup k údajom na čipe dokladu

Pri prístupe na doklad (čip) sa rozlišujú dva typy terminálov:

Inšpekčný systém (IS), ktorý umožňuje vykonať kontrolu dokladu a vyčítať z neho údaje bez zadania osobného kódu PIN. Tento princíp sa používa pri kontrole dokladu:

- kontrola po personalizácii

Autentifikačný systém (AS), ktorý umožňuje vykonať kontrolu dokladu a vyčítať z neho údaje s nutnosťou zadať osobný kód PIN. Takýto systém navyše (podľa oprávnení v CV certifikáte vo formáte podľa[1]) umožňuje otvoriť kartu pre zápis. Tento princíp sa používa pri:

- kontrola dokladu pracovníkom jednotného pracoviska (JP)
- kontrola dokladu v Kioskoch
- zápis/zmena osobných údajov vo vybraných DG
- zavedenie aplikácie pre ZEP a zápis certifikátov na RA (postpersonalizácia)
- zavedenie aplikácie pre Autentizáciu a zápis certifikátu AC na RA (postpersonalizácia)

6.3.1.1. Požiadavky na ochranu údajov

Z hľadiska bezpečnosti údajov je potrebné zabezpečiť doklad eID a eDoPP proti:

- klonovaniu dokladu (zabezpečuje ChipA + PA s SO_C)
- neoprávnenej zmene údajov (zabezpečuje OS karty prostredníctvom navrhnutej bezpečnostnej architektúry údajovej štruktúry dokladu)

- neoprávnenému prístupu k údajom (zabezpečuje TA a PIN)

6.3.1.2. Prostriedky pre ochranu údajov

Pre autentifikáciu s čipom budú použité autentifikačné protokoly založené na EAC PKI podľa [1]:

- overenie pravosti čipu – čipová autentifikácia (ChipA)
- overenie oprávnenia terminálu – terminálová autentifikácia (TA)
- overenie integrity a autenticity dát pre čipovú autentifikáciu – pasívna autentifikácia (PA)

Čipová a pasívna autentifikácia slúžia ako prostriedok terminálu pre overenie pravosti dokladu a kontrolu integrity a autenticity údajov použitých pre čipovú autentifikáciu.

Naopak terminálová autentifikácia slúži ako prostriedok karty pre overenie oprávnenia terminálu pre prístup k uloženým dátam.

Nasledujúca tabuľka popisuje, za akých podmienok je možné získať právo zápisu/čítania do/z jednotlivých aplikácií čipu.

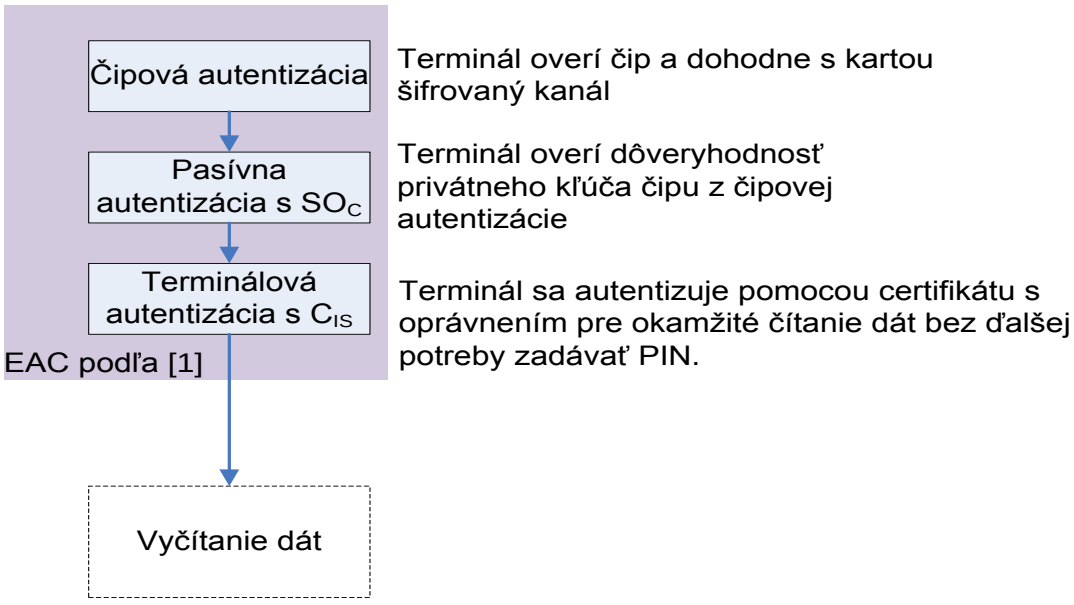
DF / aplikácia	Prístup	Požiadavky na terminál / systém	Autentizácia / prístup
Master file	Zavedenie aplikácie	Certifikát CV AS s oprávnením pre zavedenie novej aplikácie	CA + TA
eID	Čítanie údajov	Certifikát CV IS s oprávnením pre čítanie údajov eId	CA + TA
		Certifikát CV AS s oprávnením pre čítanie údajov eId	CA + TA + PIN
	Zápis údajov	Certifikát AS s oprávnením pre zápis údajov eID	CA + TA + PIN

Nasledujúca tabuľka zobrazuje oprávnenia jednotlivých typov terminálov pre prístup k údajom dokladu eID / eDoPP:

	Oprávnenie pre		
Typ klienta IS (terminál)	Kontrola dokladu	Zmena údajov	Postpersonalizácia
NPC	Kontrola dokladu po personalizácii. Autentifikácia: ChipA + TA Mód IS: inšpekčný		
JP	Kontrola dokladu pri odovzdaní občanovi Autentifikácia: ChipA + TA + PIN Mód IS: autentifikačný	Zápis/zmena osobných údajov; zmeniť je možné len polia podľa tabuľky uvedenej v kapitole 6.2.1 Autentifikácia: ChipA + TA + PIN Mód IS: autentifikačný	
Kiosk	Samoobslužná kontrola dokladu pri prevzatí dokladu Autentifikácia: ChipA + TA + PIN Mód IS: autentifikačný		
CA/RA			Zavedenie aplikácie pre ZEP a zápis certifikátu na CA/RA Zavedenie aplikácie pre Autentifikáciu a zápis certifikátu AC na CA/RA Autentifikácia: ChipA + TA Mód IS: autentifikačný

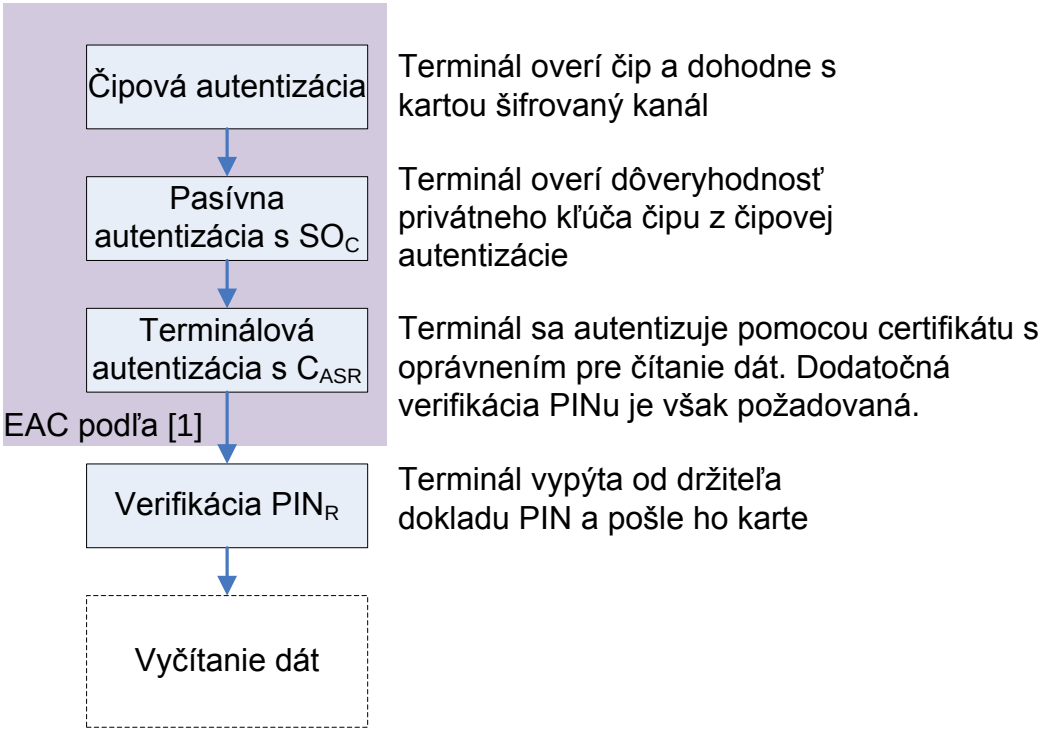
6.3.1.3. Inšpekčný Systém – Čítanie dát

Pri kontrole po persornalizacii v Personalizačnom systéme bude vykonaná inšpekčná procedúra ako postupnosť krokov pre čítanie dátových skupín z kontaktného čipu znázornená na nasledujúcom obrázku (bez zadania osobného kódu PIN):



6.3.1.4. Autentifikačný Systém – Čítanie dát

Scenár pre inšpekčnú procedúru na JP resp. pre Kiosk pre čítanie dátových skupín z čipu s použitím kódu PIN je znázornený na nasledujúcom obrázku:



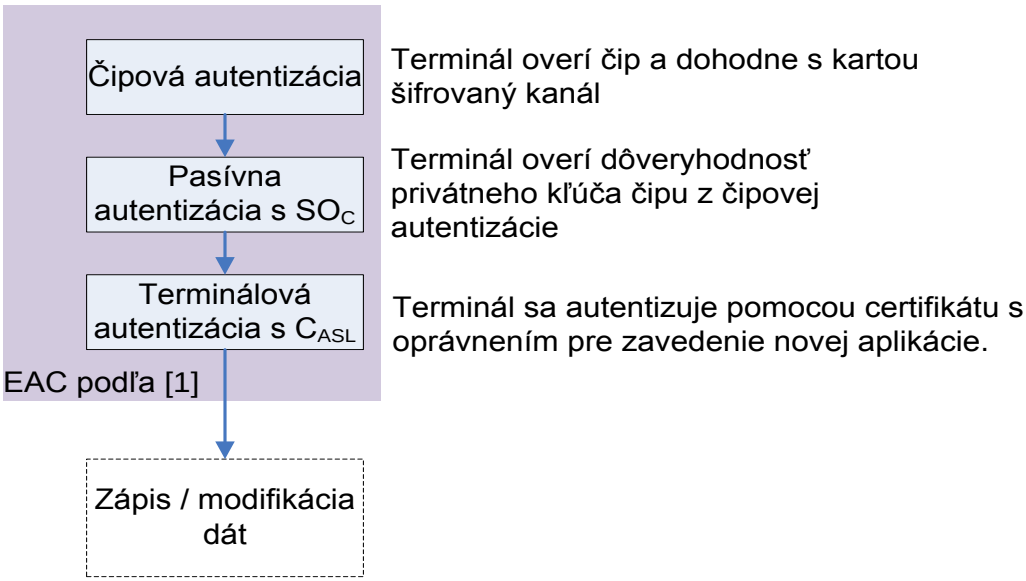
Verifikácia PINu držiteľa dokladu je implementovaná prostredníctvom zabezpečeného kanálu.

V tomto prípade sa použije CV certifikát pre autentifikačný systém s oprávnením pre kontrolu dokladu a vyčítanie údajov v kombinácii so zadaním osobného kódu PIN. Formát CV certifikátu podľa [1] bude špecifikovaný v analytickej fáze dodávky projektu.

6.3.1.5. Autentifikačný Systém – Postpersonalizácia

Mechanizmus umožňujúci zavedenie ďalšej kartovej aplikácie (napr. aplikácia pre ZEP alebo pre autentifikáciu na báze certifikátu AC so zápisom prislušných certifikátov na pracoviskách RA) prostredníctvom autentifikácie a bezpečnostného kanálu na báze CV certifikátu a EAC podľa [1]– čipová a terminálová autentifikácia.

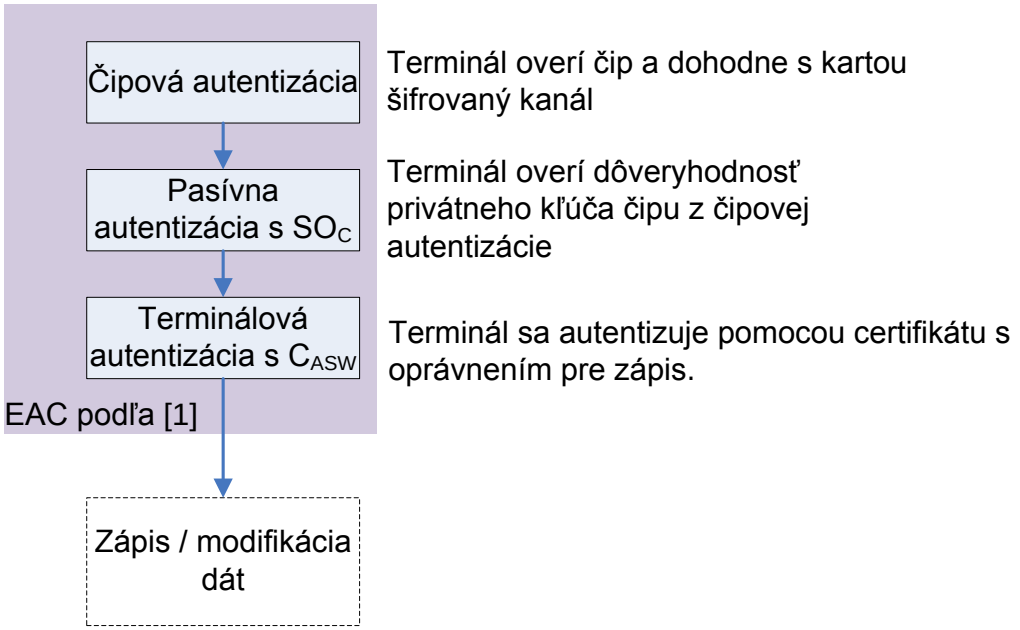
Scenár pre zavedenie novej aplikácie (napr. ZEP alebo AC na RA) do čipu je znázornený na nasledujúcom obrázku:



V tomto prípade sa použije CV certifikát pre autentifikačný systém s oprávnením pre zavedenie novej aplikácie – napr. oprávnenie. Formát CV certifikátu podľa [1] bude špecifikovaný v analytickej fáze dodávky projektu.

6.3.1.6. Autentifikačný Systém – Zápis

Scenár pre zápis dátových skupín (len vybraných) do čipu je znázornený na nasledujúcom obrázku:



V tomto prípade sa použije CV certifikát pre autentifikačný systém s oprávnením pre zápis do vybraných dátových skupín. Formát CV certifikátu podľa [1] bude špecifikovaný v analytickej fáze dodávky projektu.

Navrhovaný Inšpekčný subsystém (obrázok č.4) bude pozostávať:

- klienta inšpekčného systému ktorý zabezpeči:
  - Autentifikáciu s čipom dokladu eID a eDoPP: Overenie autenticity čipu (čipová autentizácia + pasívna autentizácia údajov použitých pri autentizácii), získanie prístupu pre čítanie údajov z čipu (terminálová autentizácia prostredníctvom služieb servera inšpekčného systému), vytvorenie bezpečného komunikačného kanála s kartou (vznikne počas čipovej autentizácie)
  - Vyčítanie údajov z čipu a kontrola voči MRZ
  - Rozhranie pre aplikácie s ktorými sa integruje

- Komunikáciu s čipom dokladu eID a eDoPP
- Autentizáciu voči serveru inšpekčného systému na báze SSL – „Client authenticated SSL session“

- servera inšpekčného systému, ktory poskytuje služby ohľadom autentifikácie s čipom:
  - poskytnutie CSCA a DS certifikátov pre použitie v pasívnej autentifikácii
  - poskytnutie IS a DV certifikátov pre použitie v terminálovej autenttifikácii
  - podpis autentizačných údajov počas vykonania terminálovej autentifikácie, tzn. server bude mať v HSM uložený IS privátny kľúč a IS certifikát
  - autentifikácia klienta na báze SSL – na základe predloženého X509 certifikátu sa pomocou Active Directory identifikuje klient a k nemu prislúchajúci CV certifikát pre terminálovú autentifikáciu -> jeden server môže zastupovať rôzne role podľa rolí jednotlivých klientov špecifikovaných v Active Directory. V prípade, že v IT prostredí, kde bude inšpekčný systém inštalovaný, nebude dostupné Active Directory, bude server inšpekčného systému vykonávať autentizáciu na základe tzv. „Client authenticated SSL session“ a vždy použije rovnaký CV certifikát pre terminálovú autentizáciu.
  - funkcionalitu pre generovanie kľúčového páru IS
  - komunikácia s PKI infraštruktúrou DV CA za účelom
    - vydania certifikátu pre terminálovú autentifikáciu (IS certifikát)
    - získania certifikátov CSCA, CVCA, DV
  - komunikáciu s HSM

6.3.2 Subsystém pre zápis (modifikáciu) údajov na kontaktný čip

Je z pohľadu funkcionality modifikáciou Inšpekčného subsystému a je určený pre modifikáciu a zápis údajov a bude implementovaný podobne ako inšpekčný systém, tzn. bude pozostávať z nasledujúcich komponentov:

Klient, ktorý bude integrovaný s aplikáciou tretej strany, napr. aplikáciou pre JP (jednotné pracoviská). Klient slúži pre

- poskytnutie funkčného rozhrania pre aplikáciu na JP
- otvorenie dokladu pre zápis vykonaním čipovej, pasívnej a terminálovej autentifikácie
- zápis údajov do karty
- komunikáciu so serverom (autentifikácia s čipom dokladu)
- komunikáciu s čipom dokladu eID a eDoPP
- autentizáciu voči serveru na báze SSL – „Client authenticated SSL session“

Server, ktorý má rovnakú funkcionalitu ako server inšpekčného systému z obrázku č. 4. Pre terminálovú autentizáciu sa však použije CV certifikát typu „Autentizačný systém s právom pre zápis“. Zapisovať / modifikovať bude možné len dátové skupiny DG17 až DG21.

6.3.3 Subsystém pre postpersonalizáciu

Postpersonalizácia predstavuje mechanizmus umožňujúci zavedenie ďalšej aplikácie do čipovej karty (napr. aplikácia pre ZEP resp. AC so zápisom pislušných certifikátov na CA/RA) prostredníctvom autentifikácie a bezpečnostného kanálu na báze CV certifikátu a EAC podľa [1] – čipová a terminálová autentifikácia.

Pre tento účel bude použitý IS v autentifikačnom móde, pričom sa použije CV certifikát s príslušnými oprávneniami. V rozsahu tejto ponuky bude dodaný komponent, ktorý pomocou IS na princípe EAC otvorí doklad eID / eDoPP pre postpersonalizáciu.

Samotnú post-personalizáciu však musí vykonať komponent / aplikácia tretej strany (napr. CA/RA). Preto je pre zavedenie a použitie aplikácie pre ZEP, resp. AC, nutný ďalší komponent. Pre použitie certifikátov (ZEP alebo AC) pomocou štandardných mechanizmov a rozhraní je nutné vyvinúť integračný komponent, ktorý klientskym aplikáciám (napr. web prehliadač pre autentifikáciu a nadviazanie zabezpečenej komunikácie alebo aplikácie pre vytváranie ZEP) umožní použitie čipovej karty pre vytváranie elektronického podpisu v ZEP alebo pre autentifikáciu pomocou AC.

Takéto integračné komponenty (sú mimo rozsah tejto ponuky) umožnia aplikáciám tretej strany zaviesť certifikáty do dokladov eID / eDoPP štandardnou cestou, ako aj umožnia použitie dokladov pre autentifikáciu a vytváranie elektronického resp. zaručeného elektronického podpisu.

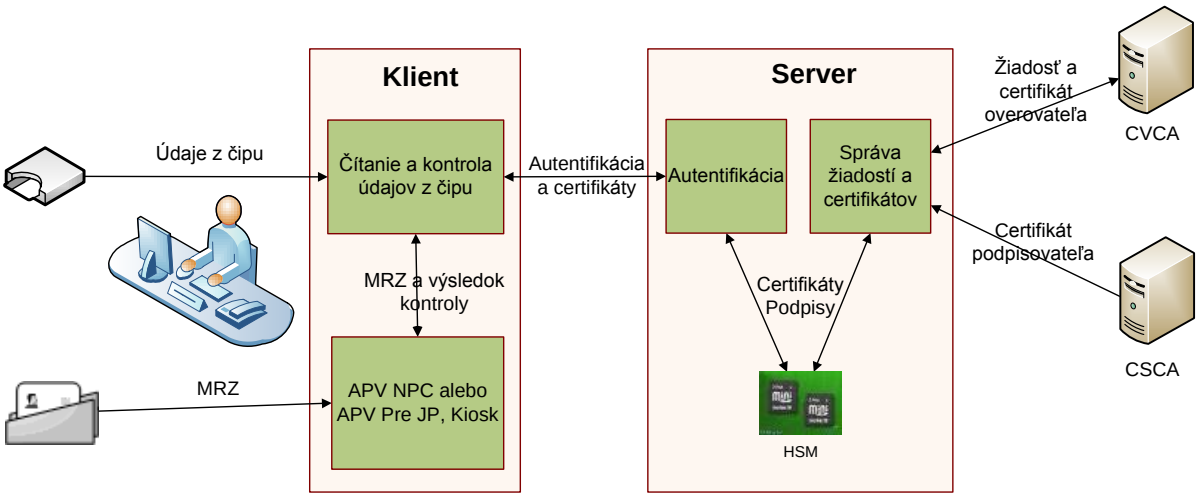
Subsystém pre postpersonalizáciu je z pohľadu funkcionality modifikáciou Inšpekčného subsystému a je určený pre zabezpečenie postpersonalizácie na pracoviskách RA a bude podobne ako inšpekčný systém pozostávať z:

Klienta určeného pre

- poskytnutie funkčného rozhrania pre aplikáciu RA,
- otvorenie dokladu pre zavedenie novej čipovej aplikácie vykonaním CA a TA autentifikácie,
- komunikáciu so serverom (autentifikácia s čipom dokladu),
- autentifikáciu voči serveru na báze SSL

a

Servera, ktorý má rovnakú funkcionalitu ako server inšpekčného systému. Pre terminálovú autentizáciu sa však použije CV certifikát typu „Autentizačný systém s právom pre zavedenie novej aplikácie“. Z hľadiska rozdelenia do komponentov sa v prípade serveru jedná o rovnaký komponent ako je server Inšpekčného systému uvedený na obrázku č.4.



Obrázok č. 4. Komponentová architektúra Inšpekčného subsystému

6.4. PKI infraštruktúra pre zabezpečenie udajov na čipe pre doklady eID a eDoPP

Autentifikačné mechanizmy pre prístup k údajom na čipe dokladu vyžadujú certifikáty a PKI infraštruktúru.

Pasívna autentifikácia zabezpečí ochranu voči pozmeňovaniu údajov na čipe dokladu. Pasívna autentifikácia pozostáva z overenia bezpečnostného objektu dokladu (SO_c). Bezpečnostný objekt dokladu (SO_c) obsahuje zahašovanú podobu dátového objektu a je digitálne podpísaný privátnym kľúčom podpisovateľa dokladu (DS).

Táto technológia je založená na infraštruktúre verejných kľúčov (PKI) a je implementovaná ako Country Signing Certification Authority - CSCA. Bude použitá externá Certifikačná autorita (CSCA) krajiny generuje súkromné a verejné kľúče pre podpisovateľa dokladov. Ďalej, súkromný kľúč CSCA krajiny je použitý na podpísanie certifikátu podpisovateľa dokladov (DS). Off-line rozhranie modulu HSM na CSCA krajiny je súčasťou navrhovaného riešenia. Požadovaný režim PKI z hľadiska pravidiel (procedúr) ako aj hardvérové a softvérové moduly (zahŕňajúc HSM na uchovávanie a generovanie kľúčov) sú v súlade s požiadavkami uvedenými s relevantnými štandardami pre oblasť elektronických dokladov. CSCA PKI infraštruktúra pre eID a eDoPP bude implementovaná iba rozšírením pôsobnosti existujúcej externej CSCA PKI infraštruktúry inštalovenej v NBU. Navrhujeme teda CSCA pre eTP rozšíriť o vydávanie DS certifikátov pre eID a pre eDoPP. CSCA bude umiestnená a prevádzkovaná na NBÚ.

Zabezpečenie prístupu k údajom na čipe dokladov eID a eDoPP bude mechanizmom tzv. rozšíreného riadenia prístupu (Extended Access Control, EAC). EAC pozostáva z CA a TA a silne zabezpečeného údajového kanálu pre prenos údajov z/do čipu. EAC systém je navrhnutý na základe kryptografických mechanizmov overovania

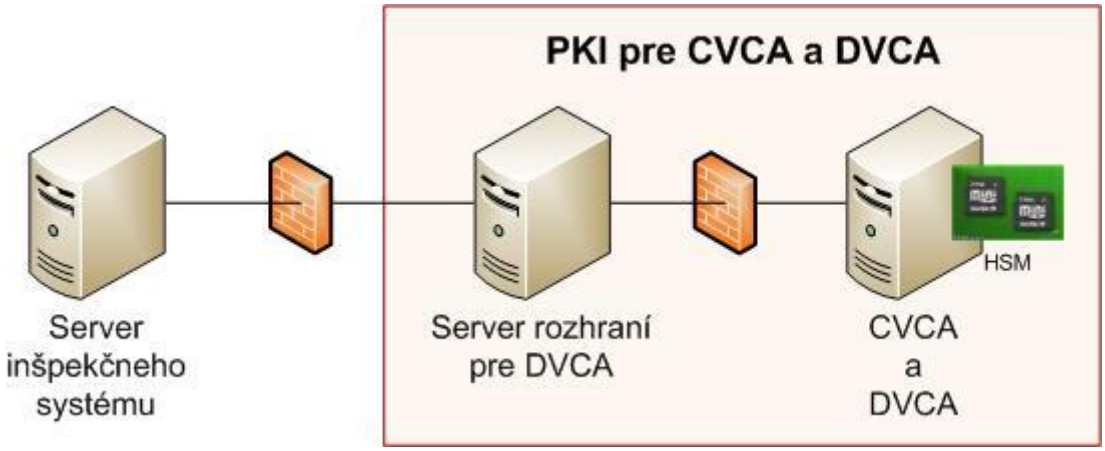
prístupov k údajom, jadrom systému je PKI infraštruktúra, ktorá zaručuje bezpečnú certifikáciu komunikujúcich strán na základe certifikátov CVC a priradzuje im konkrétne prístupové práva pre prístup k jednotlivým údajovým skupinám (DG) na eID a eDoPP.

EAC PKI bude v súlade medzinárodnými štandardami zavedenými pre biometrické cestovné doklady a ekvivalentná technológia bude postavená aj pre riadenie prístupu pre eID a eDoPP dokumenty. Hlavným riadiacim štandardom je Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 2.0 alebo Version 1.1.

Systém EAC má trojvrstvovú hierarchickú organizáciu, v ktorej sú smerom zhora nadol delegované práva pre podriadené úrovne pre prístup k jednotlivým údajom eID a eDoPP. Vrcholom hierarchie EAC je štátna certifikačná autorita pre overovanie – Country Verifying Certification Authority CVCA. Jej sú podriadené certifikačné autority pre overovanie dokumentov – Document Verifying Certification Authority DVCA, ktoré buď geograficky alebo funkčne určujú prístupové práva. Najnižším stupňom hierarchie sú jednotlivé pracoviská pre overovanie eID a eDoPP, vybavené tzv. inšpekčnými systémami – IS alebo terminálmi.

Certifikačné autority CVCA a DVCA budú vybudované použitím štandartných modulov riešenia Verizon Business UniCERT, ktorá bola použitá aj pre slovanské biomentické pasy, s implementáciou rozšírení pre správu CVC formátu certifikátov potrebných pre eID/eDoPP EAC PKI ako je definovaná v medzinárodných štandardoch.

Technická architektúra realizácie CVCA a DVCA pre eID a eDoPP dokumenty je znázornená na nasledujúcom obrázku. CVCA a DVCA budú realizované ako dve funkčne oddelené certifikačné autority v chránenom prostredí a so silnou ochranou kryptografických kľúčov umiestnených na tzv. HSM – hardvérových moduloch. Navrhované HSM moduly - nCipher nShield F3 500 HSM sú certifikované na úroveň EAL4+ podľa Common Criteria evaluation. Komunikáciu pre certifikačné procesy pre Inšpekčné systémy bude zabezpečovať vysunutý modul "Server rozhraní" poskytujúci http/https služby a chránený dvojicou firewallov. Administrátorské rozhranie pre operátorov certifikačných autorít (CAO) bude dostupné na systémoch CVCA a DVCA a bude zabezpečné dvojfaktorovou autentifikáciou čipovými kartami.



Obrázok č. 5. EAC PKI infraštruktúra

Táto EAC PKI infraštruktúra určená pre kontrolu prístupu k eID a eDoPP bude vybudovaná ako nová inštancia a bude inštalovaná v SITB.

7. Návrh (dizajn) APV

Návrh APV Personalizačného systému bude tvorený z nasledovných súčastí:

- Dizajn zmien APV pre riadenie personalizácie a logistiky výroby dokladov ID-1

- Dizajn zmien ePerso
- Dizajn zmien Inšpečného/autenfifikačného subsystému

7.1. Dizajn zmien APV pre riadenie personalizácie a logistiky výroby dokladov ID-1

Návrh zmien komponentov systému a používateľských rozhraní (ďalej len „Návrhu (dizajn) zmien APV“) bude vyhotovený na základe Analýzy požiadaviek na zmenu APV pre doklady elektronický OP a DoPP.

Návrh (dizajn) zmien APV bude:

- zaisťovať, čo najvyššiu mieru opakovaného použitia existujúcich komponentov použitých pre personalizáciu existujúcich typov dokladov
- štandardizovať vzhľad a správanie vyvíjaných častí APV
- špecifikovať zmeny funkčnosti tak, aby bolo možné zavedenie dokladov elektronického OP a elektronického DoPP

Návrh (dizajn) zmien APV bude definovať potrebné zdroje a metodiku na transformáciu zmien modelov typových úloh do zmien existujúcich návrhových modelov. Transformácia bude urobená do existujúcich návrhových modelov z nasledovných vrstiev architektúry.

Pre vrstvy uvedené vyššie budú v Návrhu (dizajne) zmien APV špecifikované zmeny návrhových modelov, ktoré sa stanú východiskom pre programovú realizáciu. Konkrétne návrhové modely, ktoré budú zmenené na základe Analýzy požiadaviek na zmeny APV spomedzi nasledovných modelov:

- diagramy tried,
- dátový model,
- návrh používateľských rozhraní (obrazovky).

Návrh (dizajn) zmien APV bude tiež špecifikovať zmeny existujúcich komponentov systému ako aj zmeny existujúcich používateľských rozhraní a rozhraní na externé kooperujúce systémy.

7.2. Dizajn zmien ePerso

Návrh zmien komponentov systému (ďalej len „Návrhu (dizajn) zmien APV“) bude vyhotovený na základe Analýzy požiadaviek na zmenu ePerso pre nové doklady elekronický OP a DoPP.

Návrh (dizajn) APV bude špecifikovať najmä vyvíjané komponenty subsystému ePerso pre zápis (personalizáciu) kontaktného čipu pre vybranú platformu OS pre doklady eID a eDoPP a podľa popisu funkcionality tak ako je uvedené v predošlom texte.

APV personalizácie čipu (ePerso) bude obsahovať tieto komponenty:

- Komponent na personalizáciu čipu – generuje príkazy pre zápis dátovej štruktúry LDS. Na komunikáciu s čipom počas jeho personalizácie, získava podpis na object SO_c od komponentu eSIGN-HSM
- eSIGN-HSM bude využitý komponemt vyvinutý v rámci dodávky projektu OoE. Prostredníctvom funkcií HSM modulu a kľúčového páru podpisovateľa dokladov (DS) generuje bezpečnostný objekt (SO_c).
- Komponent na správu žiadostí a certifikátov – generuje kľúčový pár a žiadosť o certifikát podpisovateľa dokladov (DS), importuje certifikát DS do HSM. Bude prepoužity komponent vyvinutý v rámci dodávky projektu OeE.

Ďalšie komponenty súvisiace s APV personalizácie čipu (ePerso):

- Manažér personalizačného zariadenia (Syntera) – je jednotným rozhraním pre moduly na komunikáciu s kontaktným čipom od výrobcu personalizačného zariadenia.
- Off line rozhranie na Národnú certifikačnú autoritu (CSCA) – slúži na výmenu žiadosti o certifikát a certifikátu medzi národnou certifikačnou autoritou a personalizačným pracoviskom.

- Online rozhranie na CVCA, DVCA.

7.3. Dizajn zmien Inšpekčného/autentifikačného sybsystému

Návrh zmien komponentov systému a používateľských rozhraní (ďalej len „Návrhu (dizajn) zmien APV“) bude vyhotovený na základe Analýzy požiadaviek na zmenu na APV na kontrolu pre elektronický OP a eDoPP. Pre kontrolu dokladov bude APV resp. jeho komponenty navrhnuté tak, aby boli použiteľné pre kontrolu dokladov vydávaných v rezorte MV. Súčasný inšpekčný systém bude rozšírený tak, aby umožňoval aj kontrolu nových typov dokladov eID a eDoPP. Vybudovaním takéhoto Inšpekčného systému vznikne Jednotný inšpekčný systém ako univerzálna platforma pre kontrolu dokladov vydávaných v rámci kontroly dokladov na Jednotných pracoviskách v Personalizačných centrách a na Kioskoch. Oprávnenie pracovníka (resp. inšpekčného terminálu) pre vykonávanie kontroly dokladov eID resp. eDoPP bude riadené prostredníctvom služieb servera Jednotného inšpekčného systému prepojeného na správu používateľov LDAP.

Dizajn APV bude zaisťovať, čo najvyššiu mieru opakovaného použitia už existujúcich komponentov a špecifikovať návrh funkcionality tak, aby APV (jeho komponenty) bolo preložiteľne pri požadovaných inšpekčných procedúrach rezortu MV (personalizačne centra, JP, Kiosky). APV bude navrhnuté pre nasledovné účely:

- Pre prostredie hrubého klienta pre účel kontroly po personalizácii v Personalizačnom systéme. V tomto prípade bude APV inšpekčného systému (jeho klient) integrované do nadradenej aplikácie (APV pre riadenie personalizácie a logistiky výroby dokladov).
- Pre nšpekčný systém na JP (jednotné pracoviská) a pre Kiosky. V tomto pripade bude APV (jeho klient) integrované do príslušných aplikácii.
- Pre pracoviská RA na vykonanie postpersonalizácie (zavedenie ZEP aplikácie a certifikátov) a prípadne zmenu údajov vo vybraných dátových grupách DG na čipe dokladu.

8. Implementácia APV

Implementácia zmien APV navrhovaného systému bude tvorená z nasledovných súčasti:

- Implemenácia zmien APV pre riadenie personalizacie a logistiky výroby dokladov ID-1
- Implementácia zmien (ePerso) subsystému
- Implementácia zmien Inšpekčného/autentifikačného subsystému

Na základe schváleného návrhu dizajnu zmien APV a preferovaného technologického prostredia (.NET) budú implementované navrhnuté zmeny komponentov APV resp. nové komponenty. Perzistentná údajová vrstva bude implementovaná v prostredí MS SQL servera.

Budú implementované rozšírenia APV vyplývajúce zo špecifikácie (analýzy) požiadaviek na rozšírenie funkcionality a z návrhu (dizajnu) zmien APV.

Implementácia zmien APV bude uskutočnená tak, aby boli skompilované a otestované komponenty APV nasaditeľné do riadnej rutinnej prevádzky. Klient komponent APV Inšpekčného/autentifikačného systému bude implementovaný ako ActiveX komponent pre jednoduchú integráciu do cieľových prostredí v rámci rezortu MV. Testovanie APV a jeho jednotlivých súčastí bude vykonané na základe návrhu testovacích procedúr a scenárov, ktoré budú špecifikovať unit a integračné testy. Výsledkom tejto aktivity bude otestované APV nasaditeľné do rutinnej prevádzky.

Poznámka. Implementácia APV a IT infraštruktury pre pracoviská RA nie je predmetom tejto ponuky, Preto nie je v tomto čase možné špecifikovať spôsob integrácie a implementáciu autentifikačného subsystému (zapis, postpersonalizácia) do APV pre RA.

Súčasťou tejto časti je realizácia EAC PKI infraštruktúry - inštalácia HW, SW, konfigurácia APV. Implementácia testovacieho prostredia, inštalácia a konfigurácia testovacej CVCA a DVCA.

9. Záložné personalizačné centrum (personalizačné zariadenia)

Personalizačný systém dokladov ID-1 bude navrhnutý tak, aby existujúce typy dokladov vydávané v pôsobnosti rezortu MV:

- Vodičský preukaz
- Povolenie na malý pohraničný styk

A nové typy elektronických dokladov s kontaktnými čipmi:

- Elektronický OP (eID)
- Elektronické osvedčenie o evidencii vozidla OoE I
- Elektronický DoPP (eDoPP)

mohli byť personalizované paralelne. Každé personalizačné zariadenie bude schopné personalizovať ktorýkoľvek z vyššie uvedených typov dokladov.

Personalizačný systém záložného personalizačného centra pre personalizaciu ID1 dokladov, bude vybavený 3 zhodnými personalizačnými zariadeniami MX6000 spoločnosti Datacard s nasledovnou konfiguráciou modulov:

- Riadiaci modul (PC a SW pre obsluhu zariadenia a konfiguráciu modulov)
- 2 x modul vstupného zásobníka
- Čítací modul pre OCR
- 2 x zapisovací modul do čipu
- 3 x laserový gravírovací modul
- Výstupný zásobník

Riadiaci modul

Tento modul je povinný v akejkoľvek konfiguracii zariadenia. Riadiaci modul (jeho SW) riadi prácu všetkych ostatných modulov personalizačného zariadenia. Obsahuje konzolu, prostredníctvom ktorej obsluha zadáva povely na personalizáciu dávok dokladov alebo vykonáva konfiguráciu modulov personalizačného zariadenia.

2 x modul vstupného zásobníka

Modul vstupného zásobníka sa skladá z dvoch vstupných podávačov, z ktorých je zariadenie napĺňané dokladmi. Špecifikácia a hlavné charakteristiky:

- Kapacita vstupných zásobníkov je 2 x 550 dokladov (ID-1)

Čítací modul pre OCR

Modul zabezpečí načítanie OCR-B čísla na čistopise dokladu. Oblasť s číslom dokladu je zosnímaná kamerou a prostredníctvom OCR softvéru je v nej rozpoznané číslo. Po prečítaní/rozpoznaní je číslo dokladu odovzdané riadiacemu modulu personalizačného zariadenia na ďalšie spracovanie.

2 x zapisovací modul do čipu

Modul vykonáva inicializáciu/zápis údajov do čipu, ktorý je zaintegrovaný do čistopisu dokladu. Zapisovací modul do čipu sa skladá z modulu na zápis do kontaktného čipu a z modulu na zápis do bezkontaktného čipu. Každý modul je vybavený štyrmi zapisovacími pozíciami umožňujúcimi paralelnú personalizáciu čipov dokladov. Pre prípadné potreby zvýšenia priepustnosti je modul rozširiteľný o ďalšie zapisovacvie hlavy. Moduly na zápis do čipu môžu prostredníctvom riadiaceho modulu personalizačného zariadenia a siete komunikovať s externými zariadeniami (napr. iný server, HSM).

Špecifikácia a hlavné charakteristiky:

- Modul pre zápis do kontaktného čipu
    - Podpora rozhrania pre komunikáciu s kontaktným čipom podľa ISO 7816.
    - 8 zapisovacích hláv

- Rozširiteľnost o ďalšie zapisovacie hlavy
- Modul pre zápis do bezkontaktného čipu
  - Podpora rozhrania pre komunikáciu s bezkontaktným čipom podľa ISO 14443
  - 4 zapisovacie hlavy
  - Rozširiteľnosť o ďalšie zapisovacie hlavy

3 x laserový gravírovací modul

Tento modul personalizuje texty rôznych veľkostí a fontov, fotografie, čiarové kódy, čiernobiele logá a ďalšie grafické prvky technológiou laserového gravírovania. Medzi ďalšie podporované funkčnosti patrí zameriavanie (vision registration) pre správne zarovnanie personalizovaných elementov voči elementom alebo zameriavacim značkám predtlačeným na čistopise, obracanie dokladu priamo v module pre personalizáciu oboch strán dokladu a personalizáciu bezpečnostných prvkov pomocou technológie gravírovania z rôznych uhlov. V prípade potreby zvýšenia priepustnosti je systém možné v budúcnosti rozšíriť o ďalšie laserové gravírovacie moduly.

Špecifikácia a požadované charakteristiky:

- Pevný laser triedy 1
- Umožnuje hmatateľné (na povrchu dátovej strany), ale aj nehmatateľné (prejaví sa len vo vrstve dátovej strany citlivej na laser) gravírovanie
- Zameriavacia funkcionalita na správne zarovnanie personalizovaných elementov voči elementom predtlačeným na čistopise dokladu
- Integrovaný obracač pre personalizáciu oboch strán dokladu v jednom module
- Rozšírená záruka na 5 rokov

Modul výstupného zásobníka

Výstupný zásobník uchováva personalizované doklady. Obsahuje dve osobitné dráhy na ukladanie dokladov. Jedna dráha uchováva úspešne personalizované doklady a druhá dráha uchováva vyradené doklady a nepodarky.

Špecifikácia a hlavné charakteristiky:

- Dve dráhy na ukladanie dokladov
- Kapacita 2 x 495 dokladov (ID-1)

Obrázok 6: Konfigurácia personalizačného zariadenia MX6000

Požadovaný ročný výkon (250 dní x 7,5 hodín) jedného personalizačného zariadenia bude dosahovať aspoň 400.000 personalizovaných ID-1 dokladov. Platí pre všetky typu dokladov ID-1 v súčasnosti vydávaných v pôsobnosti MV SR a vizuálny typ personalizácie. Potom smenovy výkon (smena je 7,5 hod.) na jedno zariadenie je aspoň 1660 dokladov.

Personalizačný systém bude spôsobilý na zvýšenie kapacity a to najmä, nie však výlučne, pridaním ďalšej smeny alebo predĺžením už zavedenej smeny (v dôsledku čoho bude možné dosiahnuť až dvojnásobnú kapacitu Personalizačného systému), alebo pridaním ďalšieho personalizačného zariadenia do Personalizačného systému.

10. Podpora skartácie ID1 dokladov (čítacie zariadenie)

Doklady po skončení svojej platnosti alebo aktuálnosti údajov budu zasielané späť na personalizačné pracovisko za účelom ich fyzickej skartácie. Pred vykonaním skartácie je nevyhnutné skontrolovať čísla na samotných dokladoch voči elektronickej evidencii. Kedže v budúcnosti sa predpokladá veľký objem dokladov prichádzajúcich na skartáciu (rovnajúci sa približne množstvu personalizovaných dokladov) a manuálne vykonávanie kontroly čísiel voči zoznamom by bolo nespolahlivé a neefektívne je potrebné podporiť túto činnost automatizáciou.

Čítacie zariadenie ID-1 dokladov bude slúžiť na automatické čitanie skupín ID-1 dokladov určených na skartáciu a tým bude táto činnosť pre obsluhu zjednodušená a chybovosť minimalizovaná.

Ako čítacie zariadenie ID-1 dokladov bude použité zariadenie MX2000 od spoločnosti Datacard, ktorého modulová konfigurácia bude nasledovná:

- Riadiaci modul
- Vstupný zásobník
- Čitací modul pre OCR (predná strana ID-1 dokladu)
- Čitací modul pre MRZ (zadná strana ID-1 dokladu)
- Výstupný zásobník

Riadiaci modul

Riadiaci modul personalizačného zariadenia riadi prácu všetkych ostatnych modulov. Obsahuje konzolu prostredníctvom, ktorej obsluha zadáva povely na personalizáciu dávok dokladov alebo vykonáva konfiguráciu software a modulov personalizačného zariadenia.

Modul vstupného zásobníka

Modul vstupného zásobníka obsahuje vstupný podávač, z ktorého si zariadenie automatocky odoberá doklady na spracovanie. Špecifikácia a hlavné charakteristiky:

- Kapacita vstupného zásobníka je 550 dokladov (ID-1)

Čítací modul pre OCR

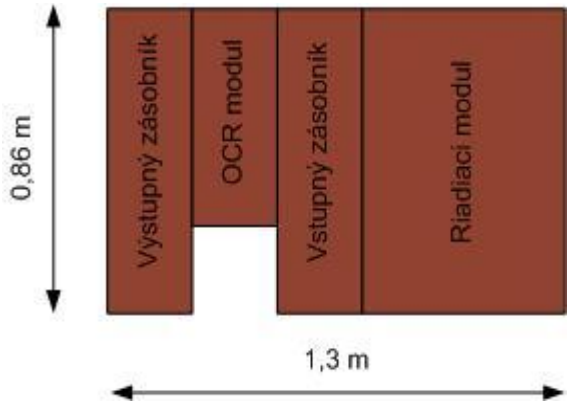
Modul zabezpečí načítanie OCR-B čísla na doklade. Oblasť s číslom dokladu je zosnímaná kamerou a prostredníctvom OCR softvéru je v nej rozpoznané číslo. Po prečítaní/rozpoznaní je číslo dokladu odovzdané riadiacemu modulu čítacieho zariadenia.

Modul výstupného zásobníka

Výstupný zásobník uchováva spracované doklady. Obsahuje dve osobitné dráhy na ukladanie dokladov. Jedna dráha uchováva doklady úspešne spracované/prečítané a druhá dráha doklady vyradené.

Špecifikácia a hlavné charakteristiky:

- Dve dráhy na ukladanie dokladov
- Kapacita 2 x 495 dokladov (ID1)



Obrázok 7: Konfigurácia čítacieho zariadenia MX2000

11. Externé rozhrania Personalizačného systému

11.1. Rozhranie na objednovkový systém IIS SA

Zaslanie objednávky na personalizáciu dokladov do Záložného centra

Navrhované riešenie (jeho APV) iniciuje proces zaslania objednávky na personalizáciu. Systém IIS SA v prípade, že má zaevidovanú objednávku, pre ktorú nebolo zrealizované potvrdenie prevzatia vygeneruje výstupné XML z tejto objednávky. Inak vytvorí novú objednávku a zaradí do nej požadovaný počet dokladov. Na základe objednávky následne vygeneruje výstupné XML.

Potvrdenie prevzatia objednávky na personalizáciu dokladov

Po prijatí objednávky Personalizačný systém iniciuje proces potvrdenia objednávky. V prípade úspešného prijatia objednávky systém NPC zašle ako vstupné XML potvrdenie objednávky, inak systém NPC zašle ako vstupné XML zamietnutie objednávky.

Pripravenosť dokladov na distribúciu

Po skontrolovaní kvality dokladov výrobnej dávky Personalizačný systém iniciuje proces informovania o pripravenosti dokladov na distribúciu. V rámci vstupného XML sú zaslané informácie o čísle dokladu a čísle balíka, v ktorom bude doklad doručený na príslušný JP. Súčasťou vstupného XML bude aj číslo kartičky (čistopisu). Po spracovaní vstupného XML vygeneruje systém IS SA ako odpoveď výstupné XML, ktoré pre každý doklad z vstupného XML obsahuje dohodnutý status spracovania.

Prevzatie balíka kuriérom

Po prevzatí balíka kuriérom Personalizačný systém iniciuje proces informovania o distribuovaní dokladov z Personalizačného centra. V rámci vstupného XML je zaslané číslo distribuovaného balíku.

Potvrdenie prevzatia balíka dokladov na JP

Personalizačný systém v definovaných intervaloch overuje stav distribuovaného balíka dokladov.

Zaslanie skartačných zoznamov

Personalizačný systém iniciuje zaslanie skartačných zoznamov systémom IIS SA. Vo vstupnom XML zašle dátum a čas zaslania balíka - vo význame posledný dátum a čas ktorý bol uvedený na posledne zaslanom skartačnom balíku. Systém IIS SA poskytne všetky skartačné zoznamy, ktorých dátum a čas vytvorenia je väčší (mladší) ako vstupný parameter.

Potvrdenie prevzatia dokladov na skartáciu

Personalizačný systém iniciuje potvrdenie prevzatia dokladov na skartáciu. Vo vstupnom XML pre každý doklad zaradený do identifikovaného skartačného zoznamu, zašle informáciu o spôsobe jeho prevzatia na skartáciu.

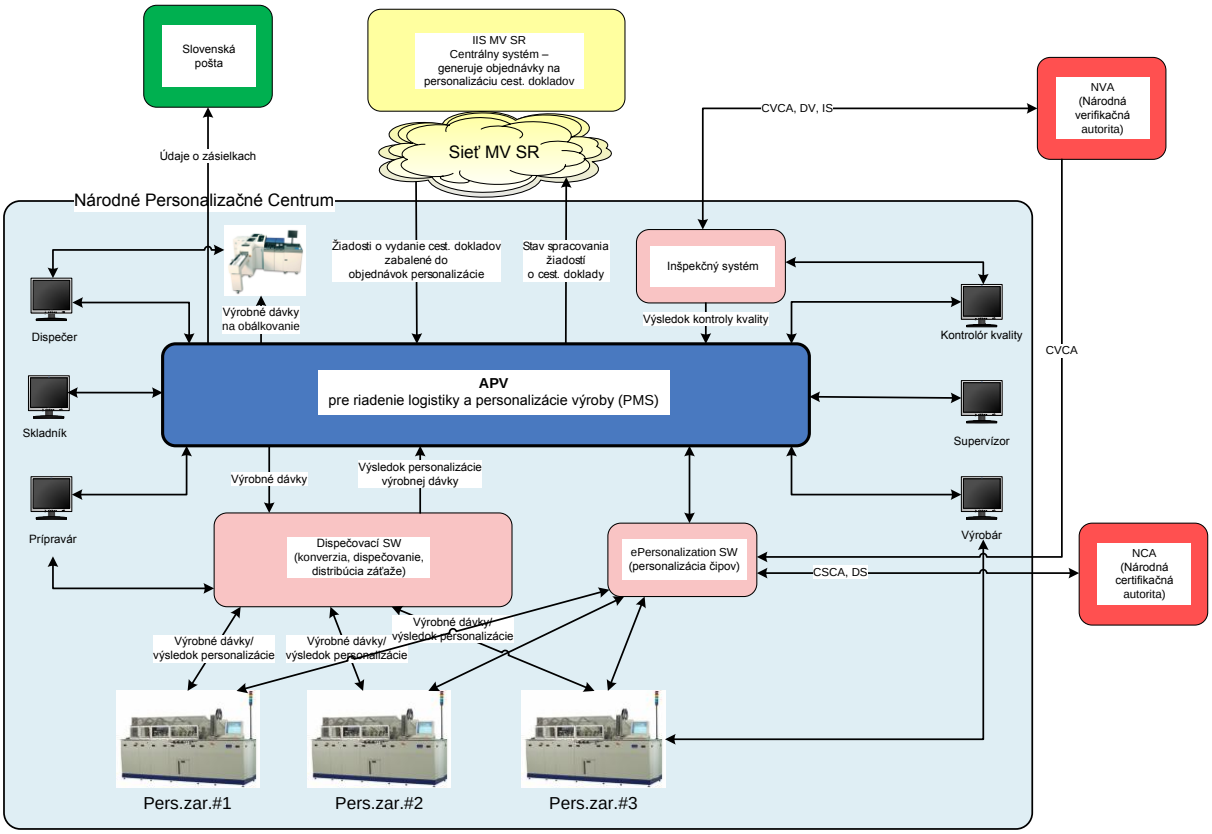
Potvrdenie skartácie dokladov

Personalizačný systrém iniciuje potvrdenie skartácie dokladov pre systém IS SA. Vo vstupnom XML zašle číslo balíku, ktorého doklady boli fyzicky skartované.

11.2. Rozhrania na Národnú certifikačnú autoritu

Národná certifikačná autorita krajiny (NBU) generuje súkromné a verejné kľúče pre tzv. rootový (selfsigned) certifikát CSCA. Súkromný kľúč CSCA krajiny je použitý na podpísanie certifikátu podpisovateľa dokladov (DS) pre eID a eDoPP.

Prostredníctvom off-line rozhranie APV pre riadenie personalizácie a logistiky výroby dokladov v Personalizačnom centre na CSCA krajiny je zaslaná žiadosť o nový certifikát DS a následne je pomocou tohto rozhrania nahratý nový certifikát DS do Personalizačného systému.



Obrázok č. 8. Personalizačný systém s rozhraniami

12. Aktualizácia pracovných rolí a procedúr

Aktualizácia dokumentu Pracovné role a procedúry v rámci projektu pre zavedenie eID a eDoPP bude zahŕňať nasledovné doplnenia a úpravy:

Nadefinovanie pracovných rolí a procedúr pre Záložné Personalizačné centrum, pričom tieto pracovné role a procedúry budú vychádzať z existujúcich a overených pracovných rolí a procedúr v Personalizačnom centre.

Dodefinovanie pracovných postupov súvisiacich s prerozdelením zodpovedností a zdieľaním pracovného zaťaženia medzi Personalizačným centrom a Záložným personalizačným centrom. Ide najmä o činnosti súvisiace so skladovaním a evidenciou čistopisov, presunmi čistopisov medzi oboma centrami, presunmi dokladov na reklamáciu a skartáciu a koordináciou reklamačných a skartačných procesov.

Prerozdelenie a dodefinovanie zodpovedností a pracovných úkonov Prípravára a Supervízora v dôsledku zavedenia skladu v Záložnom Personalizačnom centre.

Stanovenie pracovných rolí a procedúr pre prípad havarijných stavov s potrebou presunu personalizácie medzi Personalizačným centrom a Záložným personalizačným centrom.

13. Aktualizácia bezpečnostného zámeru, Analýza bezpečnosti, Bezpečnostná smernica

Dodávka bezpečnostného projektu bude obsahovať najmä tieto časti:

- bezpečnostný zámer (míľnik1),
- analýzu bezpečnosti (míľnik 2),
- bezpečnostnú smernicu (míľnik3),
- a bude vyhotovený v zmysle a za podmienok uvedených nižšie.

Bezpečnostný projekt musí najmä:

- obsahovať všetky náležitosti podľa zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov a ďalších právnych predpisov Slovenskej republiky
- obsahovať podrobnú špecifikáciu a poradie všetkých úkonov v rámci technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na Personalizačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti,
- obsahovať návrh komplexného riešenia bezpečnosti APV Personalizačného systému pokrývajúci:
- zaznamenávanie všetkých činností v APV Personalizačného systému (vyhodnocovanie),
- ochranu dát pred neoprávneným prístupom,
- ochranu pred neoprávneným používaním alebo zneužitím Personalizačného systému,
- zabezpečenie bezpečnej komunikácie konkrétnych pracovísk s APV Personalizačného systému,
- správu užívateľov a účtov dodaného APV,
- umožňovať efektívne fungovanie Personalizačného systému z hľadiska času, finančných nákladov, počtu potrebných zamestnancov objednávateľa a nesmie obmedzovať riadnu prevádzku Personalizačného systému podľa Zmluvy,
- zohľadniť v analýze riziká identifikované počas prevádzky existujúceho personalizačného pracoviska/systému cestovných a identifikačných dokladov,
- byť efektívne rozšíriteľný v prípade práce s novými typmi dokladov na personalizačnom pracovisku,
- zohľadňovať certifikačné činnosti súvisiace s technológiou personalizačného systému,
- zohľadniť nároky na havarijné plánovanie spojené s personalizačným systémom,
- zohľadniť požiadavky na spoľahlivosť expresného vybavovania žiadostí,
- zohľadniť požiadavky na bezpečné zavedenie iných typov personalizačných zariadení do Personalizačného systému,

Bezpečnostný projekt bude vypracovaný v súlade s požiadavkami zákona NR SR č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov ohľadom týchto typov Dokladov:

- elektronického Občianskeho preukazu na báze hrubého polykarbonátu s kontaktným čipom (eID)
- elektronického Dokladu o povolení na pobyt na báze hrubého polykarbonátu s kontaktným čipom (eDoPP)

Bezpečnostný projekt bude vypracovaný aj v súlade s medzinárodnými normami a štandardami ISO/IEC 13335, ISO 27 005:2008 a ISO 27001:2005 a ISO 27002:2005 (bývalá norma ISO 17799), ktoré určujú vyžadované (ako aj odporúčané) praktiky v oblasti riadenia systémov ochrany informačných systémov a údajov.

Bezpečnostný zámer

Pri vyhotovovaní bezpečnostného zámeru vykoná zhotoviteľ v potrebnom rozsahu najmä nasledovné činnosti:

- Inicializácia projektu, predstavenie cieľov a fáz projektu,
- Definícia projektového tímu,
- Určenie rozsahu participácie projektového tímu (konzultácie, poskytovanie informácií, pripomienkovanie výstupov projektu,
- Získanie podkladov, vrátane analýzy stavu informačnej bezpečnosti, stavu implementovaných bezpečnostných opatrení, analýza bezpečnostných vlastností implementovaných aplikácií, s tým spojených

procesov a organizácie personalizačného pracoviska

- Identifikácia prebiehajúcich spracovaní osobných údajov,
- Analýza a vyhodnotenie podkladov,
- Formulácia základných bezpečnostných cieľov.
- Časť Bezpečnostného projektu označená ako bezpečnostný zámer bude obsahovať najmä:
- formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia,
- vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,
- vymedzenie hraníc určujúcich množinu zvyškových rizík.

Analýza bezpečnosti

Pri vyhotovovaní Analýzy bezpečnosti informačného systému budú v potrebnom rozsahu vykonané najmä nasledovné činnosti:

- vypracovanie analýzy rizík a zoznamu hrozieb,
- vypracovanie návrhu bezpečnostných opatrení.

Časť Bezpečnostného projektu označená ako Analýza bezpečnosti informačného systému bude obsahovať najmä:

- vysvetlenie aplikovanej metodiky určenia rizík
- kvalitatívnu analýzu rizík, ktorá predstavuje určenie rizika s ohľadom na identifikované aktíva, na ktoré pôsobia hrozby s identifikovanou pravdepodobnosťou pri definovaných dopadoch
- identifikáciu aktív, ktoré boli zohľadnené v rámci analýzy rizík
- zoznam identifikovaných hrozieb pre identifikované aktíva,
- návrh opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík,
- súpis nepokrytých rizík z pohľadu ochrany osobných údajov,
- použitie bezpečnostných štandardov a určenie iných metód a prostriedkov ochrany osobných údajov,
- posúdenie zhody a miery implementácie navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardmi, metódami a prostriedkami.

Klasifikácia rizík použitá zhotoviteľom pri vypracovaní Bezpečnostného projektu bude mať nasledovné významy:

- A – bezpečnostné opatrenie k riziku musí byť prijaté
- B – bezpečnostné opatrenie k riziku by malo byť prijaté
- C – riziko musí byť priebežne monitorované
- D – opatrenie sa nevyžaduje

Bezpečnostný projekt bude obsahovať navrhované bezpečnostné opatrenia priradené k jednotlivým rizikám a „vlastníkov“ týchto opatrení.

Jednotlivé riziká uvedené v rámci Bezpečnostného projektu budú zhotoviteľom vyjadrené formou nasledovnej tabuľky:

ID	Identifikátor
Aktívum	Aktíva, na ktoré sa identifikované riziko vzťahuje
Hrozba	Identifikované ohrozenia aktív
Dopad	Identifikácia miery dopadov na uvedené aktíva pri realizácii hrozieb Dopad môže byť nízky, stredný alebo vysoký
Pravdepodobnosť	Identifikácia miery pravdepodobnosti, s akou môžu byť hrozby realizované Pravdepodobnosť môže byť nízka, stredná alebo vysoká
Zraniteľnosť	Popis identifikovanej zraniteľnosti vzhľadom na špecifické okolnosti systému informačnej bezpečnosti

ID	Identifikátor
Riziko	Označenie kategórie rizika (A-D). Riziko je určené na základe pravdepodobnosti hrozieb a dopadov aktív so zohľadnením aktuálnej zraniteľnosti systému
Opatrenia	Špecifikácia existujúcich alebo potrebných opatrení informačnej bezpečnosti, ktoré eliminujú výskyt, pravdepodobnosť alebo dopad rizík
Miera uplatnenia	Miera uplatnenia existujúceho alebo potrebného opatrenia, ktorým sa transformuje riziko na reziduálne (zostatkové) riziko.
Zvyškové riziko	Identifikácia zvyškového rizika po zohľadnení opatrení
Odporúčania	Odporúčania pre ďalšiu elimináciu rizík pre dosiahnutie miery zvyškového Rizika určeného v bezpečnostnom zámere.

Forma tabuľkového vyjadrenia rizík môže byť na základe výsledkov analytických prác upravená tak, aby riziko charakterizovala adekvátnym spôsobom,

Bezpečnostné smernice

Pri vyhotovovaní Bezpečnostnej smernice budú v potrebnom rozsahu vykonané najmä nasledovné činnosti:

- spracovanie bezpečnostnej smernice,
- zaškolenie zodpovedných osôb,
- konzultácie k výsledkom bezpečnostného projektu.
- Bezpečnostná smernica, ktorá bude súčasťou Bezpečnostného projektu bude obsahovať:
- Popis technických, organizačných a personálnych opatrení vymedzených v Bezpečnostnom projekte a ich využitie v konkrétnych podmienkach pri zohľadnení špecifík informačného systému,
- štruktúru a rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, návrh spôsobu ich identifikácie a autentifikácie pri prístupe k informačnému systému pri zohľadnení špecifík informačného systému,
- štruktúru a rozsah zodpovedností oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,

návrh spôsobu, formy a periodicity výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému so zohľadnením špecifík informačného systému,

Štruktúra a obsahová náplň smerníc bude v potrebnom rozsahu prispôsobená existujúcej predpisovej základni objednávateľa, pokiaľ bude zhotoviteľovi zapožičaná zo strany objednávateľa v čase nevyhnutne potrebnom na riadne a včasné splnenie povinností zhotoviteľa podľa Zmluvy.

14. Školenia

Zhotoviteľ poskytne zamestnancom objednávateľa školenia pre používanie a správu Personalizačného systému (t.j. na všetky dodávané aplikačné programové vybania – Personalizačný systém, ePerso a Inšpekčný systém a personalizačné zariadenia) za nasledujúcich podmienok:

Miesta školení:

školiace pracoviská objednávateľa, ktoré budú oznámené zhotoviteľovi najneskôr 3 pracovné dni pred začatím príslušného školenia,

Jazyk školenia:

slovenský a/alebo formou prekladu z anglického do slovenského jazyka.

V rámci aktivity Školenie objednávateľ okrem toho, že zrealizuje vlastné školenia zamestnancov objednávateľa podľa špecifikácií nižšie, vykoná všetky činnosti spojené s prípravou a vyhodnotením školení. Zhotoviteľ pripraví školiacu dokumentáciu, ďalej pripraví na školenie systémy (t.j. personalizačné zariadenia, PMS (Personalizačný Management System), ePerso – aplikáciu pre zápis dát do čipu, Inšpekčný systém), v systémoch pripraví dáta pre školenia, vytvorí užívateľské a administrátorské kontá v systémoch.

Po vlastnej realizácii školení vyhodnotí školiteľ spätnú väzbu účastníkov školenia na funkcionalitu a kvalitu APV.

Školiteľ zabezpečí praktické cvičenia pre zamestnancov objednávateľa na školiacich verziách systémov PMS, ePerso a IS, a tiež praktické cvičenia na personalizačných zariadeniach MX6000 a čítacích zariadeniach

MX6000. Zhotoviteľ poskytne koučing zamestnancom objednávateľa pri osvojení si práce s novým Personalizačným systémom.

14.1. Školenia administrátorov, operátorov a používateľov NPC

Pre pracovníkov NPC poskytne zhotoviteľ nasledujúce školenia:

Názov	Min. počet účastníkov	Dĺžka trvania	Čas vykonania
Školenie operátorov a uživateľov APV Personalizačného systému č. 3	3	2 školenia po 1 dni	V súlade s Harmonogramom
Školenie administrátorov NPC pre ePerso a IS	6	1 deň	V súlade s Harmonogramom

Obsah školenia operátorov a uživateľov APV Personalizačného systému

1) Skladovanie a obeh čistopisov
2) Load-balancing objednávok
3) Spracovanie výrobných dávok
4) Reklamačné a skartačné procesy
5) Správa výrobných pracovných zmien
6) Správa pracovných zmien vnútorného oddelenia (VO)
7) Praktické cvičenia s APV
8) On job coaching

Obsah školenia administrátorov NPC pre ePerso a IS

1) Inštalácia a konfigurácia
    - Personalizačný server – inštalované komponenty a servisy
    - Inšpekčný server – inštalované komponenty a servisy
2) Obsluha
    - Aplikácia pre správu podpisovacích certifikátov (ASPC)
    - Aplikácia pre správu šifrovacích certifikátov (ASSC)
    - Aplikácia pre import kľúčov (AIK)
    - Aplikácia pre správu certifikátov (ASC) Inšpekčného systému
3) Praktické cvičenia
4) On job coaching

14.2. Školenia administrátorov, operátorov a používateľov ZNPC

Pre pracovníkov NPC poskytne zhotoviteľ nasledujúce školenia:

Názov	Min. počet účastníkov	Dĺžka trvania	Čas vykonania
Školenie operátorov MX 6000 („školenie č.1“)	3	1 deň	V súlade s Harmonogramom
Školenie operátorov MX 2000 (MX	3	1 deň	V súlade s Harmonogramom

6000 čítacích zariadení) („školenie č.2“)			
Školenie užívateľov APV Personalizačného systému („školenie č.3“)	6	2 dni	V súlade s Harmonogramom

Obsah školenia operátorov MX 6000

1) Identifikácia modulov a vysvetlenie ich funkcií
2) Identifikácia a spôsob doplnenia spotrebného materiálu
3) Identifikácia ovládacích prvkov stroja (hlavný vypínač, ochranné prvky – Interlock-y)
4) Ukážka korektnej štartovacej a vypínacej procedúry
5) Vysvetlenie jednotlivých komponentov základnej produkčnej obrazovky
6) Nahratie a vymazanie výrobnej dávky
7) Spustenie a ukončenie produkčnej dávky
8) Spracovanie nepodarkov
9) Zobrazenie aktuálneho stavu spracovania výrobnej dávky
10) Odstraňovanie chýb
11) Praktické cvičenia
12) On job coaching

Školenie operátorov MX 2000 (MX 6000 čítacích zariadení)

1) Identifikácia modulov a vysvetlenie ich funkcií
2) Identifikácia a spôsob doplnenia spotrebného materiálu
3) Identifikácia ovládacích prvkov stroja (hlavný vypínač, ochranné prvky – Interlock-y)
4) Ukážka korektnej štartovacej a vypínacej procedúry
5) Vysvetlenie jednotlivých komponentov základnej produkčnej obrazovky
6) Nahratie a vymazanie výrobnej dávky
7) Spustenie a ukončenie produkčnej dávky
8) Spracovanie nepodarkov
9) Zobrazenie aktuálneho stavu spracovania výrobnej dávky
10) Odstraňovanie chýb
11) Praktické cvičenia
12) On job coaching

Školenie užívateľov APV Personalizačného systému

1) Doplnenia a zmeny funkcionality APV
2) Skladovanie a obeh čistopisov
3) Load-balancing objednávok
4) Obeh výrobných dávok
5) Kontrola kvality personalizácie
6) Expedícia dokladov na JP
7) Obálkovanie dokladov
8) Reklamačné procesy
9) Skartačné procesy
10) Správa výrobných zmien
11) Správa pracovných zmien vnút. odd
12) Zmeny technológií
    - Personalizačná technológia

- Technológia na podporu skartačných procesov

13) Organizačné zmeny a pracovné postupy
14) Praktické cvičenia
15) On job coaching

14.3. Zaškolenie PKI administrátorov a operátorov

Pre 2 pracovníkov objednávateľa poskytne zhotoviteľ špecializované 2 dňové školenie pre používanie a správu EAC PKI s nasledujúcim obsahom:

1) Úvod k EAC PKI
2) Slovenská CVCA/DVCA pre EID (EACPKI2)
3) EAC PKI certifikáty (štruktúra, životný cyklus)
4) Správa certifikačných autorít
5) Role správcov, PKI dokumentácia, bezpečnosť CA
6) Produkty UniCERT a nCipher
7) Hlavné úlohy a postupy správy Slovenskej CVCA/DVCA pre EID
8) Dennodenné činnosti správcov Slovenskej CVCA/DVCA pre EID
9) Správa infraštruktúry
10) Ďalšie úlohy (ceremónia, certifikačné činnosti, HSM administrácia)
11) Praktické cvičenia
12) On job coaching

15. Dokumentácia

Obsahom dodávky je Dokumentácia, tak ako je uvedené nižšie:

Technická dokumentácia a prevádzková dokumentácia k personalizačným zariadeniam (MX 6000, MX 2000) v písomnej forme v počte 1 kus a v elektronickej forme na CD, ktorá bude obsahovať:

- popis zariadenia (SW prostredie, názvoslovné konvencie, logické závislosti, verzia),
- operátorský manuál
- zoznam a popis rutinných činností,
- chybové a neštandardné stavy a dostupné spôsoby ich riešenia,
- popis pokračovania po odstránení chyby,
- funkčný popis konfigurácie a nastavenia systému

Aktualizácia používateľskej dokumentácie APV Personalizačného systému

Obsahom dodávky je aktualizácia používateľskej dokumentácie v písomnej forme v počte 1 kus a v elektronickej forme na CD, tak ako je uvedené nižšie:

- Používateľská príručka k APV Personalizačného systému, ktorá bude obsahovať aktualizácie v dôsledku zavedenia eID a eDoPP najmä v nasledovných oblastiach
  - popis APV Personalizačného systému a jeho funkcií,
  - postupy a úkony potrebné pre riadne používanie APV Personalizačného systému,
  - chybové a neštandardné stavy a dostupné spôsoby ich riešenia.
- Používateľska príručka APV Inšpekčného systému
  - popis APV Inšpekčného systému a jeho funkcií,
  - postupy a úkony potrebné pre riadne používanie APV Inšpekčného systému,
  - chybové a neštandardné stavy a dostupné spôsoby ich riešenia.

- Administrátorská príručka k APV Personalizačného systému v písomnej forme v počte 1 kus a v elektronickej forme na CD, ktorá bude obsahovať aktualizácie v dôsledku zavedenia eID a eDoPP najmä v nasledovných oblastiach
  - aktualizovaný dátový model systému,
  - väzby na iné systémy,
  - inštalačný postup aplikácie,
  - chybové stavy a postup ich riešenia,
  - popis procedúr pre zálohovanie a obnovu dát,
  - popis použitých technických číselníkov, ich naplnenie pri inicializácii,
  - popis recovery procedúry.

Dokumentácia k časti EAC PKI bude obsahovať nasledujúcu prevádzkovú dokumentáciu:

- Inštalačná príručka - Dokumentácia inštalačného postupu riešenia
- CP dokument – Zameraný na certifikáty a zodpovednosti CA, obsahuje použitie, postup vydávania, registrácia, obnovovanie certifikátov.
- CPS dokument – Transformácia CP do prevádzkových postupov na úrovni CA.

16. Príprava rutinnej prevádzky a podpora Riadnej rutinnej prevádzky

V rámci prípravy rutinnej prevádzky zhotoviteľ zabezpečí prípravu Personalizačného systému (t.j. APV PMS, ePerso a IS, a personalizačné zariadenie na rutinnú prevádzku. V rímci prípravy prevádzky zhotoviteľ zabezpečí najmä:

- Inštaláciu a konfigurácia ePerso plugin pre produkčnú prevádzku
- Inštaláciua a konfigurácia eVRC plugin pre produkčnú prevádzku
- Konfigurácia účtov a oprávnení, zaradovanie účtov do aplikačných rolí pre produkčnú prevádzku
- Inštalácia ID1 Client pre produkčnú prevádzku
- Nastavenie audit setup
- Inštalácia a konfigurácia ID1 Audit Service pre produkčnú prevádzku
- Inštalácia a konfigurácia ID1 Audit Skartácia pre produkčnú prevádzku
- Konfigurácia produkčnej databázy
- Kalibrácia laserov pre ID layout
- Kalibrácia laserov pre DL layout
- Kalibrácia laserov pre eVRC layout
- Kalibrácia laserov pre eBP layout
- Kalibrácia laserov pre eRP layout
- Príprava referenčných vzoriek zo všetkých typov dokladov
- Príprava novej produkčnej databázy a migrácia dát

Pri podpore Riadnej rutinnej prevádzky Personalizačného systému zhotoviteľ uskutoční najmä nasledovné činnosti:

- Metodickú podporu pri práci s Personalizačným systémom,
- Technickú pomoc pri obsluhe personalizačných zariadení,
- Metodickú pomoc pri tvorbe výstupov z Personalizačného systému,
- Metodickú pomoc pri zmenových prácach v Riadnej rutinnej prevádzke Personalizačného systému,
- Metodickú podporu súvisiacu so správou a používaním Personalizačného systému (zálohovanie dát, správa oprávnení a pod.),
- Inú metodickú podporu súvisiacu s používaním Personalizačného systému.

17. Rozšírená podpora nábehu rutinnej prevádzky

Pri nábehu systémov NPC a ZNPC a po ich zavedení do rutinnej prevádzky bude zhotoviteľ zabezpečovať zvýšenú podporu prevádzky podľa potrieb objednávateľa. Realizuje sa skúšobný pilot, retestovanie za účasti zhotoviteľa a preklopenie do produkcie. Počas tohto obdobia bude zabezpečená účasť zástupcov zhotoviteľa pre jednotlivé fázy nábehu priamo v priestoroch zákazníka.

V rámci rozšírenej podpory nábehu rutinnej prevádzka budú vykonávané činnosti:

- Príprava predprodukt ívnej prevádzky
- Retestovanie za účasti zhotoviteľa
- Dohľad nad nábehom systému
- Koučovanie zamestnancov objednávateľa
- Zvýšená konzultačná podpora – účasť implementačných tímov zhotoviteľa na mieste

Zhotoviteľ poskytne Rozšírenú podporu nábehu rutinnej prevádzky podľa potrieb objednávateľa pri nábehu rutinej prevádzky ZNPC, pri zavedení do rutinnej prevádzky verzie Personalizačného systému, ktorej funkcionalita pokrýva legislatívne zmeny vyplývajúce z novely zákona o občianskych preukazoch platných k 1.7.2012 a pri zavedení finálnej verzie všetkých systémov (IS PMS, ePerso, IS a všetkých personalizačných zariadení nastavených na nové typy dokladov) do rutinnej prevádzky.

18. Zoznam použitých skratiek

Skratka	Popis
ZPC	Záložné personalizačné centrum
eID	Elektronicky občianský preulaz
eDoPP	Elektronicke povolenien na pobyt na územi SR pre cudxincov
IS	Informačný Systém.
APV	Aplikačne Programové Vybavenie.
ZEP	Zaručený elektronický podpis
AC	Autentifikačný certifikácy
SC	Šifrovaci certifikát
MRZ	„Machine Readable Zone“ - Strojovo čitateľná zóna (na dokladoch).
OCR	„Optical Character Recognition” – Rozpoznávanie znakov alebo preklad obrázkov na znaky.
PKI	„Public Key Infrastructure“ – Ifraštruktúra verejného kľuča.
ISO	„International Organization for Standardization“ – Medzinárodná organizácia pre štandardizáciu.
ID1,ID3	Formáty dokladov podľa normy ISO 7810.
VD	Výrobná Dávka.
JP	Jednotné Pracovisko.
RA	Pracovislo Registračnej autority
SMS	„Short Message Service“ – Služba na posielanie krátkych textových správ.
CASE nástroj	„Computer Aided Software Engineering“ – Nástroje na podporu vývoja veľkých programových systémov.
EU	„Europeaný Union“ – Európska únia.
EC	„European Commission“ – Európska komisia.
ICAO	„International Civil Aviation Organization“ – Organizácia vydávajúca štandardy v leteckej preprave.
LDS	„Logical Data Structure“ – Logická dátová štruktúra.
EAC	Rozšírená kontrola prístupu k údajom na čipe dokladu
CSCA NCA	„Country Signing Certification Authority“ - Národná (podpisujúca) Certifikačná Autorita.

Skratka	Popis
HSM	„Hardware Security Module“ – Modul pre šifrovacie operácie a bezpečné uloženie kľúčov.

ČASŤ II ROZŠÍRENIE IS SA AGENDA OBČIANSKYCH PREUKAZOV O FUNKČNOSŤ REALIZUJÚCU VYGENEROVANIE A SPRACOVANIE VÝROBNÝCH OBJEDNÁVOK NA PERSONALIZÁCIU ELEKTRONICKEJ EID KARTY

1. Súlad riešenia s relevantnými normami

Riešenie bude realizované v súlade so súvisiacou legislatívou a to najmä so Zákonom o občianskych preukazoch a o zmene a doplnení niektorých zákonov č. 226/2006 a Zákonom o pobyte cudzincov 463/2006.

2. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej súťaži v prílohe B1 - Opis predmetu zákazky časť II: „Rozšírenie IS SA agenda občianskych preukazov o funkčnosť realizujúcu vygenerovanie a spracovanie výrobných objednávok na personalizáciu elektronickej eID karty“.

3. Predmet Technického riešenia

V súčasnosti je proces vydávania identifikačných dokladov v rozsahu občiansky preukaz pre občanov a doklad o povolení na pobyt pre cudzincov s povoleným pobytom na území SR automatizovaný. Proces zberu žiadostí, ich spracovania a zaslania na personalizáciu je realizovaný s využitím APV JP a príslušných agendových IS – APV IS SA Agenda občianskych preukazov, APV IS REGOB Evidencia cudzincov.

Predmetom technického riešenia je rozšírenie APV IS SA Agenda občianskych preukazov o funkčnosť realizujúcu vygenerovanie a spracovanie výrobných objednávok na personalizáciu elektronickej eID karty a rozšírenie APV IS REGOB Evidencia cudzincov o funkčnosť realizujúcu vygenerovanie a spracovanie výrobných objednávok na personalizáciu elektronickej eDoPP karty.

Predmetom technického riešenia je zároveň realizácia definovaných zmenových požiadaviek.

V rámci úpravy APV IS SA Agenda občianskych preukazov budú zrealizované úpravy potrebné vzhľadom na zavedenie nového typu občianskeho preukazu – elektronickej ID karty a s ňou súvisiacich úprav procesov. Zároveň budú zrealizované úpravy v nasledujúcom rozsahu:

- Vytvoriť číselník krvných skupín so všetkými druhmi krvnej skupiny a pri evidovaní novej žiadosti o OP umožniť používateľom vyplniť položku Osobitné záznamy na OP (vždy do nového riadku) maximálne jednou hodnotou z tohto číselníka.
- Vytvoriť číselník dôvodov vydania OP, pričom vybratie hodnoty z tohto číselníka pri evidovaní žiadosti o vydanie OP bude povinné a vybraná hodnota bude uvedená pri type žiadosti.
- Pri zobrazovaní detailov žiadosti v rámci celej APV pre OP zrušiť duplicitnú možnosť zobrazovania detailov žiadosti (v detaile žiadosti uvádzať na jednom mieste všetky detaily vrátane podpisu a fotky).
- Umožniť modifikovať pre číselník Typ žiadosti pre vydanie OP položky Skrátený názov a Názov.
- Vo všetkých štatistikách umožniť vytvárať štatistiky pre celú SR, vybraný kraj alebo vybrané pracovisko. Vo všetkých reportoch umožniť vytvárať reporty za vybrané pracovisko.
- Pri zmene údajov o občanovi v REGOB, ktoré sú evidované na OP automaticky označiť v agende OP doklad ako doklad s neaktuálnymi údajmi (cez špeciálny príznak) v prípade, že je aktuálne doklad v stave Vydaný. Následne APV pre OP pri práci s takto označeným OP zobrazí upozornenie o neaktuálnosti údajov uvedených na OP.
- V rámci činnosti pre opravu údajov o OP doplniť možnosť opravy špeciálneho príznaku aktuálnosti údajov na OP.
- Upraviť rozhranie do APV Personalizačného systému (NPC resp. ZPC) pre zaslanie požiadavky na výrobu OP a upraviť zaznamenávanie údajov o žiadosti o vydanie OP v súvislosti so zavedením čipu do OP.
- Rozšíriť rozhranie na APV Personalizačného systému v súvislosti s procesom skartácie kedy Personalizačný systém iniciuje potvrdenie prevzatia dokladov na skartáciu.
- Vytvorenie webservisu, ktorý na základe zadaných základných údajov z OP vyhodnotí, či je takýto OP evidovaný v agende OP a či tento OP je platný.
- Vytvoriť činnosť pre spravovanie číselníka Typ predloženého dokumentu.
- Vytvoriť logovanie lustrácií OP a vytvoriť činnosť pre prezeranie logov lustrácií OP.

V rámci úpravy APV IS REGOB Evidencia cudzincov budú zrealizované úpravy potrebné vzhľadom na zavedenie nového typu dokladu o povolení na pobyt – elektronickej ID karty a s ňou súvisiacich úprav procesov. Zároveň budú zrealizované úpravy v nasledujúcom rozsahu:

- Upraviť existujúci report Počet s pobytom podľa štátnej príslušnosti tak aby bolo možné vybrať na vstupe viacero typov pobytu a aj viacero účelov pobytu prislúchajúce k vybraným typom pobytu.
- Do variabilných zoznamov a štatistík ktoré obsahujú na vstupe voľbu okres doplniť na vstup číselník pracovísk OCP, kde po zvolení pracoviska budú vypísané osoby s pobytom na adrese v územnej pôsobnosti vybraného OCP.
- Do variabilných zoznamov doplniť na výstup Akronym2 štátnej príslušnosti.
- Do variabilných zoznamov doplniť na vstup možnosť zakliknúť Historické údaje. V prípade, že bude zakliknutá táto možnosť tak budú podmienky zo vstupu vyhodnotené ako doteraz, t.j. na aktuálne údaje, ale do výstupu bude osoba zaradená viackrát v závislosti od toho koľko historických záznamov o pobyte sa pre danú osobu našlo, t.j. pre každý pobyt osoby bude vyplnený samostatný celý riadok o osobe.
- Dopracovať report Počet osôb s dlhodobým pobytom kde Vstup: K dátumu, Pohlavie (nepovinne) a Výstup: Os Y - štátna príslušnosť, Os X - počet osôb, s platným pobytom, t.j. Dátum začiatku platnosti pobytu <= K dátumu <= Dátum ukončenia pobytu a zároveň má tento pobyt nastavený účel pobytu, ktorý je označený ako OSOBA S DLHODOBÝM POBYTOM – ES.
- Doplniť stav dokladu „Vydaný - Neplatný“ . Dopracovať aplikáciu tak aby umožňovala v definovaných činnostiach (napr. zrušenie pobytu) zmenu stavu dokladu ako aj samostatnú činnosť na zmenu stavu dokladu. Tieto zmeny realizovať pre všetky druhy dokladov CUP, Dopp, NPP, MPS. Zrealizovať poskytovanie informácie o takomto doklade pre integrované systémy (napr. CLK) ako informácia závažného typu.
- V udelení tolerovaného pobytu z úradnej moci vždy vytvoriť pobyt aj keď má osoba ešte platný pobyt.
- Umožniť pre vybrané žiadosti zasielanie požiadavky na stanovisko do VIS až pri činnosti Vyhovenie žiadosti, resp. Zamietnutie žiadosti.

4. Funkčný návrh systému

Predmetom rozšírenia APV IS SA Agenda občianskych preukazov je úprava rozhraní pre komunikáciu s sAPV JP resp. s APV Personalizačného systému vzhľadom na zmeny, ktoré vyplynú zo zavedenia elektronickej eID karty.

Čo sa týka rozhraní na JP, je to najmä úprava nasledujúcich rozhraní:

- spracovanie žiadosti o vydanie eID a zadanie PIN a jeho šifrovanie
- prevzatie dokladov na JP – elektronický preberací protokol,
- odoslanie dokladu na skartáciu do NPC (rep. ZPC) (skartačný zoznam).

Čo sa týka rozhraní na Personalizčné centrum , je to najmä úprava resp. vybudovanie nasledujúcich rozhraní:

- zaslanie údajov na personalizáciu,
- rozširenie rozhrania o PIN v šifrovanej podobe
- prevzatie údajov na personalizáciu,
- príprava dokladov na distribúciu,
- odovzdanie zaobalkovaných dokladov kuriérovi, resp. vybranému poštovému operátorovi na individuálne doručenie
- prevzatie dokladov na JP – elektronický preberací protokol,
- odoslanie dokladu na skartáciu do NPC (resp. ZPC) (skartačný zoznam),
- potvrdenie prevzatia dokladu na skartáciu,
- realizácia skartácie dokladu.

Systémová komunikácia s vybraným poštovým operátorom

Po skončení personalizácie bude pre individuálne doručené doklady prebiehať v rámci distribúcie vybraným poštovým operátorom komunikácia NPC a systému vybraného poštového operátora. Komunikácia je realizovaná pre nasledujúce udalosti :

- poskytnutie zoznamu identifikačných čísel a ďalších údajov o zásielkach určených na distribúciu

vybraným poštovým operátorom.

Predmetom riešenia je zároveň realizácia definovaných zmenových požiadaviek na úpravu APV IS SA Agenda občianskych preukazov a realizácia úprav agendového spracovania, ktorá vyplynie zo zavedenia nových eID kariet. Uvedené úpravy budú plne rešpektovať súčasnú funkčnú dekompozíciu APV IS SA Agenda občianskych preukazov. Uvedené úpravy budú plne rešpektovať kvalitatívne požiadavky na aktuálne prevádzkované APV IS SA Agenda občianskych preukazov.

Predmetom rozšírenia APV IS REGOB Evidencia cudzincov je úprava rozhraní pre komunikáciu s APV JP resp. s APV Personalizačného systému vzhľadom na zmeny, ktoré vyplynú zo zavedenia elektronickej eDoPP karty.

Čo sa týka rozhraní na JP, je to najmä úprava nasledujúcich rozhraní:

- spracovanie žiadosti o vydanie eDoPP,
- prevzatie dokladov na JP – elektronický preberací protokol,
- ,
- odoslanie dokladu na skartáciu do NPC (resp. ZPC) (skartačný zoznam).

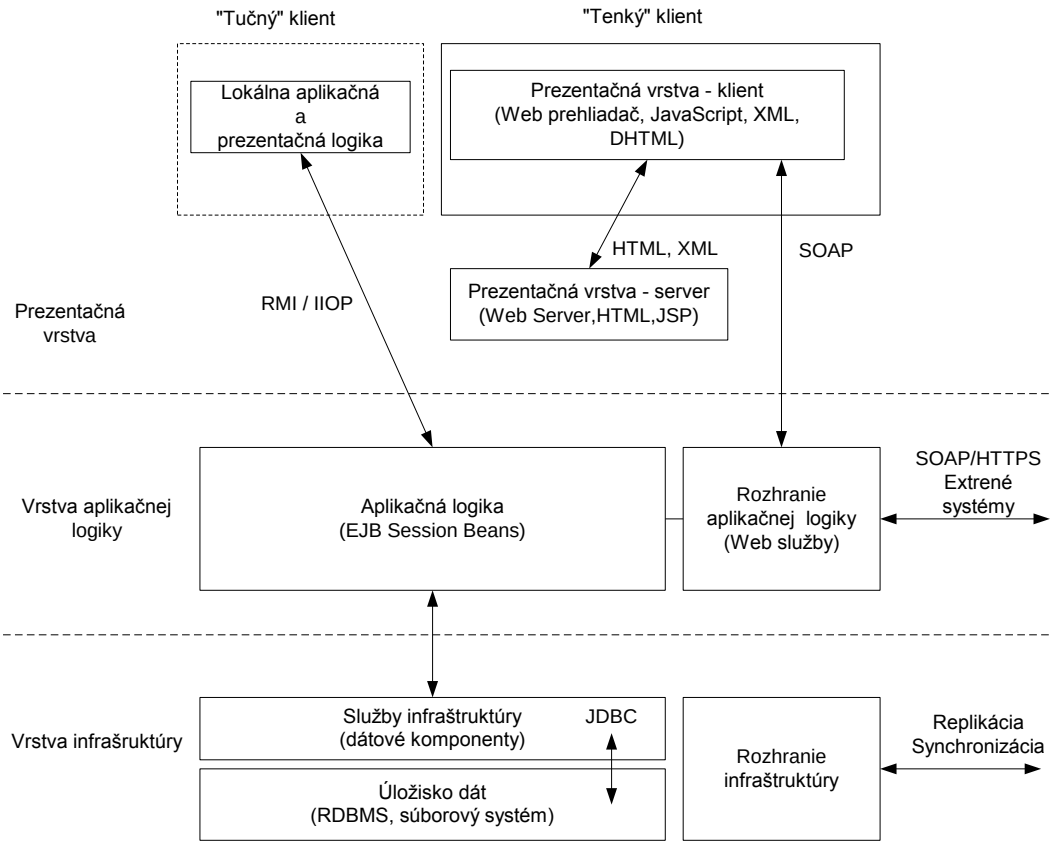
Čo sa týka rozhraní na Personalizačný systém , je to najmä úprava resp. vybudovanie nasledujúcich rozhraní:

- zaslanie údajov na personalizáciu,
- prevzatie údajov na personalizáciu,
- príprava dokladov na distribúciu,
- odovzdanie dokladov kuriérovi,
- prevzatie dokladov na JP – elektronický preberací protokol,
- odoslanie dokladu na skartáciu do NPC (resp. ZPC)(skartačný zoznam),
- potvrdenie prevzatia dokladu na skartáciu,
- realizácia skartácie dokladu.

Predmetom riešenia je zároveň realizácia definovaných zmenových požiadaviek na úpravu APV IS REGOB Evidencia cudzincov a realizácia úprav agendového spracovania, ktorá vyplynie zo zavedenia nových eDoPP kariet. Uvedené úpravy budú plne rešpektovať súčasnú funkčnú dekompozíciu APV IS REGOB Evidencia cudzincov. Uvedené úpravy budú plne rešpektovať kvalitatívne požiadavky na aktuálne prevádzkované APV IS REGOB Evidencia cudzincov.

5. Návrh (dizajn) APV

Keďže technické riešenie bude budované ako rozšírenie IS SA, bude zachovaná 3 vrstvová aplikačná architektúra riešenia použitá pri IS SA. Členenie na vrstvy z logického pohľadu vyjadruje úlohy a zodpovednosti jednotlivých vrstiev v systéme. Logický pohľad je doplnený pohľadom fyzickým, ktorý zobrazuje rozmiestenie komponentov systému zo softvérového a hardvérového hľadiska. Nasledujúca schéma zobrazuje logické členenie systému:



Obr.1 Aplikačná architektúra

Systém pozostáva z prezentačnej, aplikačnej a infraštruktúrnej vrstvy. Každá z vrstiev je zodpovedná za poskytovanie služieb nadradeným vrstvám prípadne používateľovi a zároveň využíva služby nižších vrstiev. Jednotlivé logické vrstvy sú popisované v ďalších kapitolách. Návrh vrstiev a služieb vychádza z pravidla, že nadriadená vrstva používa služby iba bezprostredne podriadenej vrstvy a podriadená vrstva je nezávislá od vrstiev nadradených. Týmto je možné dosiahnuť želanú modularitu a flexibilitu systému.

Z fyzického hľadiska sú jednotlivé komponenty implementované s použitím vybraných technológií platformy J2EE a realizované na rôznych softvérových produktoch. Rozmiestnenie komponentov na fyzických vrstvách umožňuje lepšiu škálovateľnosť aplikácie za účelom zabezpečenia požadovaného výkonu, napomáha zvýšeniu bezpečnosti systému a jeho udržiavateľnosti.

Prezentačná vrstva

Prezentačná vrstva predstavuje rozhranie informačného systému smerom k používateľovi. Sprístupňuje služby systému prostredníctvom grafického používateľského rozhrania implementovaného v klientskej aplikácii. Navrhované riešenie bude realizované ako „tenký klient“, kedy je používateľské rozhranie realizované stránkami HTML, prezentovanými používateľovi v aplikácii internetového prehliadača.

Zobrazovanie údajov, ich zadávanie, navigácia medzi obrazovkami a ostatné činnosti sú realizované prostriedkami HTML jazyka za pomoci JavaScript kódov. Zasielanie údajov na server je realizované prostredníctvom HTML formulárov. Výsledky požiadaviek používateľa, sú doručované na klientskú stanicu rovnako v podobe HTML dokumentov. V prípade takéhoto riešenia nie je na pracovnú stanicu používateľa inštalovaný samostatný softvér, ale klientská aplikácia používa internetový prehliadač a obrazovky aplikácie sú získané dynamicky z webového servera. Týmto je zabezpečená jednoduchšia správa a distribúcia verzií, ľahšia údržba a správa klientskej aplikácie.

Kombináciou techník používaných pri vývoji „klasického tenkého klienta“ s technológiami SOAP, XML, DHTML a JavaScript na platforme prehliadača Microsoft Internet Explorer je možné vytvoriť plnohodnotnú aplikáciu s bohatou prezentačnou funkcionalitou, komfortom navigácie a interakcie, optimalizovaným prenosom dát, zvýšenou bezpečnosťou a akceptovateľnými nárokmi na klientskú stanicu.

V nami navrhovanom riešení je prezentačná vrstva rozdelená na server a klient časti. Server časť predstavuje úložisko (repository) obrazoviek klientskej aplikácie. Stránky obrazoviek, menu a dialógov sú generované technológiou JSP a „stiahnuté“ na klienta štandardným spôsobom. Navigácia, zadávanie údajov, ich validácia a

ostatné prvky interakcie s používateľom sú zabezpečované klientskou časťou aplikácie. Pri tvorbe obrazoviek je snaha minimalizovať počet dotazov a prenášaných dát medzi klientom a web serverom. Odosielanie samotných údajov (business data) a ich získavanie zo servera sa deje samostatným HTTPS kanálom cez služby SOAP. Dáta sú prenášané vo formáte XML medzi aplikačným serverom a klientskou stanicou bez účasti prezentačnej vrstvy na servri. Business dáta nie sú uložené na lokálnom disku klientskeho počítača. Celá transakcia prebehne v pamäti. Formát XML je ďalej používaný klientskou aplikáciou na zobrazovanie, transformácie ako aj interné ukladanie dát.

Navrhovaná implementácia klienta umožní využitie štandardných autentifikačných mechanizmov s použitím HTTP basic autentifikácie aj autentifikácie klientskými certifikátmi.

Prezentačná vrstva bude realizovaná v slovenskom jazyku.

Vrstva aplikačnej logiky

Vrstva aplikačnej logiky implementuje služby komponentami EJB Session Bean. Navonok sú sprístupňované prostredníctvom webových služieb (SOAP web services) alebo EJB rozhraním (local/remote EJB interface). Použitý typ rozhrania závisí od typu klienta. Klientská aplikácia (včítanie rozšíreného klienta pre prácu s biometrickými údajmi) bude používať SOAP webové služby, interné aplikácie iných agend môžu využívať lokálne EJB rozhrania a externé EJB kompatibilné aplikácie môžu komunikovať prostredníctvom vzdialených EJB rozhraní a protokolu RMI/IIOP. Rôzne typy prístupu k vrstve aplikačnej logiky poskytujú možnosť voľby optimálneho spôsobu pripojenia k systému pre rôzne aplikácie.

Služby systému budú implementované ako metódy na komponentoch EJB Session Bean. Služby budú implementované ako „stateless“ bez uchovávania kontextu medzi volaniami rôznych služieb. V prípade potreby bude kontext simulovaný na klientskej vrstve alebo JSP vrstve, prípadne iným aplikačným spôsobom. Základnou úlohou bude implementácia kontroly obchodných pravidiel ako aj referenčnej a dátovej integrity. Vrstva EJB komponentov bude zabezpečovať riadenie databázovej transakcie, poskytovať a spravovať identifikátory transakcií (TID). Služby budú používať XML rozhrania, pričom syntax a sémantika XML správ bude kontrolovaná pomocou XSD schém a dodatočnými validačnými pravidlami.

Riadenie prístupu

Prístupové body rozhrania budú využívať vstavané mechanizmy J2EE aplikačného servera na autentifikáciu používateľov v kombinácii s ostatnými prvkami infraštruktúry. Pre uloženie a správu používateľov a skupín sa predpokladá nasadenie samostatného LDAP servera v rámci systémovej infraštruktúry (s možnosťou mapovania SSL certifikátov a používateľov). Riadenie prístupu a prideľovanie oprávnení bude riešené na aplikačnej úrovni samostatným bezpečnostným modulom.

Rozhranie na vrstvu infraštruktúry

Na prístup k vrstve infraštruktúry bude vrstva aplikačnej logiky používať špecializované dátové komponenty – DAC objekty. Tieto sú zodpovedné za vkladanie, modifikáciu a čítanie objektov z databázy a ich transformáciu z/do podoby XML a Java objektov. Implementovať bude aj vyrovnávaciu pamäť (cache) číselníkových hodnôt.

Vrstva infraštruktúry

Vrstva infraštruktúry primárne poskytuje služby pre uloženie údajov používaných v systéme. Kritériá na úložisko zahŕňajú bezpečnosť, garanciu integrity, transakčnosť operácií nad dátami, výkonnosť pri prístupe k údajom a ich modifikácii. Pri budovaní systému sa počíta s použitím moderného RDBMS databázového servera doplneného v prípade potreby o možnosti ukladania dát na súborový systém.

Dátový model bude realizovaný v schémach jednej databázovej inštancie. Fyzický databázový model aplikácie bude odtienený od ostatných vrstiev a databáza bude komunikovať zásadne prostredníctvom uložených procedúr. Aktuálny databázový model bude rozšírený o údajové štruktúry súvisiace so spracovaním žiadostí a integráciou s APV Personalizačného systému.

Infraštruktúrna vrstva nebude plne využívať relačnú podporu RDBMS servera, ale bude implementovať vlastnú kontrolu dátovej integrity. Tento zámer vychádza z použitia špecifických návrhových vzorov. Infraštruktúrna vrstva bude vytvárať transakčný žurnál – evidovať čas, poradie, miesta zmien, meno používateľa a ďalšie údaje o zmenách a prístupoch do systému.

Pre uloženie niektorých údajov používaných systémom sa predpokladá použitie súborového systému. Ide prevažne o konfiguračné súbory, vstupné a výstupné súbory pre import a export dát a údaje, ktorých uloženie v relačnej databáze by bolo neefektívne.

Bezpečnostné mechanizmy

Ponúkané technické riešenie v plnej miere zachová bezpečnostné mechanizmy použité v IS SA resp. v IS REGOB.

Implementácia rozšírenia IS SA a IS REGOB bude realizovaná na rovnakej platforme ako IS SA a IS REGOB. Vzhľadom na uvedené bude využitý v súčasnosti implementovaný spôsob zálohovania dát ako aj existujúce disaster/recovery procedúry

6. Implementácia rozšírenia APV

Implementácia rozšírenia IS SA Agenda občianskych preukazov bude realizovaná na rovnakej prevádzkovej platforme ako IS SA Agenda občianskych preukazov. Vzhľadom na uvedené bude využitý v súčasnosti implementovaný spôsob zálohovania dát ako aj existujúce disaster/recovery procedúry.

Implementácia rozšírenia IS REGOB Evidencia cudzincov bude realizovaná na rovnakej prevádzkovej platforme ako IS REGOB Evidencia cudzincov. Vzhľadom na uvedené bude využitý v súčasnosti implementovaný spôsob zálohovania dát ako aj existujúce disaster/recovery procedúry.

Deployment model rozšírenia IS SA a IS REGOB bude plne rešpektovať aktuálny stav nasadených aplikácií popísaný v nasledujúcej časti:

IHS

Na servroch je inštalovaný statický obsah webu prezentačnej vrstvy a webu web servisov.

WAS

Na servroch je inštalovaná EJB a WebServis vrstva ako aplikácie regob, ktorej súčasťou sú moduly pre APV IS SA Agenda občianskych preukazov a APV IS REGOB Evidencia cudzincov.

LDAP

Na LDAP serveroch sú vytvorené aplikačné a systémové kontá potrebných používateľov. P a T prostredia zdieľajú spoločné LDAP repository.

DB

Produkčné prostredie je inštalované na servri DB1 ako samostatná databáza.

Čo sa týka realizácie resp. úpravy údajových rozhraní na iné informačné systémy, budú zachované v súčasnosti používaný štandard vo forme Web Service rozhraní.

Skutočná fyzická realizácia deploymentu bude spracovaná ako súčasť prevádzkovej dokumentácie.

7. Externé rozhrania

Všetky rozhrania uvedené v nasledujúcej časti budú zrealizované v rámci APV IS SA Agenda občianskych preukazov aj v rámci APV IS REGOB Evidencia cudzincov.

8. Zaslanie objednávky na personalizáciu dokladov

Personalizačný Systém iniciuje proces zaslania objednávky na personalizáciu. Vo vstupnom XML zašle požadovaný počet dokladov na personalizáciu. Systém IS SA v prípade, že má zaevidovanú objednávku, pre ktorú nebolo zrealizované potvrdenie prevzatia vygeneruje výstupné XML z tejto objednávky. Inak vytvorí novú objednávku a zaradí do nej požadovaný počet dokladov. Ak je požadovaný počet väčší ako počet dokladov pripravených na personalizáciu, zaradí všetky doklady do objednávky a vygeneruje objednávku s menším počtom dokladov ako bol požadovaný. Na základe objednávky následne vygeneruje výstupné XML.

Ak v systéme IS SA nie je žiadny doklad pripravený na personalizáciu je vygenerované prázdne výstupné XML. Po zaradení dokladu do objednávky sa jeho stav zmení na „Zadaný na personalizáciu“.

9. Potvrdenie prevzatia objednávky na personalizáciu dokladov

Po prijatí objednávky Personalizačný systém iniciuje proces potvrdenia objednávky. V prípade úspešného prijatia objednávky Personalizačný systém zašle ako vstupné XML potvrdenie objednávky, inak systém NPC zašle ako vstupné XML zamietnutie objednávky. Po potvrdení objednávky systém IS SA pre všetky doklady zaradené do objednávky zmení stav na „Personalizovaný“. Pokiaľ nie je objednávka potvrdená alebo zamietnutá, nie je možné vygenerovať novú objednávku.

10. Pripravenosť dokladov na distribúciu

o skontrolovaní kvality dokladov výrobnej dávky Personalizačný systém iniciuje proces informovania o pripravenosti dokladov na distribúciu. V rámci vstupného XML sú zaslané informácie o čísle dokladu a čísle balíka, v ktorom bude doklad doručený na príslušný JP. Súčasťou vstupného XML bude aj číslo kartičky (čistopisu). Po spracovaní vstupného XML vygeneruje systém IS SA ako odpoveď výstupné XML, ktoré pre každý doklad z vstupného XML obsahuje dohodnutý status spracovania.

11. Prevzatie balíka kuriérom

o prevzatí balíka kuriérom Personalizačný systém iniciuje proces informovania o distribuovaní personalizovaných dokladov z . V rámci vstupného XML je zaslané číslo distribuovaného balíku. Systém IS SA nastaví stav dokladov pre požadovaný balík na „Distribuovaný“.

12. Potvrdenie prevzatia balíka dokladov na JP

Personalizačný systém v definovaných intervaloch overuje stav distribuovaného balíka dokladov. Po prevzatí balíka na JP je jeho stav nastavený na „Prebratý“.

13. Zaslanie skartačných zoznamov

Personalizačný systém iniciuje zaslanie skartačných zoznamov systémom IS SA. Vo vstupnom XML zašle dátum a čas zaslania balíka - vo význame posledný dátum a čas ktorý bol uvedený na posledne zaslanom skartačnom balíku. Systém IS SA poskytne všetky skartačné zoznamy, ktorých dátum a čas vytvorenia je väčší (mladší) ako vstupný parameter.

14. Potvrdenie prevzatia dokladov na skartáciu

Personalizačný systém iniciuje potvrdenie prevzatia dokladov na skartáciu. Vo vstupnom XML pre každý doklad zaradený do identifikovaného skartačného zoznamu, zašle informáciu o spôsobe jeho prevzatia na skartáciu vzhľadom na výsledok procesu fyzického preberania dokladov na skartáciu:

- Fyzicky došlé doklady na skartáciu presne súhlasia s elektronickým skartačným zoznamom. V takom prípade APV Personalizačného systému elektronicky odošle do IS SA potvrdenie prevzatia dokladov.
- 1-n dokladov, ktoré boli v elektronickom skartačnom zozname, neboli fyzicky dodané. APV NPC elektronicky odošle do IS SA informáciu, ktoré doklady neboli dodané. Na strane IS SA sa vykoná zmena stavu nedodaných dokladov tak, aby následne bolo možné na JP takéto doklady opätovne zaradiť do iného skartačného zoznamu a odoslať do NPC (resp. ZPC).
- Doklad nie je možné identifikovať. Neidentifikované doklady v elektronickom skartačnom zozname budú v NPC (ZPC) považované za nedodané a APV Personalizačného systému o nich odošle informáciu do IS SA.

15. Potvrdenie skartácie dokladov

Personalizačný Systém iniciuje potvrdenie skartácie dokladov pre systém IS SA. Vo vstupnom XML zašle číslo balíku, ktorého doklady boli fyzicky skartované. Systém IS SA pre každý doklad z balíku, pre ktorý bolo potvrdené prevzatie na skartáciu, nastaví stav na „Skartovaný“.

16. Školenia

Školenie zamestnancov MV SR pre používanie APV IS SA Agenda občianskych preukazov budú zrealizované v nasledujúcom rozsahu

Názov	Počet účastníkov	Dĺžka trvania	Čas vykonania
Školenie používateľov APV (školenie č.1)	Minimálne 100	1 deň	V súlade s Harmonogramom
Školenie používateľov APV (školenie č.1)	Minimálne 100	1 deň	V súlade s Harmonogramom
Školenie Helpdesk (školenie č.2)	10	1 deň	V súlade s Harmonogramom
Školenie administrátorov a operátorov	10	1 deň	V súlade s Harmonogramom

Školenie zamestnancov MV SR pre používanie APV IS REGOB Evidencia cudzincov budú zrealizované v nasledujúcom rozsahu

Názov	Počet účastníkov	Dĺžka trvania	Čas vykonania
Školenie používateľov APV (školenie č.1)	20	1 deň	V súlade s Harmonogramom
Školenie používateľov APV (školenie č.1)	20	1 deň	V súlade s Harmonogramom
Školenie Helpdesk (školenie č.2)	10	1 deň	V súlade s Harmonogramom
Školenie administrátorov a operátorov	10	1 deň	V súlade s Harmonogramom

Školenia budú zrealizované za nasledujúcich podmienok:

Miesta školení: školiace pracoviská MV SR vybavené zodpovedajúcou technikou, ktoré budú oznámené predávajúcemu zo strany kupujúceho najneskôr 3 pracovné dni pred začatím príslušného školenia,

Jazyk školenia: slovenský

V rámci školení budú účastníci školenia (bez ohľadu na rolu v systéme), vyškolení na procesné zmeny ohľadne žiadostí a vydávania dokladov a budú im poskytnuté všetky potrebné informácie a predvedené jednotlivé postupy a úkony pre oblasti dotknuté zavedením nového typu dokladu.

Súčasťou školení pre Helpdesk bude aj zaškolenie v problematike riešenia neštandardných situácií.

Súčasťou školení pre administrátorov a operátorov bude aj zaškolenie v problematike prevádzky a údržby systému a zmien fyzického dátového modelu.

V rámci aktivity Školenie objednávateľ okrem toho, že zrealizuje vlastné školenia zamestnancov objednávateľa, vykoná všetky činnosti spojené s prípravou a vyhodnotením školení. Zhotoviteľ pripraví školiace verzie systémov vrátane dát pre školenia, vytvorí užívateľské a administrátorské kontá v systémoch.

Po vlastnej realizácii školení vyhodnotí školiteľ spätnú väzbu účastníkov školenia na funkcionalitu a kvalitu APV.

Školiteľ zabezpečí praktické cvičenia pre zamestnancov objednávateľa na školiacich verziách systémov. Zhotoviteľ poskytne koučing zamestnancom objednávateľa pri osvojení si práce s novým APV.

Zhotoviteľ dodá zamestnancom objednávateľa, ktorí sa zúčastnia príslušného školenia, pred začatím tohto školenia všetky potrebné materiály pre účastníkov príslušného školenia a to najneskôr v deň začiatku školenia.

17. Dokumentácia

Zhotoviteľ dodá nasledujúcu dokumentáciu.

- Technickú dokumentáciu, ktorá bude obsahovať:
  - technickú (implementačnú) dokumentáciu k elektronickým službám.
  - dokumentáciu zverejnených rozhraní,
  - fyzický dátový model vo formáte XML vrátane väzieb medzi tabuľkami,
  - logický dátový model systému,
  - zdrojové kódy s popisom.

- Prevádzkovú dokumentáciu, ktorá bude obsahovať:
  - inštalačný postup aplikácie,
  - konfigurácia systémového SW serverov a pracovných staníc,
  - chybové stavy a postup ich riešenia,
  - popis mechanizmu riadenia prístupu používateľov k dátam a k funkciám aplikácie,
  - popis použitých a navrhovaných technických číselníkov, ich naplnenie pri inicializácii,

- Používateľskú dokumentáciu, ktorá bude obsahovať:
  - popis systému a jeho funkcií,
  - dokumentáciu pre realizáciu školení,
  - návrh testovacích procedúr a testovacie scenáre,
  - postupy a úkony potrebné pre riadne používanie systému,
  - chybové a neštandardné stavy a dostupné spôsoby ich riešenia.

Vyššie uvedená dokumentácia bude dodaná v písomnej forme v počte 1 kus a v elektronickej forme na CD.
Metadáta v softvérovom prostriedku na správu metadát v elektronickej forme na CD.

18. Podpora rutinnej prevádzky

Po spustení systému do rutinnej prevádzky bude poskytnutá podpora v trvaní min 2 týždne v rámci ktorej budú vykonávané najmä nasledovné aktivity:

- podpora používateľov systému,
- podpora dopracovania metodického rámca,
- podpora riešenia konfliktných situácií,
- odstraňovanie zistených nedostatkov APV.

19. Rozšírená podpora nábehu rutinnej prevádzky

Pri nábehu systémov IS SA a po ich zavedení do rutinnej prevádzky bude zhotoviteľ zabezpečovať zvýšenú podporu podľa potrieb objednávateľa. Realizuje sa skúšobný pilot, retestovanie za účasti zhotoviteľa a preklopenie do produkcie. Počas tohto obdobia bude zabezpečená účasť zástupcov zhotoviteľa pre jednotlivé fázy nábehu priamo v priestoroch zákazníka.

V rámci rozšírenej podpory nábehu rutinnej prevádzka budú vykonávané činnosti:

- Príprava predprodukčnej prevádzky
- Retestovanie za účasti zhotoviteľa
- Dohľad nad nábehom systému
- Koučovanie zamestnancov objednávateľa
- Zvýšená konzultačná podpora – účasť implementačných tímov zhotoviteľa na mieste

Zhotoviteľ poskytne Rozšírenú podporu nábehu rutinnej prevádzky podľa potrieb objednávateľa pri zavedení do rutinnej prevádzky verzií IS SA , ktorých funkcionalita pokrýva legislatívne zmeny vyplývajúce z novely zákona o občianskych preukazoch platných k 1.7.2012 a pri zavedení finálnej verzie IS SA do rutinnej prevádzky.

20. Zoznam použitých skratiek

Skratka	Popis
IS SA	Informačný systém správnych agend
IS REGOB	Informačný systém registra obyvateľov
ECU	Evidencia cudzincov
APV	Aplikačné programové vybavenie
eID	Elektronická identifikačná karta
eDoPP	Elektronické povolenie na pobyt
SR	Slovenská republika
JP	Jednotné pracoviská
OP	Občiansky preukaz
REGOB	Register obyvateľov
NPC	Národné personalizačné centrum
OCP	
DoPP	Doklad o povolení na pobyt
CUP	Cudzinecký pas
NPP	Nálepka povolenie na pobyt
MPS	Doklad malého pohraničného styku
CLK	Centrálna lustračná konzola
VIS	Vízový IS
IS ECU	Informačný systém evidencie cudzincov
CVS	Centrálne výpočtové stredisko MV SR
IS MV SR	Informačný systém MV SR
MV SR	Ministerstvo vnútra RS

ČAST III ROZŠÍRENIE TECHNICKÉHO RIEŠENIA PRE JEDNOTNÉ PRACOVISKÁ MV PRE ZBER ŽIADOSTÍ NA VYDÁVANIE ELEKTRONICKÝCH EID KARIET

1. Súlad riešenia s relevantnými normami

Bezpečnostné mechanizmy a PKI

- Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)Version 2.0

Normy pre kontaktné čipové karty

- ISO/IEC 7816-1-Integrated Circuit(s) Cards with Contacts - Part 1: Physical Characteristics
- ISO/IEC 7816-2-Integrated Circuit(s) Cards with Contacts - Part 2: Dimensions and Location of the Contacts
- ISO/IEC 7816-3-Integrated Circuit(s) Cards with Contacts - Part 3: Electronic Signals and Transmission

Protocols

- ISO/IEC 7816-4-Integrated Circuit(s) Cards with Contacts - Part 4: Interindustry Commands for Interchange
- ISO/IEC 7816-4-/Amd1-Integrated Circuit(s) Cards with Contacts - Part 4: Interindustry Commands for Interchange AMENDMENT 1: Impact of Secure Messaging on the Structures of APDU Messages
- ISO/IEC 7816-5-Integrated Circuit(s) Cards with Contacts - Part 5: Numbering System and Registration Procedure for Application Identifiers
- ISO/IEC 7816-6-Integrated Circuit(s) Cards with Contacts - Part 6: Interindustry Data Elements
- ISO/IEC 7816-8-Integrated Circuit(s) Cards with Contacts - Part 8: Security Related Interindustry Commands
- ISO/IEC 7816-9-Integrated Circuit(s) Cards with Contacts - Part 9: Additional Interindustry Commands and Security Attributes
- ISO/IEC 7816-10-Integrated Circuit(s) Cards with Contacts - Part 10: Electronic Signals and Answer to Reset for Synchronous Cards
- Certifikácia pre kryptografický modul kontaktnej čipovej karty minimálne podľa štandardu FIPS -140 level 2 alebo Common Criteria EAL 4+ (ISO-IEC-15408)
- Certifikácia v zmysle §10, ods. 2 písm j) zákona NR SR č. 215/2002 o elektronickom podpise

Biometria

- ISO/IEC 19794-5:2005, Biometric Data Interchange Formats – Part 5: Face Image Data
- ISO/IEC 19794-4:2005, Biometric Data Interchange Formats – Part 5: Finger Image Data
- ANSI/NIST-ITL 2-2008, XML Version of ANSI/NIST-ITL 1-2007, American National Standard for Information Systems—Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information – Part 2: XML Version

2. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej súťaži v prílohe B1 - Opis predmetu zákazky časť III: „Rozšírenie technického riešenia pre Jednotné pracoviska MV pre zber žiadosti na vydávanie eID kariet“.

3. Predmet Technického riešenia

Predmetom ponuky je rozšírenie technického riešenia informačného systému Integrovaného riešenia Jednotných pracovísk pre zber žiadostí od občanov, zber údajov, kontrolu údajov, kontrolu dokladov a vydávanie vodičských preukazov, cestovných pasov a občianskych preukazov v pôsobnosti ODE PPZ (ďalej IS JP), a rozšírenie technického riešenia informačného systému Integrovaného riešenia Jednotných pracovísk na objednávanie výroby dokladov v pôsobnosti ÚHCP MV SR (ďalej IS OVD), na zabezpečenie funkcionality vydávania a používania elektronických ID kariet.

Cieľom požadovaných úprav a rozšírení technického riešenia Jednotných pracovísk je zabezpečenie vydávania elektronických identifikačných dokladov SR, menovite elektronickej ID karty (eID) a elektronického dokladu o povolení na pobyt cudzinca (eDoPP).

V súčasnosti IS JP pre občianske preukazy podporuje vydávanie ID kariet bez čipu, resp. IS OVD vydávanie dokladov povolenia na pobyt cudzinca (ďalej DoPP) bez čipu. Technické riešenie pozostáva z funkčných (aplikačných) blokov:

- Aplikácia „Workflow“ podporuje podanie a spracovanie žiadosti o doklad, pričom vytvorí žiadosť so zodpovedajúcimi alfanumerickými a biometrickými dátami podľa typu žiadosti.
- Aplikácia „Biometria“ umožňuje zosnímať fotografiu tváre, odtlačky prstov a podpis a zabezpečuje kontrolu kvality a overovanie totožnosti pomocou Kontrolného systému biometrie na základe odtlačkov prstov (iba pre potreby ÚHCP MV SR) a podoby tváre.
- Aplikácia „Sledovanie životného cyklu a distribúcie dokladu“ poskytuje informácie a reporty o aktuálnom stave dokladov. Zároveň zabezpečuje automatizovanú podporu procesu distribúcie vyrobených dokladov medzi NPC a JP resp. procesu distribúcie dokladov medzi jednotlivými JP. Zároveň podporuje proces preberania dokladov po prevzatí balíka personalizovaných dokladov na JP.
- Aplikácia „Vydanie dokladov“ zabezpečuje proces identifikácie predloženej žiadosti, a vykonanie všetkých náležitostí spojených s vydaním dokladu držiteľovi.

- Kontrola dokladov je zabezpečená aplikáciami „Kontrola dokladov“ a „EAC PKI“, spolu vytvárajúcimi Inšpekčný systém na kontrolu dokladov. Kontrola identifikačného dokladu spočíva predovšetkým v overení jeho autentickosti a integrity ako v optickej, tak v elektronickej časti, a v poskytnutí takto získaných údajov. Špecifickým použitím je overenie funkčnosti elektronickej časti nového dokladu a zobrazenie obsahu čipu (ak doklad čip obsahuje) pri jeho vydaní držiteľovi. Aplikácia „EAC PKI“ má špecifickú úlohu poskytovania resp. distribúcie certifikátov potrebných na vykonávanie kontroly dokladov.

V rámci podprojektu zrealizované riešenie umožní vydávanie nového typu občianskeho preukazu – elektronickej ID karty a elektronického DoPP. Požadované úpravy technického riešenia Jednotných pracovísk musia zabezpečiť poskytovanie všetkých súvisiacich služieb na jednom mieste čo najjednoduchším spôsobom, bez zbytočných komplikácií a prieťahov, tak, aby bol priebežne informovaný o stave vybavovania svojej žiadosti.

Rozšírenie Kontrolného systému biometrie prinesie zvýšenú bezpečnosť procesov vydávania dokladov povolenie na pobyt cudzinca a cudzineckých cestovných dokladov, ako aj samotnej identifikácie držiteľov týchto dokladov.

Súčasný Inšpekčný systém Jednotných pracovísk na kontrolu dokladov nebude v rámci tohto projektu upravovaný. Kontrola, overenie funkčnosti a postpersonalizácia dokladov eID a eDoPP v rozsahu požiadaviek predloženého „Opisu predmetu zákazky“ bude zabezpečená príslušnými modulmi jednotného inšpekčného systému pre eID a eDOPP, integrovaným cez jeho klientsky komponent do technického riešenia Jednotných pracovísk.

Požadované úpravy požadovaným spôsobom zabezpečia vydávanie elektronických identifikačných dokladov SR, menovite eID a eDoPP.

4. Popis navrhovaného riešenia

Pre účely vydávania nového typu občianskeho preukazu – elektronickej ID karty a elektronického DoPP budú vykonané:

- úpravy a rozšírenia technického riešenia informačného systému Integrovaného riešenia Jednotných pracovísk v pôsobnosti ODE PPZ, vrátane úpravy systémových a procesných rozhraní na technické riešenie správnej agendy občianskych preukazov,
- úpravy a rozšírenia technického riešenia informačného systému Integrovaného riešenia Jednotných pracovísk v pôsobnosti ÚHCP MV SR, vrátane úpravy systémových a procesných rozhraní na technické riešenie správnej agendy evidencia cudzincov,
- vytvorenie systémových a procesných rozhraní na riešenie DVCA certifikačnej autority pre vydávanie eID a eDoPP kariet,
- vytvorenie a integrácia klientskeho komponentu jednotného inšpekčného systému pre eID a eDoPP do agendy Jednotných pracovísk,
- implementácia serverovského komponentu jednotného inšpekčného systému pre eID a eDoPP,
- rozšírenie a dobudovanie kontrolného systému biometrie pre Jednotné pracoviská ÚHCP MV SR o centrálnu funkcionalitu identifikácie a kontroly duplicitných identít na základe biometrických údajov.

Súčasťou rozšírenia technického riešenia bude dodávka softvéru, hardvéru a systémového softvéru, menovite:

- Hardvérové vybavenie potrebné pre implementáciu Jednotného inšpekčného systému a Rozhrania na Zastupiteľské úrady v prostredí záložného výpočtového strediska OSK SITB MV SR
- Hardvérové vybavenie servrov Kontrolného systému biometrie pre centrálnu funkcionalitu identifikácie a kontroly duplicitných identít na základe biometrických údajov
- Softvérové vybavenie servrov Kontrolného systému biometrie pre centrálnu funkcionalitu identifikácie a kontroly duplicitných identít na základe biometrických údajov – licencie na 50.000 identít z odtlačkov desiatich prstov a 150.000 identít s fotografiou tváre
- Softvérové vybavenie pre správu off-line žiadostí a systémových číselníkov pre potreby mobilných pracovísk
- Hardvérové a softvérové vybavenie pre obsluhu eID a eDoPP na strane klienta Jednotného inšpekčného systému – čítačka kontaktných čipov s ovládačmi pre pracoviská pre zber žiadostí a pre pracoviská pre výdaj dokladov v počte 410 ks
- Celostranové čítačky na kontrolu elektronických cestovných dokladov v počte 44 kusov.

5. Procesný model

5.1. Popis procesu vydávania eID resp. eDoPP

Procesný model sa zameria predovšetkým na mapovanie kľúčových procesov.

Procesné mapy budú dokumentované vo forme schém realizovaných vo vhodnom CASE nástroji.

5.1.1 Podanie žiadosti na JP

5.1.1.1. Prijatie žiadosti o vydanie dokladu

Pracovník JP prijme od občana žiadosť o vydanie dokladu v písomnej alebo ústnej forme. Občan je povinný identifikovať sa predpísaným preukazom totožnosti (občianskym preukazom alebo pasom). Pracovník JP zosníma MRZ z predloženého preukazu totožnosti identifikačné údaje, prípadne zadá identifikačné údaje občana ručne. Systém overí, či sa predložený preukaz totožnosti nenachádza v evidencii stratených/odcudzených dokladov.

Na základe identifikačných údajov získa pracovník JP z registra obyvateľov aktuálne referenčné údaje. Získané údaje z registra obyvateľov môže porovnať s údajmi uvedenými na písomnej žiadosti a dodatočne tak overiť identitu osoby a platnosť údajov uvedených na žiadosti a predložených dokladoch. Pri zadani žiadosti na JP o doklad eID resp. eDoPP môže občan zadať bezpečnostný kod PIN, ktorý bude uložený v šifrovanej podobe ako súčasť žiadosti o doklad.

5.1.1.2. Preverenie držiteľa dokladu

Po identifikácii občana je automaticky zrealizovaná kontrola, či spĺňa podmienky pre vydanie dokladu. O výsledku kontroly je informovaná obsluha systému.

5.1.1.3. Vygenerovanie a zaevidovanie systémovej žiadosti

Na základe údajov získaných z registra obyvateľov (resp. IS ECU) je systémom vytvorená nová žiadosť, ktorá bude obsahovať aktuálne požadované údaje žiadateľa z registra obyvateľov (resp. IS ECU).

Pracovník JP na základe okolností potvrdí alebo zmení výšku správneho poplatku určenú systémom a spôsob jeho úhrady, a po jeho uhradení zaeviduje túto skutočnosť v systéme.

Pracovník JP následne žiadosť vytlačí a predloží na podpis občanovi. Súčasťou vytlačenej žiadosti bude jednoznačné identifikačné číslo žiadosti vo forme jednorozmerného čiarového kódu. Po podpísaní žiadosti pracovník JP zaeviduje žiadosť v systéme. Dátum podania žiadosti bude nastavený na aktuálny dátum. Zároveň je vytvorený záznam o doklade (Stav dokladu = Požadovaný).

5.1.1.4. Kompletizácia žiadosti

Po zaevidovaní systémovej žiadosti je vykonaná jej kompletizácia, t.j. občan sa podrobí zosnímaniu fotografickej podoby tváre, podpisu. Súčasťou snímania je aj proces kontroly kvality zosnímaných údajov podľa platných štandardov a smerníc. Fotografická podoba tváre je automaticky porovnaná s predchádzajúcou elektronicky zosnímanou fotografiou osoby, aby sa znížila pravdepodobnosť nechcenej či plánovitej zámene identít. Po úspešnom zosnímaní a uložení osobných údajov sú tieto na základe potvrdenia pracovníkom JP pripojené k systémovej žiadosti. Po tomto úkone je žiadosť automaticky schválená a prostredníctvom IS SA postúpená na personalizáciu do NPC.

5.1.2 Prevzatie vyrobeného dokladu z NPC na JP

5.1.2.1. Fyzické prevzatie balíku z NPC

Pracovník JP prevezme balík s dokladmi od kuriérskej služby a potvrdí doručenku.

5.1.2.2. Kontrola doručených dokladov

Po prevzatí balíka od kuriérskej služby je pracovníkom JP realizovaná fyzická kontrola doručených dokladov. Kontroluje sa obsah doručeného balíka oproti odovzdávaciemu protokolu a záznamom v systéme. Po zadaní identifikačného čísla balíku sa pracovníkovi JP zobrazí zoznam dokladov, ktoré mali byť v balíku fyzicky doručené.

- Ak sa doklad nachádza v balíku aj v elektronickej evidencii, vykoná pracovník JP vizuálnu kontrolu dokladu a overenie platnosti údajov na ňom oproti údajom uloženým v systéme. Zároveň vykoná overenie údajov uložených v elektronickom čipe oproti údajom uloženým v systéme. V prípade, že bolo zistené poškodenie dokladu alebo chyba v údajoch na doklade, zaznamená túto skutočnosť v elektronickej evidencii (Stav dokladu = Poškodený) a iniciuje prioritné vyrobenie nového dokladu na základe údajov z existujúcej systémovej žiadosti. V prípade, že je doklad v poriadku, zaznamená jeho prevzatie v elektronickej evidencii (Stav dokladu = Prevzatý na vydanie). Držiteľ, dokladu je notifikovaný dohodnutým komunikačným kanálom (SMS, email) o pripravenosti dokladu na vydanie.
- Ak sa doklad nachádza v balíku a nenachádza sa vo výsledku vyhľadania, je potrebné ho dohľadať manuálne. Na dohľadanie sú použité identifikačné údaje žiadateľa resp. žiadosti. Po nájdení dokladu v elektronickej evidencii vykoná pracovník JP vizuálnu kontrolu dokladu a overenie platnosti údajov na ňom oproti údajom uloženým v systéme. Zároveň vykoná overenie údajov uložených v elektronickom čipe oproti údajom uloženým v systéme. V prípade, že bolo zistené poškodenie dokladu alebo chyba v údajoch na doklade, zaznamená túto skutočnosť v elektronickej evidencii (Stav dokladu = Poškodený) a iniciuje prioritné vyrobenie nového dokladu na základe údajov z existujúcej systémovej žiadosti. V prípade, že je doklad v poriadku, zaznamená jeho prevzatie v elektronickej evidencii (Stav dokladu = Prevzatý na vydanie). Držiteľ, dokladu je notifikovaný dohodnutým komunikačným kanálom (SMS, email) o pripravenosti dokladu na vydanie.
- Ak existuje iba elektronický záznam a požadovaný doklad nebol doručený v balíku, zaznamená sa neprevzatie dokladu v elektronickej evidencii (Stav dokladu = Stratený).

V prípade potreby je možné na kontrolu dokladov použiť aj automatizované prostriedky kontroly dokladov v rozsahu funkcionality modulov jednotného inšpekčného systému pre eID a eDoPP.

Po ukončení kontroly pracovník JP zo systému vytlačí preberací protokol. Systém zároveň vygeneruje elektronický preberací protokol a zabezpečí jeho distribúciu v elektronickej forme do NPC.

O skutočnosti, že jeho doklad je pripravený na vydanie, je občan informovaný prostredníctvom SMS resp. elektronickej pošty, pokiaľ o takúto službu pri podaní žiadosti požiadal.

5.1.3 Osobné odovzdanie dokladu držiteľovi na JP

5.1.3.1. Preverenie držiteľa dokladu

Po identifikácii občana je automaticky zrealizovaná kontrola, či spĺňa podmienky pre vydanie dokladu. O výsledku kontroly je informovaná obsluha systému.

5.1.3.2. Odovzdanie dokladu

Občan prevezme doklad a potvrdí jeho prevzatie. Doklad môže byť doručený občanovi v obálke ak to občan v procese žiadosti požiada.

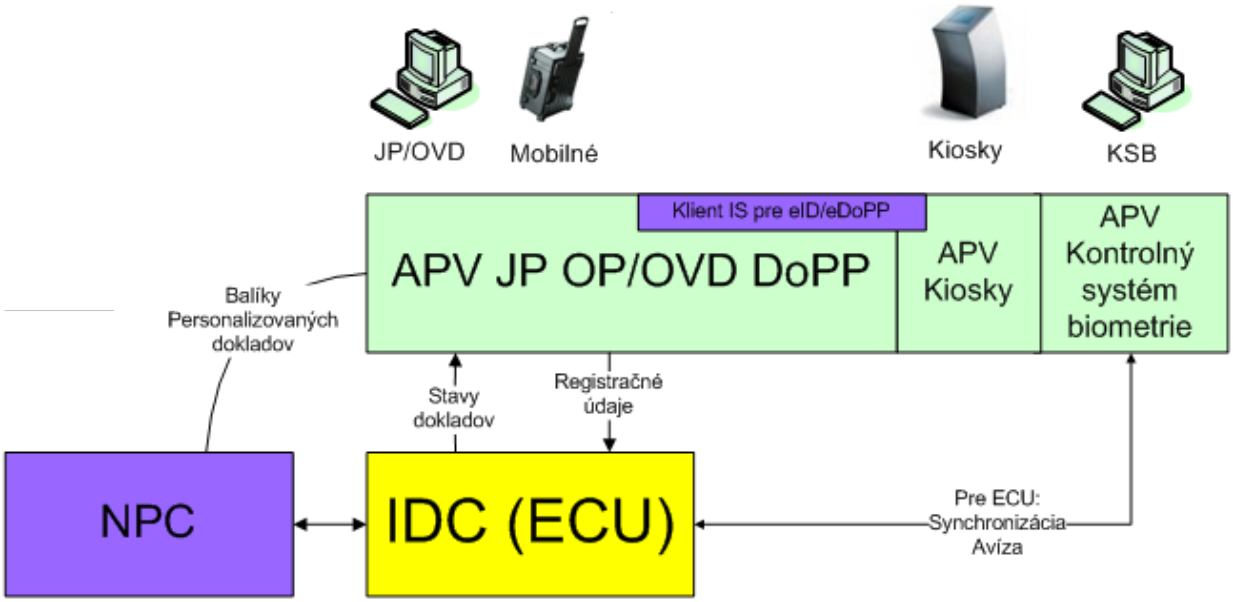
6. Funkčný návrh systému

Funkčný návrh systému sa zameria predovšetkým na:

- funkčnú dekompozíciu navrhovaného riešenia
- dokumentáciu požadovanej funkcionality
- popis požadovaných atribútov kvality riešenia.

V rámci tejto časti riešenia budú v súvislosti s vydávaním a kontrolou nových typov dokladov eID a eDoPP rozšírené, resp. implementované nasledovné kľúčové subsystémy:

- Informačný systém Integrovaného riešenia Jednotných pracovísk v pôsobnosti ODE PPZ,
- Informačný systém Integrovaného riešenia Jednotných pracovísk v pôsobnosti ÚHCP MV SR,
- Jednotný inšpekčný systém,
- Kontrolný systém biometrie pre Jednotné pracoviská ÚHCP MV SR,
- Kiosky.



Obrázok č.1– Začlenenie IS JP do okolitých IS

6.1. Jednotný inšpekčný systém

Pre kontrolu dokladov bude vybudovaný Jednotný inšpekčný systém tak, aby umožňoval aj kontrolu dokladov eID a eDoPP, pri zachovaní modulu na kontrolu cestovných dokladov so sekundárnou biometriou (ePas). Vybudovaním takéhoto Inšpekčného systému vznikne Jednotný inšpekčný systém (JIS) ako univerzálna platforma pre kontrolu dokladov vydávaných v rámci rezortu MV SR.

Oprávnenie pracovníka (resp. inšpekčného terminálu) pre vykonávanie kontroly dokladov eID resp. eDoPP bude riadené prostredníctvom služieb JIS prepojeného na centrálnu správu používateľov LDAP.

JIS bude integrovaný s aplikáciou pre riadenie personalizácie a logistiky výroby (NPC), aplikáciou pre JP (jednotné pracoviská) a aplikáciou pre Kiosky.

6.1.1 Služby JIS

JIS poskytuje nasledujúce nové služby:

- kontrola dokladov eID a eDoPP,
- zápis a modifikácia údajov dokladu eID a eDoPP,

- podpora pre post-personalizáciu dokladov eID a eDoPP.

JIS bude zohľadňovať požiadavky pre podporu viacerých typov terminálov a typov dokladov, čím vznikne Jednotný inšpekčný systém pre kontrolu všetkých v rezorte vydávaných elektronických dokladov:

Podporované typy dokladov	eID a eDoPP, ako aj ePas na základe funkčnosti existujúceho modulu na kontrolu cestovných dokladov so sekundárnou biometriou
Podporované typy terminálov	JIS v inšpekčnom móde pre kontrolu dokladu (eID, eDoPP, resp. aj ePas), JIS v autentifikačnom móde pre kontrolu dokladu s nutnosťou zadať PIN (eID, eDoPP), JIS v autentifikačnom móde pre postpersonalizáciu na CA/RA s nutnosťou zadať PIN (eID, eDoPP), JIS v autentifikačnom móde pre zmenu a zápis údajov na JP s nutnosťou zadať PIN (eID, eDoPP).
Komunikácia s PKI infraštruktúrou MV SR	JIS bude používať PKI infraštruktúru MV SR pre podpis IS certifikátov, ako aj pre import CSCA, DS, CVCA a DV certifikátov.

6.1.2 Funkcionalita JIS

JIS bude implementovať nasledujúcu funkcionalitu:

6.1.2.1. Kontrola a vyčítanie dokladu

- overenie autenticity dokladu vykonaním čipovej, pasívnej a terminálovej autentifikácie
- vyčítanie údajov z čipu a kontrola voči MRZ
- funkčného rozhranie pre aplikáciu tretej strany, napr. aplikáciu pre JP (jednotné pracoviská) - poskytnutie výsledku kontroly a vyčítaných údajov.

6.1.2.2. Modifikácia údajov na karte

- otvorenie dokladu pre zápis vykonaním čipovej, pasívnej a terminálovej autentifikácie
- funkčného rozhranie pre aplikáciu tretej strany, napr. aplikáciu pre JP (jednotné pracoviská)
- zápis údajov do karty
- zápis resp zmena PIN na karte

Pozn.: Pre terminálovú autentifikáciu sa v tomto prípade použije CV certifikát typu „Autentifikačný certifikát s právom pre zápis“ – autentifikačný mód JIS. Zapisovať / modifikovať bude možné len dátové skupiny DG17 až DG21.

6.1.2.3. Postpersonalizácia

- otvorenie dokladu pre zavedenie novej kartovej aplikácie vykonaním čipovej, pasívnej a terminálovej autentifikácie
- funkčné rozhranie pre postpersonalizáciu treťou stranou, napr. CA/RA
- sprostredkovanie komunikácie s čipom dokladu eId / eDoPP za účelom zavedenia novej kartovej aplikácie

Pozn.: Pre terminálovú autentifikáciu sa v tomto prípade použije CV certifikát typu „Autentifikačný certifikát s právom pre zavedenie novej aplikácie“ – autentifikačný mód JIS. Pre inštaláciu ZEP resp. AC sa bude jednať o oprávnenia: Install Qualified Certificate a Install Certificate.

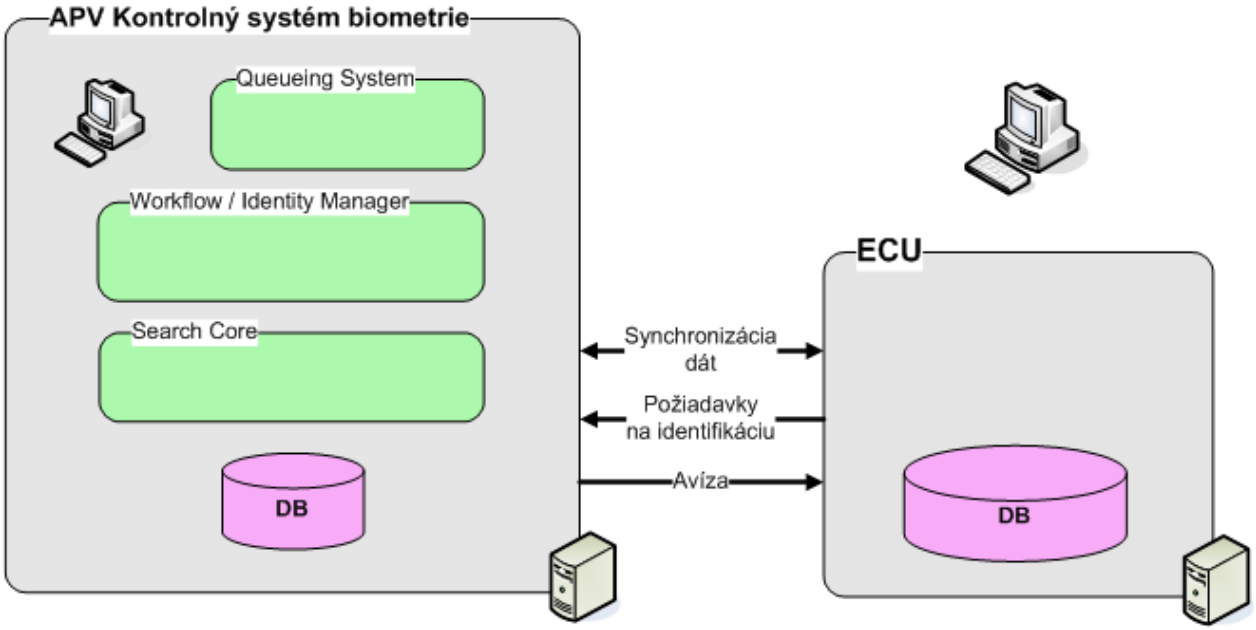
6.1.2.4. Služby PKI

- Funkcionalita pre generovanie kľúčového páru IS
- Komunikácia s PKI infraštruktúrou DV CA za účelom
  - vydania certifikátu pre terminálovú autentifikáciu (IS certifikát)
  - získania certifikátov CSCA, DS, CVCA, DV
- Komunikácia s HSM počas terminálovej autentizácie

6.2. Kontrolný systém biometrie

Kontrolný systém biometrie pre Objednávanie výroby dokladov ÚHCP MV SR bude rozšírený o centrálnu funkcionalitu identifikácie a kontroly duplicitných identít na základe biometrických údajov:

- Existujúce biometrické záznamy, t.j. existujúce identity + obrazové súbory (fotografie, odtlačky) budú vyexportované z biometrickej databázy ECU do Kontrolného systému biometrie. Kontrolný systém biometrie (Workflow / Identity Manager) tieto dáta spracuje a vykoná úvodnú kontrolu duplicitných identít.
- Pri každom zosnímaní nových biometrických údajov prostredníctvom OVD a ich následnom uložení nových do biometrickej databázy ECU pripraví pre Kontrolný systém biometrie nasledujúce údaje: identitu osoby, obrazové súbory (fotografie, odtlačky). Kontrolný systém biometrie tieto dáta spracuje a vykoná kontrolu duplicitných identít.
- Pri snímaní nových biometrických údajov v rámci činností OVD bude možnosť okrem štandardného overenia totožnosti na základe zosnímaných biometrických údajov voči evidovaným biometrickým údajom (verifikácia) získať aj informácie o identifikácii osoby na základe zosnímaných biometrických údajov voči záznamom v Kontrolnom systéme biometrie.
- Výsledky kontroly duplicitných záznamov a procesu identifikácie budú došetrené v rámci Kontrolného systému biometrie (Queueing System) na dvoch na to určených pracoviskách. Výsledky budú evidované v rámci Kontrolného systému biometrie, a následne publikované vo forme avíza v rámci ECU.
- V prípade potreby bude možné v rámci OVD zmeniť priradenia biometrických záznamov k identite. Keď sa tak stane, potom ECU postúpi túto informáciu Kontrolnému systému biometrie, ktorý zaslané dáta spracuje a zmení priradenie biometrických záznamov k identite.

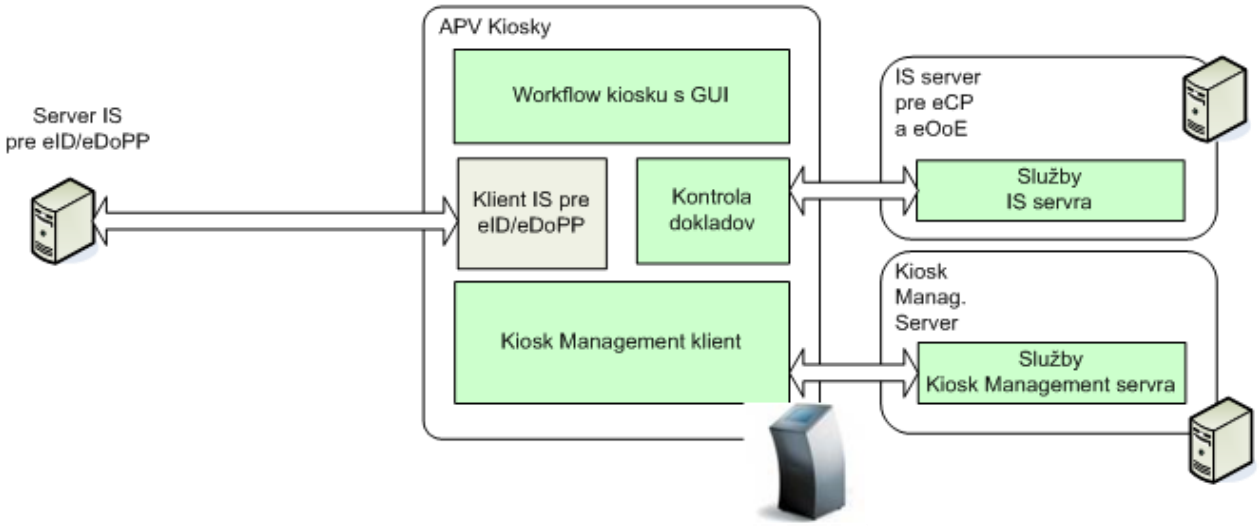


Obrázok č. 2 – Komponentová architektúra subsystému Kontrolný systém biometrie

6.3. Samoobslužné kiosky

Poskytovanie služieb modulov jednotného inšpekčného systému pre eID a eDoPP bude zabezpečené aj v prostredí samoobslužných terminálov, dodaných v rámci projektu zabezpečenia vydávania elektronických

osvedčení o evidencii vozidiel. Toto bude realizované integráciou klientských komponentov modulov Jednotného inšpekčného systému pre eID a eDoPP do aplikácie kiosku.



Obrázok č. 3 – Komponentová architektúra subsystému Samoobslužné kiosky

Na kioskoch budú zároveň sprístupnené vybrané e-Government služby. Podmienkou zahrnutia služby do prostredia aplikácie kiosku je sprístupnenie klientskej časti služby prostredníctvom webového klienta v prostredí Microsoft Internet Explorer a kompatibilita s HW prostredím kiosku.

6.4. Vybrané dodávané HW komponenty

6.4.1 Čítačka kontaktných čipov - Čítačka čipových kariet

Čítačka kontaktných čipov je Plug & Play USB čítačka čipových kariet s prenosovou rýchlosťou do 344 kbps. Vďaka zhode so všetkými industry štandardmi je táto čítačka kompatibilná prakticky s každou čipovou kartou. Čítačka kontaktných čipov je navrhnutá tak aby podporovala všetky hlavné štandardy. Kryt čítačky je navrhnutý tak aby sa dala umiestniť horizontálne.

Základné technické parametre

Podpora štandardov	ISO 7816 Class A a AB, FCC Class B part 15, CE, VCCI, USB-IF, Microsoft WHQL
Rozhranie SC	PC/SC alebo CT-API (cez wrapper on top of PC/SC)
Prenosová rýchlosť	s PC: 12Mbps (USB 2.0) s čipovou kartou: do 344Kbps
Operačný systém	Windows 7, Windows Vista, Windows XP, MacOS, Solaris, Linux 32 bit / 64 bit
Rozhranie	USB 2.0
Napájanie	Cez USB

USB kábel je súčasťou zariadenia.

6.4.2 Celostranové dokladové čítačky

Celostranové čítačky na kontrolu elektronických cestovných dokladov Viisage iA-thenticate RFID Color potrebujú pre svoju funkčnosť počítač. Minimálne HW nároky takéhoto počítača sú: Pentium IV (3.0 GHz), Windows XP, 512MB RAM, 500MB diskového priestoru, neobsadené rozhranie USB 2.0.

Multifunkčné zariadenie na kontrolu identifikačných dokladov je hardwareová platforma navrhnutá pre autentifikáciu dokumentov ako sú pasy, vodičské preukazy a ID karty. Použitím viacerých zdrojov svetla čítačka vykonáva viacnásobné bezpečnostné overovanie. iA-thenticate overuje MRZ (machine-readable zone) kontrolný súčet, dátum expirácie a overuje prítomnosť atramentu B900. Softvérové vybavenie zariadenia umožňuje čítať a analyzovať informácie obsiahnuté v cestovných dokladoch a dokladoch totožnosti a porovnávať ich s databázou bezpečnostných prvkov dokladov.

Základné technické parametre

Funkčnosť	vloženie dokladu do čítačky jednou rukou bez nutnosti pridŕžať doklad počas čítania
	automatická detekcia dokladu
	tienidlo pre potlačenie vplyvu vonkajšieho rušivého osvetlenia
	viacnásobné čítanie dokladov v rôznych vlnových dĺžkach
	zber OCR dát (strojovo čitateľná zóna)
	vylepšená schopnosť čítania a zápisu bezkontaktných čipov
Zobrazovanie	schopnosť zobrazovania v 24 bitových farbách
Komunikačný protokol	ISO 14443 typ A a typ B ICs
Kompatibilita	MS Windows 2000/XP (požiadavka na ovládače)
Kompatibilita	kompatibilita s referenčným testovacím prostredím, tzv. Golden Reader Tool (GRT), verzia 2.5.0 a vyššia
Rozhranie	USB 2.0
Napájanie	220V

Spektrálny rozsah a rozlíšenie

Skenovanie dokladov vo vlnových dĺžkach	infračervené svetlo (IR): IR B900 (ISO-1831), 890 nm (špička vyžarovania)
	viditeľná oblasť spektra: 400 - 700 nm spektrálneho rozsahu
	ultrafialové svetlo (UV): 370 nm (špička vyžarovania)
Optická hĺbka	24 bitov (farba)
Efektívne výstupné rozlíšenie	400 dpi

Napájací zdroj aj USB kábel je súčasťou dodávky.

7. Návrh (dizajn) APV

Návrh (dizajn APV bude riešiť predovšetkým kľúčové princípy dizajnu pre:

- používateľské rozhrania (GUI),
- business logiku (komponenty, web služby a pod.),
- aplikačné programové rozhrania (API),
- perzistentnú vrstvu.

Celý systém bude v čo najväčšej miere podporovať procesy agendových a evidenčných úkonov a minimalizovať nutné úkony obsluhy.

Zálohovanie dát (Backup) bude vykonávané automaticky jestvujúcimi prostriedkami infraštruktúry výpočtového strediska OSK SITB MV SR. Obsluha má zabezpečovať len výmenu zálohovacích dátových médií.

Systém musí byť navrhnutý tak, aby – pokiaľ je to zmysluplné – jeden človek mohol zastávať jednu, viac alebo všetky pracovné role odrazu. Systém má umožňovať zmenu priradenia človeka (pridanie/uberanie) k jednotlivým pracovným roliam bez nutnosti odstávky systému.

8. Externé rozhrania

Súčasťou dodávky bude aj úprava nasledujúcich rozhraní na systémy upravované v rámci tohto projektu:

- rozhranie na technické riešenie správnej agendy občianskych preukazov (IDC)
- rozhranie na technické riešenie správnej agendy evidencia cudzincov (ECU).

9. Dokumenty a dokumentácia

V rámci projektu budú dodané nasledovné dokumenty v slovenskom jazyku:

- Procesný model
- Špecifikácia (analýza) požiadaviek
- Detailná špecifikácia rozhraní
- Plán testov vrátane návrhu testovacích procedúr
- Technická a prevádzková dokumentácia
- Používateľská dokumentácia

Dokumenty budú dodané v tlačenej forme v počte 1 kus ako aj v elektronickej forme v počte 1ks na CD nosiči.

V rámci projektu bude dodaná nasledovná dokumentácia:

- Dokumentácia k HW komponentom – Štandardná dokumentácia od výrobcov k jednotlivým HW komponentom. Pokiaľ nie je dostupná v slovenskom jazyku, táto bude dodaná v anglickom jazyku, vo formáte poskytovanom výrobcom.

10. Školenia

V rámci dodávky budú vykonané nasledovné školenia:

Názov	Počet účastníkov	Jeden turnus	Dĺžka trvania	Typ školenia / školiaci priestor	Čas vykonania
Školenie pracovníkov OTI („školenie č.1“)	30	30	0,5 dňa	Školiaca miestnosť	V súlade s Harmonogramom
Školenie administrátorov OSK SITB MV SR („školenie č.2“)	5	5	1 deň	Výpočtové stredisko, zasadačka	V súlade s Harmonogramom
Školenie užívateľov APV Jednotných pracovísk („školenie č.3“)	600	100, podľa kapacity	1 deň	Aulové školenie	V súlade s Harmonogramom
Školenie odborných používateľov Kontrolného systému biometrie („školenie č.4“)	5	5	3 dni	Určené pracovisko	V súlade s Harmonogramom

Školenie pracovníkov OTI a Školenie administrátorov OSK SITB MV SR bude vykonané na základe dispozícií objednávateľa podľa možnosti spoločne s týmto typom školení v rámci subprojektu „Rozšírenie technického riešenia pre Jednotné pracoviská MV o Mobilné pracoviská na zber žiadostí pre vydávane elektronických eID kariet“.

Školenie č. 4 je určené pre 5 expertných používateľov kontrolného systému biometrie, ktorí budú centrálne spracúvať a vyhodnocovať jednotlivé prípady nálezov pri kontrole duplicitných identít na dvoch na to určených pracoviskách.

Školiace priestory dostatočnej veľkosti s potrebnou infraštruktúrou zabezpečí objednávateľ.

Miesto konania školenia objednávateľ spresní najneskôr dva týždne pred konaním školenia.

Termíny školení bude spresnený v projektovom pláne.

V rámci aktivity Školenie objednávateľ okrem toho, že zrealizuje vlastné školenia zamestnancov objednávateľa, vykoná všetky činnosti spojené s prípravou a vyhodnotením školení. Zhotoviteľ pripraví školiace verzie systémov vrátane dát pre školenia, vytvorí užívateľské a administrátorské kontá v systémoch.

Po vlastnej realizácii školení vyhodnotí školiteľ spätnú väzbu účastníkov školenia na funkcionalitu a kvalitu APV.

Školiteľ zabezpečí praktické cvičenia pre zamestnancov objednávateľa na školiacich verziách systémov. Zhotoviteľ poskytne koučing zamestnancom objednávateľa pri osvojení si práce s novým APV.

Školiace materiály budú účastníkom školenia dodané najneskôr v deň školenia. Školenie bude vykonané v slovenskom jazyku.

11. Podpora rutinnej prevádzky

Po nasadení riešenia do riadnej rutinnej prevádzky u objednávateľa bude poskytnutá podpora počas 2 týždňov.

Pri podpore rutinnej prevádzky dodaného riešenia budú vykonávané najmä nasledovné činnosti:

- Metodická podpora súvisiaca so správou a používaním dodaného riešenia (monitorovacie činnosti a pod.),
- Iná metodickú podpora súvisiacu s používaním dodaného riešenia.

12. Mimo rozsahu dodávky

- Analýza a návrh vzájomnej integrácie administratívnych procesov realizovaných na JP a administratívnych procesov prebiehajúcich na registračných autoritách, následné spracovanie návrhu úpravy relevantných činností JP či návrhu nových činností, následná implementácia navrhnutých úprav
- Rozhranie na riešenie RA registračnej autority pre vydávanie zaručeného elektronického podpisu
- Migrácia dát

13. Zoznam použitých skratiek

Skratka	Popis
APV	Aplikačné programové vybavenie
Biometrická databáza	Databáza biometrických údajov pri ECU
CP	Cestovný pas
eID	Elektronická ID karta, elektronický občiansky preukaz
eCP	Elektronický cestovný pas s biometriou
eDoPP	Elektronický doklad o povolení na pobyt
ECU	Agenda evidencie cudzincov
HW	Hardvér
IDC	Agenda občianskych preukazov
JP, IS JP	Jednotné pracoviská, Integrované riešenie Jednotných pracovísk pre zber žiadostí od občanov, zber údajov, kontrolu údajov, kontrolu dokladov a vydávanie vodičských preukazov, cestovných pasov a občianskych preukazov v pôsobnosti ODE PPZ
JP CP	Jednotné pracoviská pre cestovné pasy
JP OP	Jednotné pracoviská pre občianske preukazy
JP VP	Jednotné pracoviská pre vodičské preukazy
OoE I.	Elektronický doklad Osvedčenie o evidencii vozidla
OP	Občiansky preukaz, ID karta
OVD, IS OVD	Objednávanie výroby dokladov, Integrované riešenie Jednotných pracovísk na objednávanie výroby dokladov v pôsobnosti ÚHCP MV SR
SSW	Systémový softvér
SW	Softvér
VP	Vodičský preukaz

ČAST IV EGOVERNMENT SLUŽBY POSKYTUJÚCE OBČANOM MOŽNOSŤ REALIZÁCIE VYBRANÝCH SLUŽIEB PRE VYDÁVANIE ELEKTRONICKÝCH EID PROSTREDNÍCTVOM INTERNETU.

14. Súlad riešenia s relevantnými normami

Riešenie bude realizované v súlade so súvisiacou legislatívou a to najmä so Zákon o občianskych preukazoch a o zmene a doplnení niektorých zákonov č. 226/2006.

15. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej súťaži v prílohe B1 - Opis predmetu zákazky časť IV: „eGovernment služby poskytujúce občanom možnosť realizácie vybraných služieb pre vydávanie elektronických eID prostredníctvom Internetu“.

16. Predmet Technického riešenia

Predmetom technického riešenia je vybudovanie nadstavby nad IS SA Agenda občianskych preukazov na báze eGovernment služieb poskytujúcich možnosť realizácie transakčného spracovania v IS SA Agenda občianskych preukazov pre používateľov z Internetu.

Predmetom technického riešenia je realizácia nasledujúcich eGovernment služieb:

- Generovanie Autentifikačného certifikátu pre eID kartu
- Generovanie certifikátu na vytváranie elektronického podpisu pre eID kartu
- Generovanie Šifrovacieho certifikátu pre eID kartu
- Zrušenie Autentifikačného certifikátu pre eID kartu
- Zrušenie certifikátu na vytváranie elektronického podpisu pre eID kartu
- Overenie platnosti jednotlivých certifikátov držiteľa eID karty
- Vydanie eID karty žiadateľovi
- Nahlásenie straty eID karty

Predmetom technického riešenia je aj návrh a implementácia súvisiacich formulárov. Predmetom technického riešenia nie je integrácia elektronických formulárov na Web portál MV SR.

17. Procesný model a základný popis služieb

V nasledujúcej časti je uvedený koncepčný popis procesov súvisiacich s poskytovaním požadovaných elektronických služieb ako aj základné vymedzenie funkčnosti, poskytovanej dodávanými službami.

Definitívna detailizácia a spresnenie budú zrealizované v rámci projektu ako plnenie projektovej aktivity Vypracovanie procesného modelu resp. Funkčný návrh systému.

17.1. Generovanie Autentifikačného certifikátu pre eID kartu

Službu bude poskytnutá v NPC pri personalizacii karty, kľúčový par sa generuje na karte a na kartu sa zapisuje CVCA rootovy certifikát.

17.2. Generovanie certifikátu na vytváranie elektronického podpisu držiteľa eID karty

Služba umožní vygenerovanie kľúčového páru pre ZEP v karte a zápis prvotného kvalifikovaného certifikátu na pracoviskách RA v priestoroch JP. Služba umožní vygenerovanie kľúčového paru pre ZEP v karte a zápis

následného kvalifikovaného certifikátu vzdialene cez internet. Pre úplnú realizáciu služby je vyžadovaná súčinnosť zo strany MV SR popísaná v prílohe č.5.

17.3. Generovanie Šifrovacieho certifikátu pre eID kartu

Službu poskytuje ePerso v NPC pri personalizacii karty, generuje šifrovací kľúčový par, ktorý sa zapíše do karty. Pre úplnú realizáciu služby je vyžadovaná súčinnosť zo strany MV SR popísaná v prílohe č.5.

17.4. Zrušenie Autentifikačného certifikátu pre eID kartu

Služba zabráni autentifikácii, ak karta bola v agende označená ako ukradnutá, neplatná.

17.5. Zrušenie certifikátu na vytváranie elektronického podpisu pre eID kartu

Služba umožní zrušenie certifikátu pre ZEP vzdialene cez internet. Pre úplnú realizáciu služby je vyžadovaná súčinnosť zo strany MV SR popísaná v prílohe č.5.

17.6. Overenie platnosti jednotlivých certifikátov držiteľa eID karty

Pre kvalifikovaný certifikát:

Služba umožní online overiť platnosť certifikátu kvalifikovaného certifikátu. V prípade že príslušná ACA, ktorá vydala daný certifikát neposkytuje OCSP (Online Certificate Status Protocol), bude overená platnosť certifikátu voči poslednému vydanému CRL (certificate revocation list) danej ACA. Pre úplnú realizáciu služby je vyžadovaná súčinnosť zo strany MV SR popísaná v prílohe č.5.

Pre autentifikačný certifikát:

Služba sa realizuje ako služba agendy, ktorá odpovie AS, či je kartu možné použiť na autentifikáciu

17.7. Vydanie eID karty žiadateľovi

Cieľom služby pre podanie žiadosti o vydanie OP je vytvoriť možnosť podania žiadosti občana prostredníctvom portálu MV SR a navštíviť vybrané pracovisko JP vo vybranom čase za účelom nasnímania biometrických údajov (pokiaľ tieto údaje už nebudú platné).

Po spustení služby sa načítajú údaje pre predvyplnenie žiadosti o vydanie eID karty z IS IDC. Občanovi sa zobrazí na portáli MV SR predvyplnený formulár žiadosti o vydanie OP.

Občan skontroluje jeho správnosť a úplnosť, prípadne doplní formulár o údaje (osobitné záznamy) pre účely ich vypersonalizovania na OP, kontaktné údaje (mobilné číslo, email) pre účely informovania o stave pripravenosti prevzatia vyhotoveného OP a pracovisko doručenia, resp. adresu doručenia pre prípad doručenia kuriérom. Následne občan potvrdí zadané údaje.

17.8. Nahlásenie straty eID karty

Cieľom služby pre nahlásenie straty alebo odcudzenia OP je možnosť nahlásiť stratu alebo odcudzenie OP prostredníctvom portálu MV SR bez nutnosti navštíviť pracovisko JP.

Občanovi sa zobrazí formulár s možnosťou definovania udalosti (strata alebo odcudzenie), ktorá nastala pre aktuálne vydaný OP občana. Následne občan potvrdí zadané údaje.

Poznámka : Aby nedochádzalo k zneužitiu tejto služby nemôže byť táto služba poskytnutá anonymnému používateľovi. Preferovaný spôsob autentifikácie pre eGov služby použitím eID karty ako autentifikačného tokenu nebude možný, pretože používateľ eID kartu aktuálne nemá k dipozícii. Navrhované alternatívy pre autentifikáciu občana pri strate-ukradnutí eID karty sú :

- SMS: neautetifikovaný držiteľ pri nahlasovaní straty cez eGov službu dostane jednorazový kód cez SMS. Žiadosť je akceptovaná až po zadaní jednorazového kódu vo formulári tejto eGov služby. (analógia s SMS potvrdzovaním transakcií v internetovom bankovníctve)
- Meno a heslo: občan sa prihlási cez meno/heslo. Predpokladom je že občan má pridelené meno/heslo pre eGov služby. Spôsob pridelenia mena/hesla pre eGov služby nie je predmetom tohto dokumentu.

18. Návrh (dizajn) eGovernment služieb

Elektronické služby uvedené v predchádzajúcej kapitole budú zrealizované ako nové Web Service služby v rámci IS SA Agenda občianskych preukazov a Web Service služby iných informačných systémov, potrebné na zrealizovanie elektronickej služby.

Súčasťou návrhu riešenia bude aj návrh formulárov určených pre publikovanie na Web portály MV SR.

19. Implementácia eGovernment služieb

Implementácia elektronických služieb vo forme Web Service služieb pre IS SA Agenda občianskych preukazov bude realizovaná na rovnakej platforme ako IS SA Agenda občianskych preukazov.

20. Implementácia formulárov pre Web portál MV SR

Návrh a implementácia formulárov budú v plnej miere rešpektovať požiadavky technologického prostredia MV SR.

21. Školenia

Školenie zamestnancov MV SR pre používanie eGovernment služieb budú zrealizované v nasledujúcom rozsahu

Názov	Počet účastníkov	Dĺžka trvania	Čas vykonania
Školenie Helpdesk (školenie č.2)	5	1 deň	V súlade s Harmonogramom
Školenie administrátorov a operátorov	5	1 deň	V súlade s Harmonogramom

Školenia budú zrealizované za nasledujúcich podmienok:

Miesta školení: školiace pracoviská MV SR vybavené zodpovedajúcou technikou, ktoré budú oznámené predávajúcemu zo strany kupujúceho najneskôr 3 pracovné dni pred začatím príslušného školenia,

Jazyk školenia: slovenský

V rámci školení budú účastníci školenia (bez ohľadu na rolu v systéme), vyškolení na procesné zmeny ohľadne žiadostí a vydávania dokladov a budú im poskytnuté všetky potrebné informácie a predvedené jednotlivé postupy a úkony pre oblasti dotknuté zavedením nového typu dokladu.

Súčasťou školení pre Helpdesk bude aj zaškolenie v problematike riešenia neštandardných situácií.

Súčasťou školení pre administrátorov a operátorov bude aj zaškolenie v problematike prevádzky a údržby systému a zmien fyzického dátového modelu.

V rámci aktivity Školenie objednávateľ okrem toho, že zrealizuje vlastné školenia zamestnancov objednávateľa, vykoná všetky činnosti spojené s prípravou a vyhodnotením školení. Zhotoviteľ pripraví školiace verzie systémov vrátane dát pre školenia, vytvorí užívateľské a administrátorské kontá v systémoch.

Po vlastnej realizácii školení vyhodnotí školiteľ spätnú väzbu účastníkov školenia na funkcionalitu a kvalitu APV.

Školiteľ zabezpečí praktické cvičenia pre zamestnancov objednávateľa na školiacich verziách systémov. Zhotoviteľ poskytne koučing zamestnancom objednávateľa pri osvojení si práce s novým APV.

Zhotovitel dodá zamestnancom objednavateľa, ktorí sa zúčastnia príslušného školenia, pred začatím tohto školenia všetky potrebné materiály pre účastníkov príslušného školenia a to najneskôr v deň začiatku školenia.

22. Dokumentácia

V rámci dodávky bude spracovaná a odovzdaná dokumentácia v nasledovnom rozsahu:

Zhotoviteľ dodá súčasne s dodaním elektronických služieb nasledujúcu dokumentáciu

Technickú dokumentáciu, ktorá bude obsahovať

- technickú (implementačnú) dokumentáciu k elektronickým službám vo formáte HTML (XML schémy, popis používateľského rozhrania, DB tabuľky, DB procedúry),
- dokumentáciu zverejnených rozhraní,
- fyzický dátový model vo formáte XML vrátane väzieb medzi tabuľkami,
- logický dátový model systému,
- zdrojové kódy s popisom.

Prevádzkovú dokumentáciu, ktorá bude obsahovať:

- inštalačný postup aplikácie,
- konfigurácia systémového SW serverov a pracovných staníc,
- chybové stavy a postup ich riešenia,
- popis mechanizmu riadenia prístupu používateľov k dátam a k funkciám aplikácie,
- popis nastavených a požadovaných prístupových práv používateľov a komunikujúcich systémov,
- popis dávkových procedúr, nastavenie a postupnosť ich spúšťania,
- popis procedúr pre zálohovanie a obnovu dát,
- popis použitých a navrhovaných technických číselníkov, ich naplnenie pri inicializácii,
- popis systému žurnálovania a identifikácia činností používateľa,
- popis recovery procedúry vrátane disaster recovery,

Používateľskú dokumentáciu, ktorá bude obsahovať:

- popis systému a jeho funkcií,
- dokumentáciu pre realizáciu školení,
- návrh testovacích procedúr,
- postupy a úkony potrebné pre riadne používanie systému,
- chybové a neštandardné stavy a dostupné spôsoby ich riešenia.
- testovacie scenáre.

Metadáta v softvérovom prostriedku na správu metadát v elektronickej forme na CD.

Ako softvérový prostriedok na správu metadát v elektronickej forme obsahujúci procesný model vo formáte BPM, use case diagramy, class diagramy a sekvenčné diagramy bude použitý Select Component Architect.

23. Podpora rutinnej prevádzky

Po spustení systému do rutinnej prevádzky bude poskytnutá podpora v trvaní 4 týždne v rámci ktorej budú vykonávané najmä nasledovné aktivity:

- podpora dopracovania metodického rámca,
- podpora riešenia konfliktných situácií,
- odstraňovanie zistených nedostatkov elektronických služieb.

24. Rozšírená podpora nábehu rutinnej prevádzky

Pri nábehu eGovernment služieb a po ich zavedení do rutinnej prevádzky bude zhotoviteľ zabezpečovať zvýšenú podporu podľa potrieb objednávateľa. Realizuje sa skúšobný pilot, retestovanie za účasti zhotoviteľa a preklopenie do produkcie. Počas tohto obdobia bude zabezpečená účasť zástupcov zhotoviteľa pre jednotlivé fázy nábehu priamo v priestoroch zákazníka.

V rámci rozšírenej podpory nábehu rutinnej prevádzka budú vykonávané činnosti:

- Príprava predprodukt ívnej prevádzky
- Retestovanie za účasti zhotoviteľa
- Dohľad nad nábehom systému
- Koučovanie zamestnancov objednávateľa
- Zvýšená konzultačná podpora – účasť implementačných tímov zhotoviteľa na mieste

25. Zoznam použitých skratiek

Skratka	Popis
IS SA	Informačný systém správnych agend
IS REGOB	Informačný systém registra obyvateľov
ECU	Evidencia cudzincov
APV	Aplikačné programové vybavenie
eID	Elektronická identifikačná karta
eDoPP	Elektronické povolenie na pobyt
SR	Slovenská republika
JP	Jednotné pracoviská
OP	Občiansky preukaz
REGOB	Register obyvateľov
NPC	Národné personalizačné centrum
OCP	
DoPP	Doklad o povolení na pobyt
CUP	Cudzinecký pas
NPP	Nálepka povolenie na pobyt
MPS	Doklad malého pohraničného styku
CLK	Centrálna lustračná konzola
VIS	Vízový IS
IS ECU	Informačný systém evidencie cudzincov
CVS	Centrálne výpočtové stredisko MV SR
IS MV SR	Informačný systém MV SR
MV SR	Ministerstvo vnútra RS

ČASŤ V TECHNICKÉ RIEŠENIE PRE ZABEZPEČENIE CENTRALIZOVANÉHO RIADENIA PRÍSTUPU K IMPLEMENTOVANÝM EGOVERNMENT SLUŽBÁM

1. Súlad riešenia s relevantnými normami

Navrhované riešenie je v súlade s nasledovnými štandardmi. Tieto štandardy sú používané pre zabezpečenie prístupu k eGovernment službám:

Štandard	Popis
X500	Štandard pre adresárové služby s podporou DAP(Directory Access Protocol), DSP (Directory System Protocol), DISP (Directory Information Shadowing Protocol). Adresár v tomto ponímaní predstavuje hierarchickú štruktúru.
LDAP	Lightweight Directory Access Protocol je aplikačný protokol pre dotazovanie sa voči adresárovým službám a správu dát v týchto adresároch. Adresár predstavuje hierarchickú štruktúru.
X509	X509 je štandard pre infraštruktúru verejných kľúčov pre jednotné prihlasovanie.
SAML	Security Assertion Markup Language (SAML) je štandard na báze XML pre výmenu autorizačných a autentizačných informácii medzi doménami
SOAP	Simple Object Access Protocol je protokol pre výmenu informácii prostredníctvom web služieb
CRL	Certificate revocation list je zoznam zneplatnených sériových čísiel certifikátov, ktorý je poskytovaný v definovanej časovej perióde
OCSP	Online Certificate Status Protocol (OCSP) je protokol zabezpečujúci získanie informácie o platnosti X509 certifikátu

2. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej súťaži v prílohe B1 - Opis predmetu zákazky časť V: „Technické riešenie pre zabezpečenie centralizovaného pristupu k implementovaným eGoverment službám“.

3. Predmet Technického riešenia

Systém centralizovaného riadenia prístupu k eGovernment službám objednávateľa zabezpečí

- vytvorenie centrálnej výkonnej databázy identít
- schopnosť centrálneho riadenia prístupu k web službám na základe definovaných pravidiel
- kontrolu platnosti autentizačných informácii
- zvýšenie bezpečnosti prístupu k eGov službám
- zvýšenie komfortu v súvislosti s využívaním služieb z pohľadu zabezpečenia prevádzky, auditovania a zabezpečenia systému
- zefektívnenie verejnej správy ako celku s prispením optimalizovaných služieb riadenia prístupu a definovaním pravidiel pre prístup k web službám MV
- súlad s legislatívou SR
- podporu interných používateľov pre riadenie prístupových oprávnení
- integrácia web služieb interných systémov do architektúry eGovernment služieb

Pod pojmom „eGovernment služby” pre účel tohto dokumentu rozumieme web služby poskytované vnútri prostredia Objednávateľa (MV) smerom k iným informačným systémom a používateľom pomocou integračnej platformy Objednávateľa. Pre účely tohto dokumentu je pojem „centralizované riadenie prístupu k eGovernment službám“ nahrádzaný zjednodušeným pojmom SOA Security Management.

Navrhnutý systém zabezpečí :

- poskytnutie zoznamu identít s ich autentizačnými informáciami pre eGovernment služby,
- kontrolu platnosti autentizačných informácii,
- zjednodušenie nastavenia bezpečnostných pravidiel pre používanie eGovernment služieb,
- poskytnutie informácii o možných profiloch identity pre ostatné služby eGov,
- odberateľmi služieb môžu byť
    - fyzické osoby,
    - právnické osoby,
    - verejná správa,
    - informačné systémy.

Základný popis funkcií a prínosov navrhovaného riešenia:

- Správa identít a správa databázy identít (autorizovaného zdroja informácií o identitách):
    - Správa dát
    - Import/export dát
    - Synchronizácie dát
    - Poskytnutie prístupu k identitám na základe LDAP protokolu
    - Rozhranie na eID systém
    - Voliteľne, rozhrania na iné systémy objednávateľa
    - Aplikácia pre správu identít, prípadne pre správu vzťahov
- Správa rolí, oprávnení a prístupov
- Správa integrácie s napojenými informačnými systémami na toto riešenie, správa/definícia poskytovaných web services
- Voliteľne, rozhranie pre napojenie sa na ďalšie databázy v štátnej správe (iné autoritatívne zdroje informácií)
- Definícia a realizácia správy riešenia IAM a SOA Security managementu poskytnutím štandardných rozhraní implementovaného riešenia
- Monitoring a audit

Rozsah implementácie jednotlivých bodov definovaných vyššie bude určený počas analytickej časti projektu, na základe požiadaviek objednávateľa a analýzy stavu a potrieb informačných systémov MV SR.

Postup implementácie centralizovaného riadenia prístupu k eGovernment službám z hľadiska funkčných komponentov bude vedený ako samostatné časti projektu s definovanými projektovými výstupmi. Z hľadiska predkladania tejto koncepcie, vidíme postup realizácie v rámci MV SR a potom aj prípadné ďalšie rozšírenia, na tieto sub-projekty:

- Rozsah projektu v rámci MV SR:
    - Implementácia systému pre správu identít a riadenie prístupu pre autoritatívne zdroje MV SR
    - Implementácia riadenia prístupu pre systémy MV SR
    - Poskytnutie služieb identity manažmentu pre eGovernment služby
- Budúce možné rozšírenie:
    - Napojenie na ďalšie informačné zdroje eGov
    - Rozšírenie vzťahov medzi identitami
    - Prechod alebo integrácia v rámci komplexného IAM riešenia pre eGovernment

Podpora interných používateľov pre riadenie prístupových oprávnení zabezpečí:

- Integráciu externých dodávateľov pre proces podpory integrovaných systémov
- Vybudovanie znalostnej databázy
- Vybudovanie systému pre podporu interných používateľov naprieč organizáciou
- Konfigurácia tlačových zostáv

- Konfigurácia riadenia oprávnení pre LDAP a databázové systémy

Integrácia web služieb interných systémov do architektúry eGovernment službami zabezpečí:

- Integráciu maximálne piatich interných web služieb na SOA zbernicu
- Konfigurácia integrácie web služieb a vykonanie testovania

4. Procesný model

Kapitola definuje odpovede na jednotlivé požiadavky objednávateľa a spôsob ich splnenia a ďalej špecifikuje kľúčové procesy, ktore budu detailne analyzované počas dodávky riešenia systému riadenia prístupov.

4.1. Špecifikácia kľúčových požiadaviek na riešenie

Centrálne riadenie prístupu k web službám MV SR musí spĺňať nasledovné požiadavky objednávateľa. Za každou požiadavkou je definovaný stav (Áno, Nie, Čiastočne) splnenia požiadavky.

Požiadavka / Vyjadrenie
Riadenie prístupu k web službám na základe autentizačných informácii a informácii evidovaných v systéme (napr: skupina, organizačná zložka, profil, pravidlo, čas, lokalita)
Splnenie: Áno Systém obsahuje modul Identity management pre riadenie prístupu k web službám na základe definovaných pravidiel. Pri definovaní pravidiel je možné definovať pravidlá na základe poskytnutých atribútov o identite, času, skupine a pod. Súčasťou riešenia je aj integrácia iných interných zdrojov informácii o identitách pre možnosť detailnejšej špecifikácie pravidiel na základe napr. profilu osoby.
Integrácia s RFO (register fyzických osôb) ako autoritatívnym zdrojom informácii o fyzických osobách
Splnenie: Áno Súčasťou systému je integrácia na autoritatívny zdroj informácii o fyzických osobách t.j. systém RFO. Systém čerpá informácie z autoritatívneho zdroja a synchronizuje ich s internými informáciami v X500 databáze pre zabezpečenie rýchleho prístupu k informáciám o identite a jej autentizačných údajoch.
Vytvorenie výkonného repozitára s informáciami o identitách (osoba, systém a pod.), ich profiloch, skupinách, organizačných zložkách
Splnenie: Áno Súčasťou systému je výkonná X500 databáza s informáciami o identitách získaných z autoritatívneho zdroja informácii s doplneným o informácie z iných interných systémov objednávateľa.
Prístup k informáciám z cieľových systémov a ich mapovanie na používateľské profily (lekár, pracovník matriky, policajt ...).
Splnenie: Áno Systém obsahuje integračné rozhranie pre získavanie informácii o pôsobnosti resp. profile identity napr. lekár a pod. Tieto informácie sprístupňuje aj iným systémom.
Integrácia s certifikačnou autoritou spravujúcou autentizačné certifikáty pre získavanie zoznamu zneplatnených certifikátov
Splnenie: Áno Navrhované riešenie zabezpečuje integráciu (napojenie) s jednou alebo viacerými certifikačnými autoritami pre získanie zoznamu zneplatnených certifikátov a verejných kľúčov
Integrácia s databázou verejných kľúčov vydaných autentizačných certifikátov
Splnenie: Áno Systém obsahuje štandardnú X500 databázu s možnosťou ukladania verejných kľúčov

Požiadavka / Vyjadrenie
Umožnenie integrácie na iné identity management systémy synchronizáciou informácii a priamym riadením rolí používateľov
Splnenie: Áno Riešenie umožňuje riadenie oprávnení na základe rolí pre interné systémy objednávateľa z prostredia identity management systému. Súčasne sprostredkováva rozhranie na báze web služieb pre riadenie prístupov aj pre nadradené systémy.
Systém musí byť licenčne a technicky dimenzovaný na minimálne 2 milióny identít
Splnenie: Áno Systém je licenčne dimenzovaný na 2 milióny identít s možnosťou uchovania informácii o desiatkach miliónov identít.
Poskytnutie informácii o možných profiloch identity pre ostatné služby eGov a portál
Splnenie: Áno Riešenie poskytuje informácie pre iné systémy na základe LDAP protokolu alebo web služieb. Systém umožňuje vytvorenie inštancií pre prípad uchovania informácie o identite a jej roliach pre iné interné systémy objednávateľa.
Centrálna DB identít musí byť riešená prostredníctvom štandardnej adresárovej služby s podporou implementácie minimálne pre MV SR prevádzkované platformy (Windows, Linux, HPUX, AIX)
Splnenie: Áno Systém obsahuje štandardnú X500 DB s LDAP prístupom CA Directory s možnosťou implementácie na systémy Windows, Solaris, Linux, HPUX a AIX.
Poskytnutie prístupu k centrálnej databáze identít prostredníctvom štandardného protokolu LDAP s výkonom minimálne 20000 základných operácii za sekundu
Splnenie: Áno Riešenie obsahuje X500 DB s tzv. dxGrid pamäťovým prístupom k informáciám, ktoré poskytuje aj na štandardnom hw vybavení výkon vyšší ako 20000 operácii za sekundu.
Riadenie prístupu k web službám musí byť založené na štandardnom celosvetovo rozšírenom produkte s podporou minimálne nasledovných autentifikačných protokolov (WS-Security (SAML), WS-Security (X509), WS-Security (prihlasovacie meno), SAML, XML dokument) s podporou štandardov pre oblasť adresárových služieb minimálne nasledovných MV SR prevádzkovaných adresárových služieb (IBM Directory, CA Directory) a podporou minimálne nasledovných MV SR prevádzkovaných relačných databáz (MS SQL Server, Oracle, IBM DB2)
Splnenie: Áno Riadenie prístupu je riešené prostredníctvom CA Vordel SOA Gatreway a CA SOA Security Manager (Siteminder). Obidva produkty poskytujú v súčasnosti špičkové parametre a funkcionalitu pre riadenie prístupu k web zdrojom s podporou autentifikačných protokolov (WS-Security (SAML), WS-Security (X509), WS-Security (prihlasovacie meno), SAML, XML dokument). Ako adresárové služby sú podporované Oracle Internet Directory, Sun, Novell, IBM Direcotry, CA Directory a z hľadiska databáz databázy MS SQL Server, Oracle, DB2 a iné.
Súčasťou navrhovaného centralizovaného riadenia prístupu k web službám musia byť • údaje potrebné pre evidenciu a identifikáciu identít, • pravidlá prístupu k web službám systému, • vysoko dostupný a výkonný X500 adresár identít, • systém on-line vyhodnocovania pravidiel a riadenia prístupu k web službám, • konektory do cieľových systémov (max 3 systémy špecifikované objednávateľom počas v analytickej fáze projektu) a normalizácia informácii z týchto systémov do typu profilu identity, • dostupnosť zoznamu identít pre ostatné systémy na báze LDAP protokolu.

Požiadavka / Vyjadrenie
Splnenie: Áno Definované služby poskytujú moduly Identity Manager a SOA Gateway. Riešenie súčasne integruje informácie z iných systémov (v maximálnom rozsahu 3 interné systémy) pre poskytnutie kvalitnejších informácii o identite prostredníctvom LDAP protokolu.
Riešenie musí byť postavené na štandardných produktoch a protokoloch a musí byť rozšírené o nasledujúce eGovernment služby súvisiace s centrálnym riadením prístupu k web službám: • Poskytnutie informácii o identitách a ich atribútoch (vo forme web služby aj vo forme prístupu cez LDAP protokol) • Poskytnutie informácii o možných profiloch identity • Poskytnutie informácii o platnosti autentizačných informácii • Poskytnutie informácii o pravidlách zabezpečenia
Splnenie: Áno Riešenie je postavené na štandardných produktoch Oracle DB, CA Vordel SOA Gateway, CA Directory a CA SOA Security Manager a poskytuje informácie • o identitách a ich atribútoch (vo forme web služby aj vo forme prístupu cez LDAP protokol) • o profiloch identity • o platnosti autentizačných informácii • o pravidlách zabezpečenia

4.2. Špecifikácia kľúčových procesov

V tabuľkovej podobe sú definované kľúčové procesy nabvrhovaného systému riadenia prístupov. Pre každý proces je definovaný jeho vznik, vstupy, výstupy a vykonávané činnosti.

Proces	Synchronizácia identity
Vznik	Plánovaná úloha Požiadavka na synchronizáciu identity
Zúčastnené role	Systém Identity Management, systém RFO
Vstup	Informácie z autoritatívneho zdroja RFO
Činnosť	Pridanie - deaktivácia identity Aktualizácia atribútov Uloženie do X500 DB
Výstup	Informácie o identite v X500 DB
Proces	**Zistenie informácie o identite**
Vznik	Požiadavka o informácie o identite
Zúčastnené role	Zákaznícky systém, Systém Identity Management
Vstup	Identifikátor identity resp. ldap filter, zoznam atribútov
Činnosť	Vyhľadanie identít Poskytnutie informácii
Výstup	Požadované informácie
Proces	**Synchronizácia profilu identity**
Vznik	Plánovaná úloha
Zúčastnené role	Systém Identity Management, zákaznícke systémy
Vstup	Informácie o identite a jej atribútoch v zákazníckych systémoch
Činnosť	Získanie zoznamu identít v zákazníckych systémoch Porovnanie informácii medzi Identity Management systémom a zákazníckym systémom Mapovanie informácii na profil Uloženie do X500 DB
Výstup	Informácie o profile identity v X500 DB
Proces	**Poskytnutie profilu identity**
Vznik	Požiadavka o profil identity
Zúčastnené role	Systém Identity Management, zákaznícky systém
Vstup	Identifikátor identity
Činnosť	Vyhľadanie profilov pre danú identitu
Výstup	Poskytnutie zoznamu profilov pre identitu

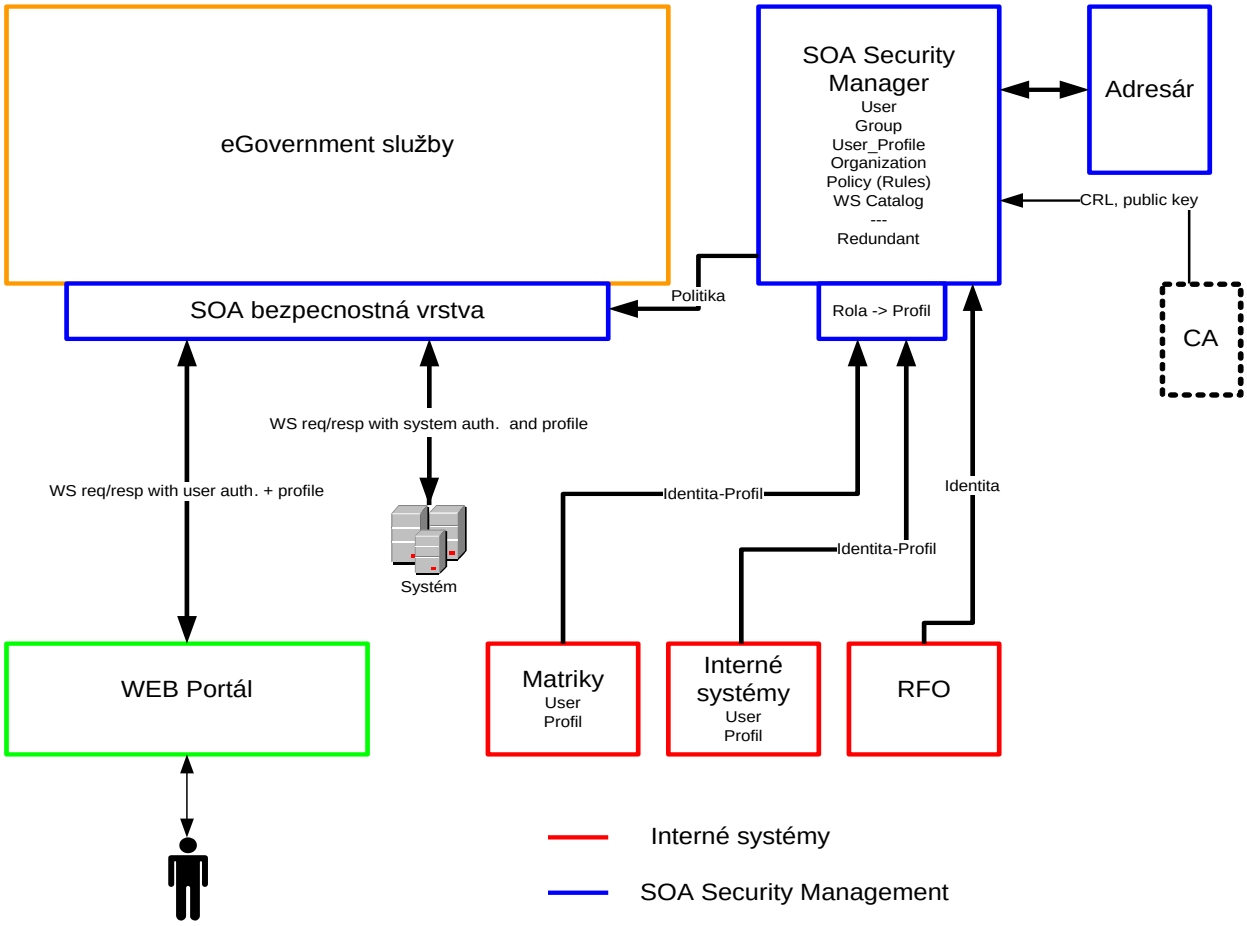
Proces	Definovanie pravidla pre prístup k web službám
Vznik	Zmena logiky riadenia prístupu, vznik - zánik služby, zmena informácii o identite
Zúčastnené role	Správca systému riadenia prístupov
Vstup	Popis pravidla (podmienok prístupu k web službám)
Činnosť	Vytvorenie pravidla Aplikácia pravidla
Výstup	Zaregistrovaná zmena pravidiel v systéme Identity Management
Proces	Registrácia systému do LDAP databázy
Vznik	Pridanie – odobratie interného systému objednávateľa
Zúčastnené role	Správca systému riadenia prístupov
Vstup	Identifikátor systému, Spravované atribúty a role
Činnosť	Pridanie-deaktivácia schémy Definovanie prístupu Prvotné naplnenie údajov
Výstup	Informácie o systéme a identitách v X500 DB
Proces	Kontrola prístupu k web službe
Vznik	Požiadavka o eGov službu
Zúčastnené role	Systém Identity Management
Vstup	Služba, autentizačné informácie identity
Činnosť	Získanie informácii Vyhodnotenie pravidiel
Výstup	Povolenie – zákaz prístupu k web službe
Proces	Validácia XML a kontrola obsahu žiadostí
Vznik	Požiadavka o eGov službu
Zúčastnené role	Systém SOA Gateway
Vstup	Služba, autentizačné informácie identity
Činnosť	Validácia XML vstupu Kontrola obsahu
Výstup	Spracovanie – odmietnutie žiadosti
Proces	Registrácia služby
Vznik	Pridanie – odobratie eGov služby
Zúčastnené role	Správca systému riadenia prístupov
Vstup	WSDL popis služby
Činnosť	Zaradenie – vyradenie služby Uloženie do katalógu služieb s riadením prístupom
Výstup	Informácie o službe v Identity management systéme
Proces	Registrácia certifikačnej autority
Vznik	Pridanie – odobratie certifikačnej autority
Zúčastnené role	Správca systému riadenia prístupov
Vstup	Informácie o certifikačnej autorite, spôsobe spracovania zneplatnených certifikátov
Činnosť	Pridanie-deaktivácia certifikačnej autority Uloženie do katalógu certifikačných autorít
Výstup	Informácie o certifikačnej autorite v Identity management systéme
Proces	Synchronizácia platnosti certifikátov
Vznik	Plánovaná úloha
Zúčastnené role	Systém Identity Management
Vstup	Katalóg certifikačných autorít
Činnosť	Získanie aktuálneho zoznamu Spracovanie a zápis do Identity Management systému
Výstup	Informácie o identite v X500 DB

4.3. Funkčný návrh systému

Navrhované riešenie zabezpečí implementáciu prístupu k eGovernment službám s nasledovnými vlastnosťami

- vynucovanie pravidiel prístupu k eGovernment službám objednávateľa na základe autentizačných informácii a informácii o identite,
- kontrolu autentizačných informácii,
- validáciu XML a XML firewalling,
- ochranu proti škodlivému kódu,
- auditovanie prístupu k web službám.

Nasledujúca bloková schéma definuje jednotlivé komponenty navrhovaného riešenia.



Modrou farbou sú definované implementované komponenty.

- eGovernment Služby – množina chránených web služieb. Riešenie zabezpečuje implementáciu vrstvy pred prístupom na integračnú zbernicu. Každé volanie služieb smerom na integračnú zbernicu bude kontrolované prostredníctvom SOA bezpečnostnej vrstvy.
- SOA Bezpečnostná vrstva – vrstva zabezpečujúca vynucovanie pravidiel prístupu, chrániaca prístup k poskytovaným službám a oddeľujúca služby od okolitého prostredia
- SOA Security Manager – systém pre správu prístupov, definíciu pravidiel a rolí
- Adresár – výkonná X500 databáza pre riadenie prístupov
- Rola -> Profil - mechanizmus pre prevod informácii z cieľových systémov na používateľské profily
- CA – certifikačná autorita
- Systém – interný systém objednávateľa pristupujúci k web službám pomocou systémového účtu
- Web Portál – grafické rozhranie pre koncových používateľov s možnosťou výberu profilu používateľa
- Interný systém – interný systém objednávateľa udržujúci informácie o používateľoch ovplyvňujúcim zoznam profilov používateľa
- RFO – register fyzických osôb

4.4. Atribúty kvality navrhovaného riešenia

4.4.1 Auditovanie

Systémy auditujú zmeny svojich objektov buď vo forme auditných žurnálov, zápisom na úrovni záznamu alebo udržiavajú históriu zmien daného atribútu. Systémy auditujú aj prístup k chráneným eGov službám. Auditové záznamy sú udržiavané na úrovni relačnej databázy.

4.4.2 Riadenie prístupov

Riadenie prístupov je riešené na základe Role Based Access Control modelu alebo na základe pravidiel. Riadenie prístupov zabezpečuje prístup k jednotlivým funkciám alebo konkrétnym objektom na základe definovaných pravidiel.

4.4.3 Overovanie

Systémy umožňujú overovanie na základe vlastných informácii alebo v niektorých prípadoch prostredníctvom externého overovacieho mechanizmu napr. LDAP, ActiveDirectory.

4.4.4 Výkonové parametre

Z hľadiska ovplyvnenia výkonových parametrov exitujúcich systémov nespôsobujú implementované systémy s výnimkou SOA Agenta na middleware vrstve výkonové obmedzenie. Aj na tejto vrstve, ale vyťaženie nepredstavuje výraznú zmenu oproti systému bez SOA Agenta. Na úrovni sieťovej komunikácie je spomalená komunikácia na úrovni SOAP protokolu prechádzajúceho cez SOA Gateway a SOA Agenta. SOA Gateway je dimenzovaná tak aby vyhovela predpokladanému zaťaženiu middleware vrstvy.

4.4.5 Dostupnosť

Systém tvorí kritický komponent pri prístupe k eGov službám. Z toho dôvodu je jeho vysoká dostupnosť nevyhnutná. Systém je navrhnutý na prevádzku 24x7. Všetky komponenty sú riešené redundantne s doplnením o replikáciu na úrovni relačnej a X500 databázy.

Predpokladaný spôsob zálohovania je riešený on-line zálohovaním databázy Oracle a X500 DB, zálohovaním konfiguračných súborov aplikácii štandardným zálohovacím mechanizmom objednávateľa.

5. Návrh (dizajn) APV

Navrhované aplikačné programové vybavenie je postavené na štandardných riešeniach. Kľúčový komponent Identity Management je postavený na trojvrstvovej architektúre s prístupom prostredníctvom web rozhrania, web služieb resp. prostredníctvom štandardného LDAP protokolu. Systém umožňuje konfiguráciu GUI pre jednotlivé role a prístup k úlohám prostredníctvom web služieb. Dodávané riešenia poskytujú štandardné zdokumentované API pre integráciu s inými systémami.

5.1. Navrhované web služby

Návrhované riešenie umožňuje získanie informácii prostredníctvom LDAP protokolu v prípade požiadavky na vysoký výkon resp. aj prostredníctvom web služieb. Systém poskytuje nasledovné web služby:

Web služba	Vstupy - Výstupy
Vytvorenie identity	Vstup: Identifikátor identity, zoznam hodnôt atribútov Výstup: Stav operácie
Zmena identity	Vstup: Identifikátor identity, zoznam hodnôt menených atribútov Výstup: Stav operácie

Deaktivácia identity	Vstup: Identifikátor identity Výstup: Stav operácie
Získanie informácii o identite	Vstup: Filtračná podmienka, zoznam atribútov Výstup: Zoznam atribútov identít
Poskytnutie profilov k identite	Vstup: Identifikátor identity Výstup: Zoznam profilov

6. Implementácia APV

Pri návrhu technickej architektúry a podporenej IT infraštruktúry je kladený dôraz najmä na zabezpečenie vysokej dostupnosti a minimalizáciu času odozvy pri kontrole prístupu k web službám.

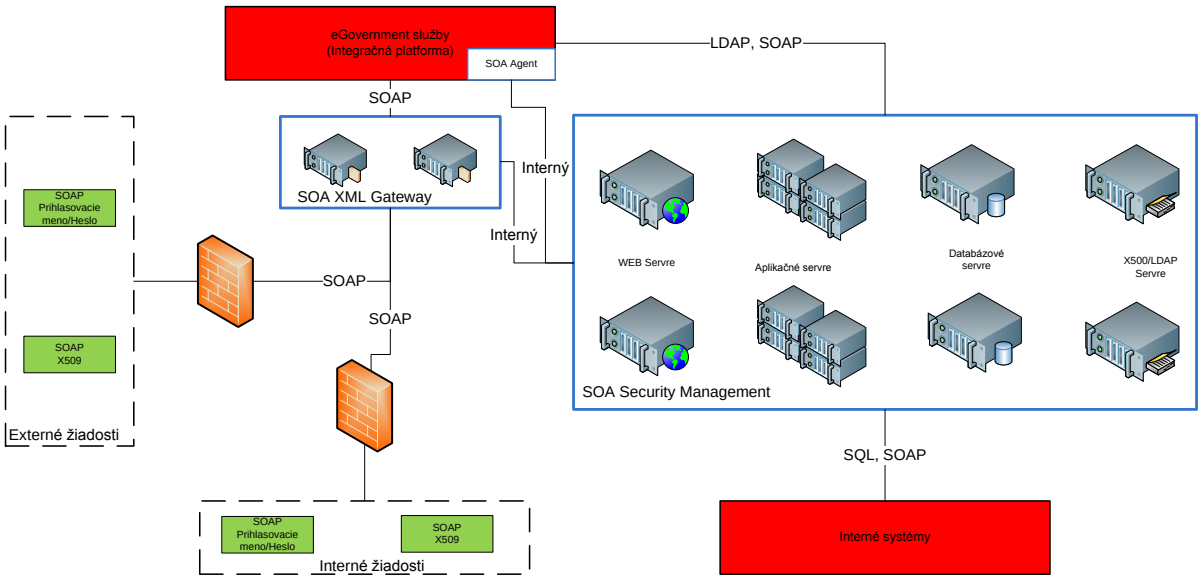
Navrhovaný systém musí byť škalovatelný, podporovat rýchlu odozvu pri veľkej záťaži a konkurenčnom prístupe k informáciám. Súčasne je systém navrhnutý ako škálovateľný v každej svojej úrovni t.j aj na úrovni adresára, na úrovni SOA Security Manager aplikačného servera aj na úrovni SOA bezpečnostnej vrstvy.

Požiadavka na vysokú dostupnosť je riešená redundanciou komponentov s využitím softvérovej replikácie na úrovni relačnej databázy a X500 adresára. Toto riešenie je cenovo efektívne a dovoľuje aj geografické oddelenie systémov. Z dôvodu priestorovej minimalizácie a pre minimalizáciu infraštruktúrnych prvkov sme využili Blade serverové riešenie na platforme HP. HP platforma bola zvolená v dôsledku vysokej spoľahlivosti, technickej podpory a celosvetového rozšírenia.

Z pohľadu softvérového vybavenia je systém postavený na celosvetovo rozšírených a overených riešeniach. V návrhu riešenia je použitý vysoko výkonná X500 adresár spracovávajúci informácie pomocou pamäťovo mapovaného modelu s real-time replikáciami, na trhu najrozšírenejší nástroj na riadenie pravidiel prístupu k web zdrojom a Oracle relačná databáza poskytujúca najmä auditové služby.

Na nasledujúcom obrázku sú znázornené technické komponenty navrhovaného riešenia. Modrou farbou sú zakreslené implementované systémy v rámci tohto projektu. Červenou farbou sú existujúce resp. budované systémy u objednávateľa. Prepojenia medzi komponentmi identifikujú použitý protokol. Z hľadiska prístupu je prístup rozdelený na prístup z externého prostredia a prístup z interného prostredia. Prístup z oboch prostredí je možný na základe autentizácie pomocou mena a hesla resp. X509 certifikátom.

Testovanie APV a jeho jednotlivých súčasti bude vykonané na základe návrhu testovacích procedúr a scenárov, ktoré budú špecifikovať unit a integračné testy. Výsledkom tejto aktivity bude otestované APV nasaditeľné ro rutinnej prevádzky.



Technická architektúra navrhovaného riešenia

Navrhovaný systém sa skladá z dvoch vzájomne prepojených blokov:

- SOA XML Gateway poskytuje funkcie kontroly autentizačných informácii, overenia identity, kontroly XML, kontroly pravidiel prístupu k službám, kontroly na škodlivý kód v prílohách.
- SOA Security Management zabezpečuje správu pravidiel prístupu k web službám, poskytuje služby úložiska identít a verejných kľúčov, LDAP adresárové služby pre implementované systémy a integráciu informácii z interných systémov.

Tabuľka definuje mapovanie blokov funkčnej architektúry na komponenty technického riešenia:

Funkčný blok	Technický komponent
SOA Bezpečnostná vrstva	SOA XML Gateway SOA Agent
SOA Security Manager	SOA Security Manager (WEB Servers, Application Servers, Database Servers)
Adresár	X500 LDAP Servers

Tabuľka definuje mapovanie operačných systémov, databáz a aplikácii na komponenty technického riešenia:

Server	Softvérové komponenty
X500 LDAP servre	Red Hat Enterprise Linux 5 CA Directory 12
Databázové servre	Red Hat Enterprise Linux 5 Oracle Standard Edition One DB 11g
Aplikačné servre	Red Hat Enterprise Linux 5 CA SOA Security Manager 12.1
WEB servre	MS Windows 2008 R2 x64 STD CA SOA Security Manager 12.1
SOA Gateway	Red Hat Enterprise Linux 5 CA Vordel XML SOA Gateway 12.1
SOA Agent	CA SOA Agent 12.1

Pri implementácii APV navrhujeme z hľadiska X500 databázy použitie štandardnej X500 LDAP schémy pre udržiavanie informácii o identitách. Takáto konfigurácia zabezpečí kompatibilitu s externými aplikáciami a možnosť nezávislého vývoja aplikácii bez nutnosti dostupnosti konkrétneho LDAP servera vo fáze vývoja resp. testovania aplikácii.

7. Externé rozhrania

Popis rozhraní definuje typ protokolu pri výmene informácii a typy informácii používaných pri vzájomnej komunikácii medzi komponentom navrhovaného riešenia a jeho okolím.

Rozhranie	Protokol
Adresár	LDAP, SOAP Prístup k identitám udržiavaným v X500 schéme je možný na základe LDAP protokolu. Súčasne obsahuje systém aj web službu pre možnosť získania informácie o identite pomocou SOAP protokolu. Preferovaným protokolom pri potrebe vysokého výkonu je LDAP protokol.
Interné systémy objednávateľa	SQL, LDAP, SOAP Pri komunikácii s internými systémami objednávateľa pre synchronzáciu profilov predpokladáme primárne využitie SQL, SOAP resp. LDAP protokolov. Systém je z tohoto pohľadu otvorený a dokáže v prípade potreby využiť aj iný typ protokolu.
SOA Gateway	Interný protokol aplikácie, SQL, LDAP Pre komunikáciu medzi SOA Security Manager a Gateway je použitý interný protokol, pri komunikácii medzi Gateway a X500 DB je použitý LDAP protokol, pri komunikácii medzi Gateway a Oracle DB je použitý SQL protokol.
SOA Agent	Interný protokol aplikácie Pre komunikáciu medzi SOA Agent a SOA Security manager je použitý interný protokol aplikácie.

8. Dokumenty a dokumentácia

Zhotoviteľ dodá súčasne s nasledujúcu dokumentáciu.

Technická dokumentácia, ktorá bude obsahovať:

- rozsah riešenia
- koncepčný návrh riešenia
- používateľské role
- poskytované služby nástroja
- funkčná špecifikácia implementovaného riešenia
- technická architektúra
- popis procesov
- licenčné podmienky a technická podpora

Prevádzkovú dokumentáciu, ktorá bude obsahovať:

- inštalačný postup aplikácie,
- konfigurácia systémového SW serverov a pracovných staníc,
- chybové stavy a postup ich riešenia,
- popis dávkových procedúr, nastavenie a postupnosť ich spúšťania,
- popis procedúr pre zálohovanie a obnovu dát,
- popis recovery procedúry vrátane disaster recovery,

- popis integračných rozhraní

Používateľskú dokumentáciu, ktorá bude obsahovať:

- dokumentáciu pre realizáciu školení,
- administratirsku priručku,

Vyššie uvedená dokumentácia bude dodaná v písomnej forme v počte 1 kus a v elektronickej forme na CD.

9. Podpora rutinnej prevádzky

Po nábehu systému do prevádzky bude zhotoviteľ zabezpečovať podporu systému v priebehu dvoch týždňov od nábehu systému do prevádzky. Počas tohto obdobia má objednávateľ právo požadovať prítomnosť jednej osoby objednávateľa priamo v priestoroch objednávateľa.

V rámci zvýšenej podpory budú vykonávané činnosti

- Dohľad nad chodom systému (výkonové štatistiky, analýza žurnálov)
- Konzultačná podpora
- Evidencia a riešenie incidentov
- Návrh rekonfigurácie systému

10. Rozšírená podpora nábehu rutinnej prevádzky

Pri nábehu systému AIM a po jeho zavedení do rutinnej prevádzky bude zhotoviteľ zabezpečovať zvýšenú podporu podľa potrieb objednávateľa. Realizuje sa skúšobný pilot, retestovanie za účasti zhotoviteľa a preklopenie do produkcie. Počas tohto obdobia bude zabezpečená účasť zástupcov zhotoviteľa pre jednotlivé fázy nábehu priamo v priestoroch zákazníka.

V rámci rozšírenej podpory nábehu rutinnej prevádzka budú vykonávané činnosti:

- Príprava predproduktívnej prevádzky
- Retestovanie za účasti zhotoviteľa
- Koučovanie zamestnancov objednávateľa
- Dohľad nad nábehom systému
- Zvýšená konzultačná podpora – účasť implementačných tímov zhotoviteľa na mieste

11. Rozšírenie technického riešenia pre zabezpečenie centralizovaného riadenia prístupu k implementovaným eGovernment službám

Ciele

- podporu interných používateľov pre riadenie prístupových oprávnení s podporou interných používateľov pre integráciu externých dodávateľov a riešenie znalostnej databázy
- integrácia web služieb interných systémov mimo rozsahu eGovernment služieb

Rozsah

- Podpora interných používateľov pre riadenie prístupových oprávnení zabezpečí
- Integráciu externých dodávateľov pre proces podpory integrovaných systémov
- Vybudovanie znalostnej databázy
- Vybudovanie systému pre podporu interných používateľov naprieč organizáciou
- Konfigurácia tlačových zostáv
- Konfigurácia riadenia oprávnení pre LDAP a databázové systémy

Integrácia web služieb interných systémov mimo rozsahu eGovernment služieb zabezpečí

- Integráciu maximálne piatich interných web služieb, ktoré sú nad rámec integrácie eGovernment služieb
- Konfigurácia integrácie a vykonanie testovania

11.1. Špecifikácia kľúčových procesov

Proces	Zaevidovanie požiadavky
Vznik	Požiadavka o službu
Zúčastnené role	Operátor, Používateľ, Riešiteľ
Vstup	Požiadavka používateľa
Činnosť	Evidencia požiadavky Spracovanie a zápis do systému Lokalizácia riešiteľa Notifikácia na riešiteľa
Výstup	Uložená požiadavka
Proces	Vyriešenie požiadavky
Vznik	Požiadavka o službu
Zúčastnené role	Používateľ, Riešiteľ
Vstup	Požiadavka v systéme
Činnosť	Analýza požiadavky Vyhľadanie v znalostnej databáze Realizácia riešenia Uzavretie požiadavky a notifikácia na používateľa
Výstup	Uzavretá požiadavka
Proces	Spracovanie požiadavky na externého dodávateľa
Vznik	Požiadavka o riešenie externým dodávateľom
Zúčastnené role	Riešiteľ, Externý riešiteľ
Vstup	Požiadavka, systém, popis požiadavky
Činnosť	Presun na externú organizáciu Spracovanie externým dodávateľom Realizácia riešenia Uzavretie požiadavky a notifikácia na riešiteľa
Výstup	Uzavretá požiadavka
Proces	Zaevidovanie znalostného dokumentu
Vznik	Požiadavka o zaevidovanie nového typu riešenia
Zúčastnené role	Riešiteľ
Vstup	Popis riešenia
Činnosť	Spracovanie dokumentu Vloženie do znalostnej databázy Definovanie oprávnení, kategórie Publikovanie dokumentu
Výstup	Publikovaná znalosť
Proces	Registrácia LDAP alebo DB systému pre riadenie oprávnení
Vznik	Požiadavka o registráciu
Zúčastnené role	Administrátor
Vstup	Požiadavka na registráciu, prístupové oprávnenia, role
Činnosť	Registrácia systému Synchronizácia údajov Definovanie politík Publikovanie systému do riadenia oprávnení
Výstup	Registrovaný systém

11.2. Školenia

Implementovaný systém je navrhovaný ako automatizovaný systém riadenia prístupu k web službám a nepredpokladá vyškolenie koncových používateľov vzhľadom k tomu, že táto rola sa nezapája priamo do systému. Školenia sú z toho dôvodu riešené ako školenia pre správcov systému.

Miesta školení:

- školiace pracoviská objednávateľa, ktoré budú oznámené predávajúcemu zo strany objednávateľa najneskôr 3 pracovné dni pred začatím príslušného školenia,

Jazyk školenia:

- slovenský

Školenia:

Názov	Počet účastníkov	Dĺžka trvania	Čas vykonania
Školenie administrátorov X500 DB, SOA Security Manager, SOA XML Gateway	3	3 dni	V súlade s Harmonogramom

Zhotoviteľ zabezpečí praktické cvičenia pre správcov systému objednávateľa a poskytne koučing zamestnancom objednávateľa pri osvojení si práce s novým systémom.

12. Zoznam použitých skratiek

Skratka	Vysvetlenie
CRL	Certificate revocation list
LDAP	Lightweight Directory Access Protocol
RBAC	Role Based Access Control
RSBAC	RuleSet Based Access Control
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
WS	Web Services
X500	Štandard pre adresárové služby

ČASŤ VI .ROZŠÍRENIE TECHNICKÉHO RIEŠENIA PRE JEDNOTNÉ PRACOVISKÁ MV O MOBILNÉ PRACOVISKÁ NA ZBER ŽIADOSTÍ PRE VYDÁVANE ELEKTRONICKÝCH EID KARIET, RESP. EDOPP

1. Súlad riešenia s relevantnými normami

Normy pre kontaktné čipové karty

- ISO/IEC 7816-1-Integrated Circuit(s) Cards with Contacts - Part 1: Physical Characteristics
- ISO/IEC 7816-2-Integrated Circuit(s) Cards with Contacts - Part 2: Dimensions and Location of the Contacts
- ISO/IEC 7816-3-Integrated Circuit(s) Cards with Contacts - Part 3: Electronic Signals and Transmission Protocols
- ISO/IEC 7816-4-Integrated Circuit(s) Cards with Contacts - Part 4: Interindustry Commands for Interchange
- ISO/IEC 7816-4-/Amd1-Integrated Circuit(s) Cards with Contacts - Part 4: Interindustry Commands for Interchange AMENDMENT 1: Impact of Secure Messaging on the Structures of APDU Messages
- ISO/IEC 7816-5-Integrated Circuit(s) Cards with Contacts - Part 5: Numbering System and Registration Procedure for Application Identifiers
- ISO/IEC 7816-6-Integrated Circuit(s) Cards with Contacts - Part 6: Interindustry Data Elements
- ISO/IEC 7816-8-Integrated Circuit(s) Cards with Contacts - Part 8: Security Related Interindustry Commands
- ISO/IEC 7816-9-Integrated Circuit(s) Cards with Contacts - Part 9: Additional Interindustry Commands and Security Attributes
- ISO/IEC 7816-10-Integrated Circuit(s) Cards with Contacts - Part 10: Electronic Signals and Answer to Reset for Synchronous Cards
- Certifikácia pre kryptografický modul kontaktnej čipovej karty minimálne podľa štandardu FIPS -140 level 2 alebo Common Criteria EAL 4+ (ISO-IEC-15408)
- Certifikácia v zmysle §10, ods. 2 písm j) zákona NR SR č. 215/2002 o elektronickom podpise

Biometria

- ISO/IEC 19794-5:2005, Biometric Data Interchange Formats – Part 5: Face Image Data
- ISO/IEC 19794-4:2005, Biometric Data Interchange Formats – Part 5: Finger Image Data
- ANSI/NIST-ITL 2-2008, XML Version of ANSI/NIST-ITL 1-2007, American National Standard for Information Systems—Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information – Part 2: XML Version

2. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej súťaži v prílohe B1 - Opis predmetu zákazky časť VI: „Rozšírenie technického riešenie pre Jednotné pracoviska o mobilné pracoviska na zber žiadosti pre vydávanie elektronických eID kariet.“.

3. Predmet Technického riešenia

Predmetom ponuky je rozšírenie technického riešenia informačného systému Integrovaného riešenia jednotných pracovísk pre zber žiadostí od občanov, zber údajov, kontrolu údajov, kontrolu dokladov a vydávanie vodičských preukazov, cestovných pasov a občianskych preukazov, o mobilné pracoviská na zber žiadostí pre vydávane elektronických eID kariet.

Cieľom požadovaných úprav a rozšírení technického riešenia Jednotných pracovísk je dodať v požadovanom počte technické vybavenie umožňujúce off-line spôsobom, t.j. bez pripojenia na centrálny systém, získať biometrické údaje potrebné pre personalizáciu vybraných dokladov.

V súčasnosti disponibilné mobilné pracoviská na zber žiadostí pre vydávanie dokladov umožňujú prácu len v on-line režime, t.j. iba tam, kde je možné ich pripojiť do mv-netu prostredníctvom prostriedkami MV SR zabezpečenej mobilnej dátovej komunikácie a VPN klienta.

Požadované riešenie musí umožňovať bezproblémové prijímanie žiadostí na akomkoľvek mieste na území SR podľa potrieb žiadateľa, ktorý sa pre bezvládnosť nemôže osobne dostaviť na pracovisko ODE PPZ a podať úplnú žiadosť o vydanie dokladu.

Riešenie bude pokrývať potreby žiadateľa v súvislosti s vydávaním CP, VP a eID kariet.

4. Popis navrhovaného riešenia

Požadované riešenie bude umožňovať bezproblémové prijímanie žiadostí na akomkoľvek mieste na území SR podľa potrieb žiadateľa, ktorý sa pre bezvládnosť nemôže osobne dostaviť na pracovisko ODE PPZ a podať úplnú žiadosť o vydanie dokladu.

Riešenie bude komplexne pokrývať potreby žiadateľa v súvislosti s vydávaním CP, VP a eID kariet.

Služby súvisiace s vydávaním, rušením a overovaním platnosti certifikátov nebudú na mobilnom pracovisku poskytované.

Súčasťou rozšírenia technického riešenia bude dodávka softvéru, hardvéru a systémového softvéru, menovite:

- softvérové vybavenie pre zaevidovanie žiadosti o doklad pre mobilné pracovisko v centrálnom systéme a následné vytvorením off-line verzie žiadosti pre prácu v teréne,
- softvérové vybavenie pre import a export off-line žiadostí na mobilné pracovisko,
- softvérové vybavenie pre spracovanie off-line verzie žiadosti a biometrických údajov v centrálnom systéme,
- hardvérové vybavenie mobilných pracovísk pre off-line zber biometrických údajov (kufríky) spolu so súvisiacim systémovým softvérom v počte 80 kusov,
- softvérové vybavenie pre získanie biometrických údajov mobilným pracoviskom a ich pripojenie k off-line žiadosti – 80 licencií,
- softvérové vybavenie pre spracovanie off-line žiadosti mobilným pracoviskom vrátane možnosti vytvorenia off-line žiadosti na mobilnom pracovisku – 80 licencií.

5. Procesný model

5.1. Popis procesu zberu žiadosti na mobilnom pracovisku

Procesný model sa zameria predovšetkým na mapovanie kľúčových procesov.

Procesné mapy budú dokumentované vo forme schém realizovaných vo vhodnom CASE nástroji.

5.1.1 Vytvorenie off-line žiadosti o vydanie dokladu

- Na základe písomnej alebo elektronickej žiadosti (vytvorenej na mobilnom pracovisku priamo v teréne) osoby s obmedzenou schopnosťou pohybu vytvorí pracovník JP systémovú žiadosť štandardným spôsobom, pričom skontroluje údaje uvedené na písomnej žiadosti oproti údajom systémovej žiadosti získaných z referenčných zdrojov.
- V prípade, že systémová žiadosť je vytváraná na základe elektronickej žiadosti vytvorenej na mobilnom pracovisku v teréne, systém umožní na základe zadaného identifikátora načítanie údajov z off-line žiadosti vytvorenej na mobilnom pracovisku a ich automatizované porovnanie s údajmi evidovanými v centrálnom systéme. Systém upozorní na prípadný nesúlad tak, aby bolo následne zaručené bezpečné pripojenie biometrických údajov k správnej osobe a žiadosti.
- Ak sa údaje zhodujú, zaeviduje pracovník JP systémovú žiadosť štandardným spôsobom.
- Ak zistí pracovník JP nesúlad medzi údajmi uvedenými v písomnej (elektronickej) žiadosti oproti údajom systémovej žiadosti získaných z referenčných zdrojov, postupuje sa obdobne ako v prípade štandardnej žiadosti, t,j, vykonajú sa kroky, aby sa dosiahol súlad medzi skutočnosťou a údajmi evidovanými v centrálnych systémoch.
- Pracovník JP vyznačí, že táto žiadosť bude spracovaná v off-line režime. K takejto žiadosti nebude možné pripojiť všetky potrebné údaje štandardným spôsobom, t.j. priamym zosnímaním v činnosti Kompletizácia.
- Systém následne na základe údajov uvedených v systémovej žiadosti vytvorí jej off-line verziu potrebnú pre ďalšie spracovanie bez pripojenia k centrálnemu systému a uloží ju v samostatnom subsystéme, o čom upovedomí pracovníka JP. Takto je off-line žiadosť pripravená na bezpečné uloženie na pevný disk mobilného pracoviska. V prípade, že systémová žiadosť je vytváraná na základe elektronickej žiadosti

vytvorenej na mobilnom pracovisku v teréne, systém nevytvára off-line žiadosť.

- Obsluha mobilného pracoviska prevezme a uloží off-line žiadosť (resp. viaceré off-line žiadosti) bezpečným spôsobom na pevný disk mobilného pracoviska. O jej (ich) úspešnom uložení na pevný disk mobilného pracoviska systém obsluhu upovedomí.

5.1.2 Získanie off-line verzie biometrických údajov

- Po príchode obsluhy mobilného pracoviska k osobe s obmedzenou schopnosťou pohybu zobrazí obsluha mobilného pracoviska off-line systémovú žiadosť a nechá podpísať.
- Následne nad vybranou off-line systémovou žiadosťou vykoná kompletizáciu štandardným spôsobom.
- Aplikačné vybavenie pripojí nasnímané biometrické údaje k off-line žiadosti. O vytvorení off-line verzie biometrických údajov a ich uložení na pevný disk mobilného pracoviska a pripojení k off-line žiadosti bude upovedomená obsluha mobilného pracoviska.
- V prípade potreby bude umožnené vygenerovať off-line žiadosť v teréne na základe údajov poskytnutých oprávneným žiadateľom. Za týmto účelom budú v určenom subsystéme udržiavané a na mobilné pracoviská replikované potrebné číselníky z centrálneho systému.

5.1.3 Import biometrických údajov

- Po príchode obsluhy mobilného pracoviska na jednotné pracovisko a pripojení sa k centrálnemu systému, umožní aplikačné vybavenie na základe uloženej off-line žiadosti a biometrických údajov import biometrií do systému a ich pripojenie k systémovej žiadosti uloženej v centrálnom systéme.
- Následne bude systémová žiadosť štandardným spôsobom postúpená na personalizáciu.
- V prípade off-line žiadosti vytvorenej v teréne na mobilnom pracovisku (viď vyššie) bude pred importom biometrických údajov potrebné prostredníctvom osobitnej činnosti vytvoriť systémovú žiadosť, ako je popísané vyššie.

5.1.4 Odovzdanie dokladu držiteľovi

Proces odovzdania dokladu držiteľovi bude prebiehať doposiaľ zavedeným spôsobom.

6. Funkčný návrh systému

Funkčný návrh systému sa zameria predovšetkým na:

- funkčnú dekompozíciu navrhovaného riešenia
- dokumentáciu požadovanej funkcionality
- popis požadovaných atribútov kvality riešenia.

7. Návrh (dizajn) APV

Návrh (dizajn APV bude riešiť predovšetkým kľúčové princípy dizajnu pre:

- používateľské rozhrania (GUI),
- business logiku (komponenty, web služby a pod.),
- aplikačné programové rozhrania (API),
- perzistentnú vrstvu.

Celý systém bude v čo najväčšej miere podporovať procesy agendových a evidenčných úkonov a minimalizovať nutné úkony obsluhy.

Zálohovanie dát (Backup) bude vykonávané automaticky jestvujúcimi prostriedkami infraštruktúry výpočtového strediska OSK SITB MV SR. Obsluha má zabezpečovať len výmenu zálohovacích dátových médií.

Systém musí byť navrhnutý tak, aby – pokiaľ je to zmysluplné – jeden človek mohol zastávať jednu, viac alebo všetky pracovné role odrazu. Systém má umožňovať zmenu priradenia človeka (pridanie/uberanie) k jednotlivým pracovným roliam bez nutnosti odstávky systému.

8. Externé rozhrania

Súčasťou dodávky je úprava rozhraní na všetky systémy, pre ktoré sú kompletizované žiadosti o vydanie dokladov, ktoré sú predmetom tejto časti projektu. Použitie mobilných pracovísk bude umožnené v rámci agend JP CP, JP VP a JP OP.

9. Dokumenty a dokumentácia

V rámci projektu budú dodané nasledovné dokumenty v slovenskom jazyku:

- Procesný model
- Špecifikácia (analýza) požiadaviek
- Detailná špecifikácia rozhraní
- Plán testov vrátane návrhu testovacích procedúr
- Technická a prevádzková dokumentácia
- Používateľská dokumentácia

Dokumenty budú dodané v tlačenej forme v počte 1 kus ako aj v elektronickej forme v počte 1ks na CD nosiči.

V rámci projektu bude dodaná nasledovná dokumentácia:

- Dokumentácia k HW komponentom – Štandardná dokumentácia od výrobcov k jednotlivým HW komponentom. Pokiaľ nie je dostupná v slovenskom jazyku, táto bude dodaná v anglickom jazyku, vo formáte poskytovanom výrobcom.

10. Školenia

V rámci dodávky budú vykonané nasledovné školenia:

Názov	Počet účastníkov	Jeden turnus	Dĺžka trvania	Typ školenia / školiaci priestor	Čas vykonania
Školenie pracovníkov OTI („školenie č.1“)	30	30	0,5 dňa	Školiaca miestnosť	V súlade s Harmonogramom
Školenie administrátorov OSK SITB MV SR („školenie č.2“)	5	5	1 deň	Výpočtové stredisko, zasadačka	V súlade s Harmonogramom
Školenie používateľov mobilných pracovísk („školenie č.5“)	80	20	1 deň	Školiaca miestnosť	V súlade s Harmonogramom

Školenie pracovníkov OTI a Školenie administrátorov OSK SITB MV SR bude vykonané na základe dispozícií objednávateľa podľa možnosti spoločne s týmto typom školení v rámci subprojektu „Rozšírenie technického riešenia pre Jednotné pracoviská MV pre zber žiadostí na vydávanie elektronických eID kariet“.

Školiace priestory dostatočnej veľkosti s potrebnou infraštruktúrou zabezpečí objednávateľ.

Miesto konania školenia objednávateľ spresní najneskôr dva týždne pred konaním školenia.

Termíny školení bude spresnený v projektovom pláne.

V rámci aktivity Školenie objednávateľ okrem toho, že zrealizuje vlastné školenia zamestnancov objednávateľa, vykoná všetky činnosti spojené s prípravou a vyhodnotením školení. Zhotoviteľ pripraví školiace verzie systémov vrátane dát pre školenia, vytvorí užívateľské a administrátorské kontá v systémoch.

Po vlastnej realizácii školení vyhodnotí školiteľ spätnú väzbu účastníkov školenia na funkcionalitu a kvalitu APV.

Školiteľ zabezpečí praktické cvičenia pre zamestnancov objednávateľa na školiacich verziách systémov. Zhotoviteľ poskytne koučing zamestnancom objednávateľa pri osvojení si práce s novým APV.

Školiace materiály budú účastníkom školenia dodané najneskôr v deň školenia. Školenie bude vykonané v slovenskom jazyku.

11. Podpora rutinnej prevádzky

Po nasadení riešenia do riadnej rutinnej prevádzky u objednávateľa bude poskytnutá podpora počas 2 týždňov.

Pri podpore rutinnej prevádzky dodaného riešenia budú vykonávané najmä nasledovné činnosti:

- Metodická podpora súvisiaca so správou a používaním dodaného riešenia (monitorovacie činnosti a pod.),
- Iná metodickú podpora súvisiacu s používaním dodaného riešenia.

12. Mimo rozsahu dodávky

- Poskytovanie služieb súvisiacich s vydávaním, rušením a overovaním platnosti certifikátov na mobilnom pracovisku,
- Migrácia dát.

13. Zoznam použitých skratiek

Skratka	Popis
APV	Aplikačné programové vybavenie
Biometrická databáza	Databáza biometrických údajov pri ECU
CP	Cestovný pas
eID	Elektronická ID karta
eCP	Elektronický cestovný pas s biometriou
ECU	Agenda evidencie cudzincov
HW	Hardvér
IDC	Agenda občianskych preukazov
JP, IS JP	Jednotné pracoviská, Integrované riešenie Jednotných pracovísk pre zber žiadostí od občanov, zber údajov, kontrolu údajov, kontrolu dokladov a vydávanie vodičských preukazov, cestovných pasov a občianskych preukazov v pôsobnosti ODE PPZ
JP CP	Jednotné pracoviská pre cestovné pasy
JP OP	Jednotné pracoviská pre občianske preukazy
JP VP	Jednotné pracoviská pre vodičské preukazy
OoE I.	Elektronický doklad Osvedčenie o evidencii vozidla
OP	Občiansky preukaz, ID karta
OVD, IS OVD	Objednávanie výroby dokladov, Integrované riešenie Jednotných pracovísk na objednávanie výroby dokladov v pôsobnosti ÚHCP MV SR
SSW	Systémový softvér
SW	Softvér
VP	Vodičský preukaz

ČAST VII TECHNICKÉ RIEŠENIE PRE VYBUDOVANIE CENTRÁLNEJ TLAČE PRE HROMADNÚ TLAČ DOKUMENTOV V PÔSOBNOSTI MV SR

1. Súlad riešenia s relevantnými normami

Navrhované technické riešenie bolo posudzované podľa § 12 ods.3 písm. g/ zákona č. 264/1999 Z. z. a je v zhode s technickými požiadavkami nasledovných vládnych nariadení:

Číslo: 392/1999

Názov: Nariadenie vlády o technických požiadavkách a postupoch posudzovania zhody pre elektrické zariadenia, ktoré sa používajú v určitom rozsahu napätia

Číslo: 394/1999

Názov: Nariadenie vlády o technických požiadavkách na výrobu z hľadiska elektromagnetickej kompatibility

Pri posudzovaní zhody boli použité nasledovné technické normy:

Elektrická bezpečnosť:	STN EN 60950+A1+A2+A3+A4+A11 : 1999,
	STN EN 292 - 1 : 1996, STN EN 292 - 2+A1 : 1996,
	STN EN 294 : 1997
EMC :	STN EN 50081 - 1 : 1995, STN EN 50082 - 2 : 1999
	STN EN 55022 : 2000, STN EN 55014+A1 : 1997
	STN EN 61000-4-2 : 1995, STN EN 61000-4-4 : 1995
	STN EN 61000-4-5 : 1995

2. Prehlásenie o zhode

Zhotoviteľ prehlasuje, že predložené technické riešenie je v zhode s požiadavkami objednávateľa prezentovanými v podkladoch k verejnej súťaži v prílohe B1 - Opis predmetu zákazky časť VII: „Technické riešenie centrálnej tlače a obálkovania“.

3. Predmet Technického riešenia

Centrálna tlač predstavuje hlavný produkčný tlačový systém a záložný tlačový produkčný systém. Hlavný systém umožňuje okrem veľkokapacitného stohovania vytlačených dokumentov vybrané zariadenia finišovať. To znamená podľa nadefinovania požiadaviek zošívať, dierovať, triediť, predeľovať deliacimi hárkami, odsadzovať. V záložnom systéme produkčnej tlače tieto funkcie finišovania nie sú. Uvedené zariadenie tlačené dokumenty stohuje pre potreby podania do obálkovacej linky. Architektúra je uvedená na obrázku nižšie.

Tlačový systém sa skladá z 2 častí – návrhová časť a tlačový engine. Tieto sú štandardne dodávané v inštalácii spoločne. V prípade záujmu je možné dodať samostatné dizajnovacie časti. Tie umožnia tvorbu a dizajnovanie tlačových aplikácií mimo produkčného PC. Takto vytvorená tlačová aplikácia môže byť dizajnovaná na samostatnom PC, uložená ako samostatný súbor a prenesená do tlačového strediska, kde je použitá k produkcii.

Pre obálkovanie plastových kariet umiestnených na nosiče ako aj na obálkovanie A4 dokumentov s prílohami slúži hlavný obálkovací systém Kern 90 + Kern 2500 a pre obálkovanie A4 dokumentov s prílohami slúži záložný obálkovací systém Kern 656.

4. Popis navrhovaného riešenia

Navrhnuté riešenie umožňuje:

- Tvorby dynamických personalizovaných dokumentov vo formáte PCL, PS a PDF, tvorbu indexových súborov.
- V plne grafickom rozhraní s možnosťou náhľadu na generované dokumenty na obrazovke, alebo tlačené aj na lokálnej tlačiarni užívateľa. Naviac je možné dokumenty prezerať na obrazovke aj s tzv. live dátami, teda užívateľ má možnosť prezerať si dokumenty a ich variabilné prvky tak ako sa budú správať pri zmenách

dátových položiek.

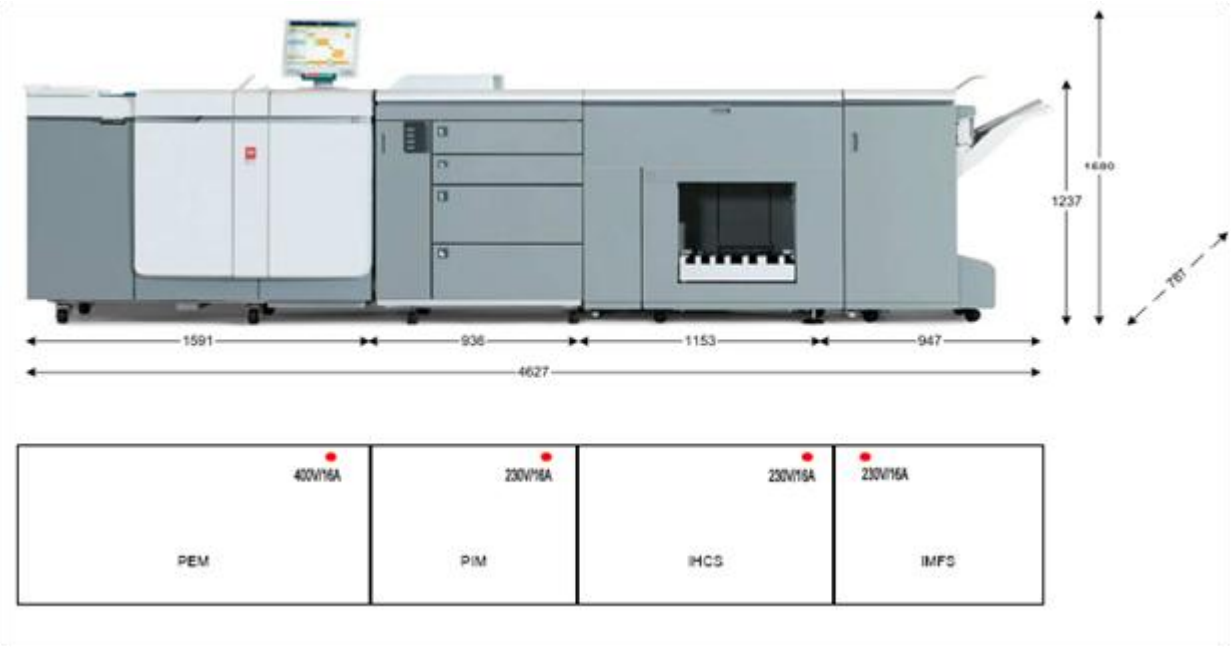
- Vkladanie dynamických dát, grafiky, čiarových kódov, kódov pre obálkovaciu linku na dokumenty.
- Tvorbu logiky pre variabilné objekty na dokumentoch.
- Tvorbu logových súborov.

Hlavný obálkovací systém Kern 90 + Kern 2500 v navrhovanej konfigurácii vykonáva čítanie OCR kódu z plastovej karty, tlač adresy a bar kódu na nosič s aplikáciou karty na personalizovaný nosič, kontrola správnosti aplikácie karty na nosič, skladanie nosiča do formátu obálky, dokladanie A4 príloh a dvoch príloh formátu obálky s následným vložením obsahu do obálky, na výstupe sa vykonáva kontrola výstupnej produkcie cez čítanie bar kóde informácií.

Halvný aj záložný obálkovací systém Kern 656 umožňujú obálkovanie dokumentov A4, ku ktorým je možné pridávať A4 prílohy a dve prílohy formátu obálky, obálky sú lepené/nelepené, môžu byť označované podľa dohodnutých kritérií. Celý proces obálkovania môže byť riadený prostredníctvom OMR značiek.

4.1. Technické parametre produkčných tlačových riešení

4.1.1 Centrálna tlač (T1)



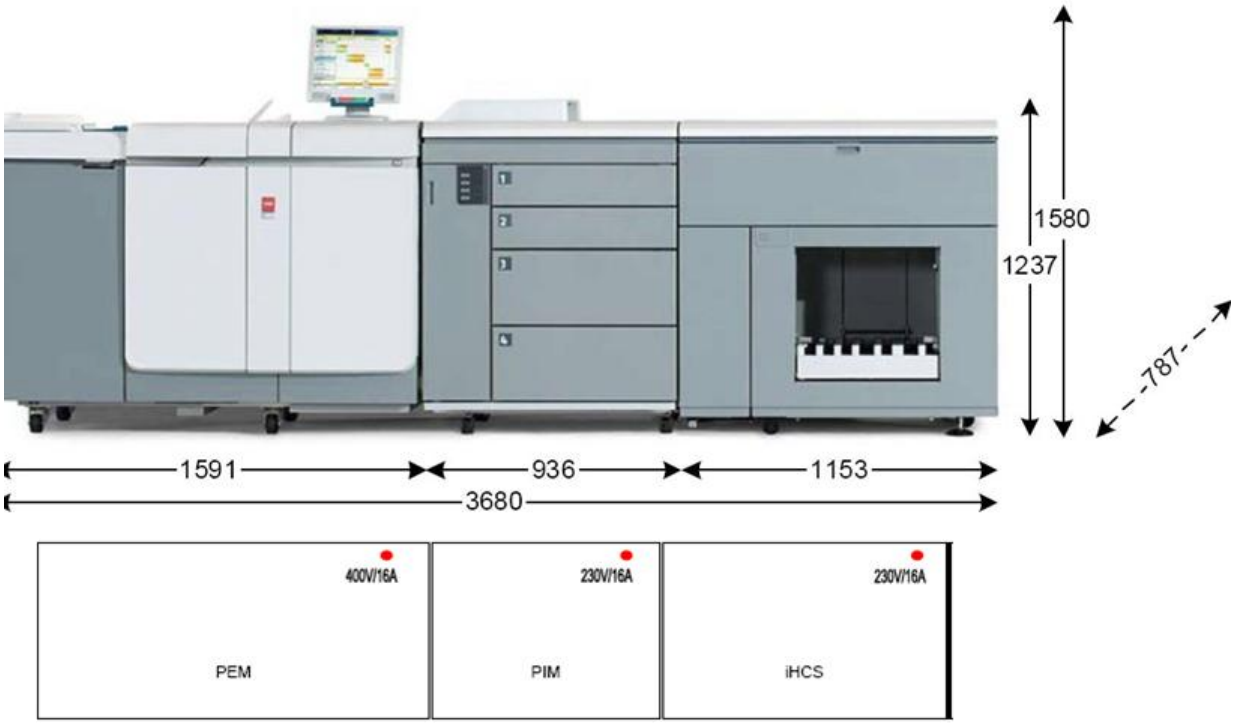
Obrázok č.4: Produkčný digitálny multifunkčný systém OCÉ VP4100 MFD (T1)

T1) Produkčný digitálny multifunkčný systém OCÉ VP4100 MFD (tlačiareň/skener/kopírovacie zariadenie)		
Konfigurácia		
Modul MFD (tlačová jednotka, kopírovacia jednotka, skenovacia jednotka)	Tlačiareň (PEM)	Rozmery 1591 x 787 x 1135 mm (šxhxv)
		Reprografický systém CopyPress
		LED, 600x1200 dpi, až 141 lpi
		Konzistentná a stabilná kvalita tlače ne širokú škálu médií
		106 tlačových strán A4/Letter/min v režime jednostrannej i obojstrannej tlače

			51 tlačových strán A3/min v režime jednostrannej i obojstrannej tlače
	Typ skeneru		skener CCD s Océ Image Logic
			automatická optimalizácia kvality pre reprodukciu originálov
			automatická detekcia podávania 2 listov/ originálov
			rýchlosť skenovania 56 strán originálu A4 za minútu
	Kopírovacia jednotka		rýchlosť kopírovania 56 strán originálu A4/min
			ADF pre 75 listov
			Plná produkcia pri obojstrannom kopírovaní
Kontroler Smart Imager HighEnd	zabudovaný kontrolér (riadiaci počítač) s celeron M2.0		
	1 GB RAM		
	Pevný disk 160 GB		
Veľkokapacitný zásobník (PIM)	Veľkosť a gramáž originálu:		60-170 g/m2
			minimálne 148 x 210 mm
			maximálne 297 x 432 mm
	Vstupné zásobníky papiera:		Rozmery 936 x 787 x 1135 mm (šxhxv)
			štandardne 4 zásobníky
			celková kapacita 4600 listov
			štandardné formáty: A4, B4. A3, Letter, Legal, Ledger
			štandardný rozsah gramáží 60-250 g/m2
			detekcia prázdneho zásobníka a indikácia množstva papiera
			doplňovanie zásobníkov pri tlači
			vzduchové oddeľovanie listov
iHCS	Rozmery 1153 x 787 x 1135 mm (šxhxv)		
	integrovaný veľkokapacitný stohovač		
	znáša 6000 listov 80g/m2 do dvoch stohov po 3000 listov		
	odoberanie výtlačkov v priebehu tlače		
iMFS	Rozmery	1153 x 787 x 815 mm (šxhxv)	
	Popis	Dokončovacie zariadenie	
		Integrovaná zošívačka rôznych formátov	
	Funkionalita	Triedenie	3 priehradky s celkovou kapacitou 4000 listov
		Zošívanie	
			Max. 100 listov v jednej sade 80g/m2
			Zošívanie v rohu, alebo v 2 miestach
		Dierovanie (doplnkovo)	Kompletný rozsah kombinácií dier
			Možnosť výmeny zákazníckeho razidla
			Dierovanie pri plnej rýchlosti stroja
Základná funkcionalita pri tlači			
Produkcia:	doporučený objem mesačnej produkcie 100.000 až 1.500.000 výtlačkov mesačne		

	špičkový objem až 2.500.000 výtlačkov mesačne
Správa tlače:	Dotyková obrazovka
	Identifikácia operátora (PIN kód), protokolácia úloh
	Optimalizácia tlačových úloh
	Automatizácia predávania tlačových súborov
	podpora fronty čakajúcich a plánovaných úloh
	podpora tlače pri rastrovaní a voliteľne streamovaní PostScript/PDF
	podpora transakčnej tlače s využitím IPDS a PJL/PCL
	súčasná tlač, skenovanie a kopírovanie
	neobmedzené programovanie ďalšej úlohy
	oddeľovacie listy – vkladanie cez studenú dráhu papiera
	rozsiahle možnosti programovania stránok v ovládači
Správa po sieti:	webové rozhranie nástrojov správy pre hlavného operátora
	webové rozhranie nástrojov správy pre systémového administrátora
	SNMP podporujúce MIB II, Host Resources, Printer, Job monitor a správu MIB
Jazyky:	Adobe Postscript, PDF 1.7, PCL, IPDS, PJL/PCL5e
Ovládače:	MS Windows 2000/XP/Vista PS3 a PCL6
	PS3 pre Macintosh OS 10.2 a vyššie
	Možnosti programovania stránok v ovládačoch PS3
	Automatizovaná tlač PDF, PS, PCL a TIFF s využitím Océ JobSubmitIT
Ostatné parametre	Rozmery 4627x787x1237 (vxšxh)
	Pre sťahovanie potrebná šírka chodby minimálne 890 mm
	Hmotnosť hlavnej jednotky: 585 kg
	Napájacie napätie: 230V/50 Hz, dvojfázový systém 15A/ jednofázový systém 30A
	Riadenie príkonu: o Automatické vypínanie o Režim zníženej spotreby energie o Režim spánku o Automatický prechod do prevádzkového režimu
	prakticky zanedbateľné emisie ozónu (koncentrácia menej ako 0,0005 ppm)
	1 W vo vypnutom stave
	Žiadny odpadový toner
	Nízka hlučnosť v pohotovostnom režime – 38 dB (A)
	Nízka hlučnosť pri prevádzke - 63 dB (A)

4.1.2 Záložná tlač (T2)



Obrázok č.5: Produkčný digitálny multifunkčný systém OCÉ VP4100 MFD (T1)

T2) Produkčný digitálny tlačový systém OCÉ VP4100		
Konfigurácia		
Tlačový modul (PEM)	Rozmery 1591 x 787 x 1135 mm (šxhxv)	
	Reprografický systém CopyPress	
	LED, 600x1200 dpi, až 141 lpi	
	Konzistentná a stabilná kvalita tlače ne širokú škálu médií	
	106 tlačových strán A4/Letter/min v režime jednostrannej i obojstrannej tlače	
	51 tlačových strán A3/min v režime jednostrannej i obojstrannej tlače	
Kontroler Smart Imager HighEnd	zabudovaný kontrolér (riadiaci počítač) s celeron M2.0	
	1 GB RAM	
	Pevný disk 160 GB	
Veľkokapacitný zásobník (PIM)	Veľkosť a gramáž originálu:	60-170 g/m2
		minimálne 148 x 210 mm
		maximálne 297 x 432 mm
	Vstupné zásobníky papiera:	Rozmery 936 x 787 x 1135 mm (šxhxv)
		štandardne 4 zásobníky
		celková kapacita 4600 listov
		štandardné formáty: A4, B4. A3, Letter, Legal, Ledger
		štandardný rozsah gramáží 60-250 g/m2
		detekcia prázdneho zásobníka a indikácia množstva papiera

		doplňovanie zásobníkov pri tlači
		vzduchové oddeľovanie listov
iHCS	Rozmery 1153 x 787 x 1135 mm (šxhxv)	
	integrovaný veľkokapacitný stohovač	
	znáša 6000 listov 80g/m2 do dvoch stohov po 3000 listov	
	odoberanie výtlačkov v priebehu tlače	
Základná funkcionalita pri tlači		
Produkcia:	doporučený objem mesačnej produkcie 100.000 až 1.500.000 výtlačkov mesačne	
	špičkový objem až 2.500.000 výtlačkov mesačne	
Správa tlače:	Dotyková obrazovka	
	Identifikácia operátora (PIN kód), protokolácia úloh	
	Optimalizácia tlačových úloh	
	Automatizácia predávania tlačových súborov	
	podpora fronty čakajúcich a plánovaných úloh	
	podpora tlače pri rastrovaní a voliteľne streamovaní PostScript/PDF	
	podpora transakčnej tlače s využitím IPDS a PJL/PCL	
	súčasná tlač, skenovanie a kopírovanie	
	neobmedzené programovanie ďalšej úlohy	
	oddeľovacie listy – vkladanie cez studenú dráhu papiera	
	rozsiahle možnosti programovania stránok v ovládači	
Správa po sieti:	webové rozhranie nástrojov správy pre hlavného operátora	
	webové rozhranie nástrojov správy pre systémového administrátora	
	SNMP podporujúce MIB II, Host Resources, Printer, Job monitor a správu MIB	
Jazyky:	Adobe Postscript, PDF 1.7, PCL, IPDS, PJL/PCL5e	
Ovládače:	MS Windows 2000/XP/Vista PS3 a PCL6	
	PS3 pre Macintosh OS 10.2 a vyššie	
	Možnosti programovania stránok v ovládačoch PS3	
	Automatizovaná tlač PDF, PS, PCL a TIFF s využitím Océ JobSubmitIT	
Ostatné parametre	Rozmery 3680 x 787 x 1237 (vxšxh)	
	Pre sťahovanie potrebná šírka chodby minimálne 890 mm	
	Hmotnosť hlavnej jednotky: 585 kg	
	Napájacie napätie: 230V/50 Hz, dvojfázový systém 15A/ jednofázový systém 30A	
	Riadenie príkonu: ○ Automatické vypínanie ○ Režim zníženej spotreby energie ○ Režim spánku ○ Automatický prechod do prevádzkového režimu	
	prakticky zanedbateľné emisie ozónu (koncentrácia menej ako 0,0005 ppm)	
	1 W vo vypnutom stave	
	Žiadny odpadový toner	

	Nízka hlučnosť v pohotovostnom režime – 38 dB (A)
	Nízka hlučnosť pri prevádzke - 63 dB (A)

4.1.3 Požiadavky pre správu tlače

Dotyková obrazovka pre používateľské rozhranie

- Systém spĺňa

Identifikácia používateľa (PIN kód), protokolácia úloh

- Systém spĺňa

Webové rozhranie nástrojov správy pre systémového administrátora, webové rozhranie nástrojov správy pre hlavného operátora,

- Systém spĺňa

Automatizácia predávania tlačových súborov

- Riešené v rámci dodávaného SW Newleaf

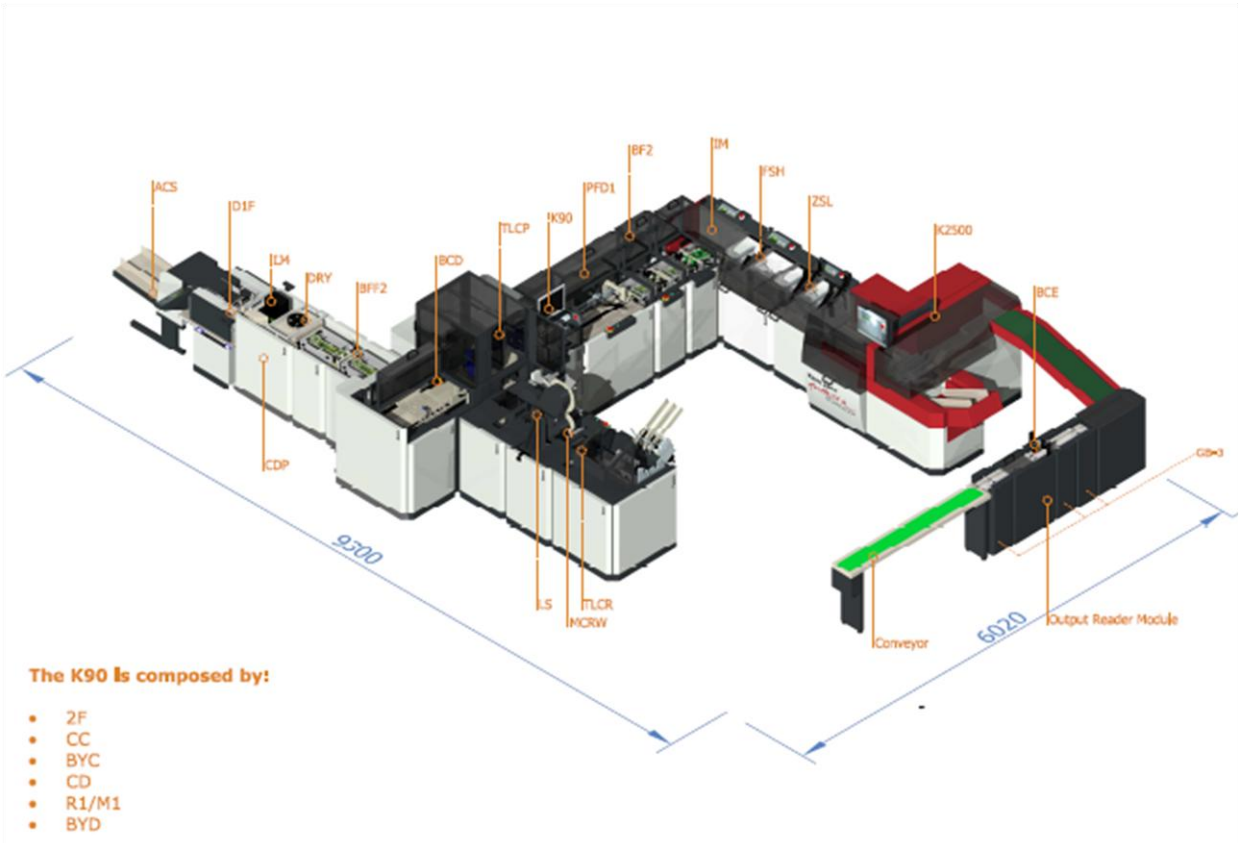
Presúvanie súborov v rámci tlačových front, optimalizácia tlače medzi viacerými tlačiarňami (hlavná, záložná)

- Riešené v rámci dodávaného SW Newleaf

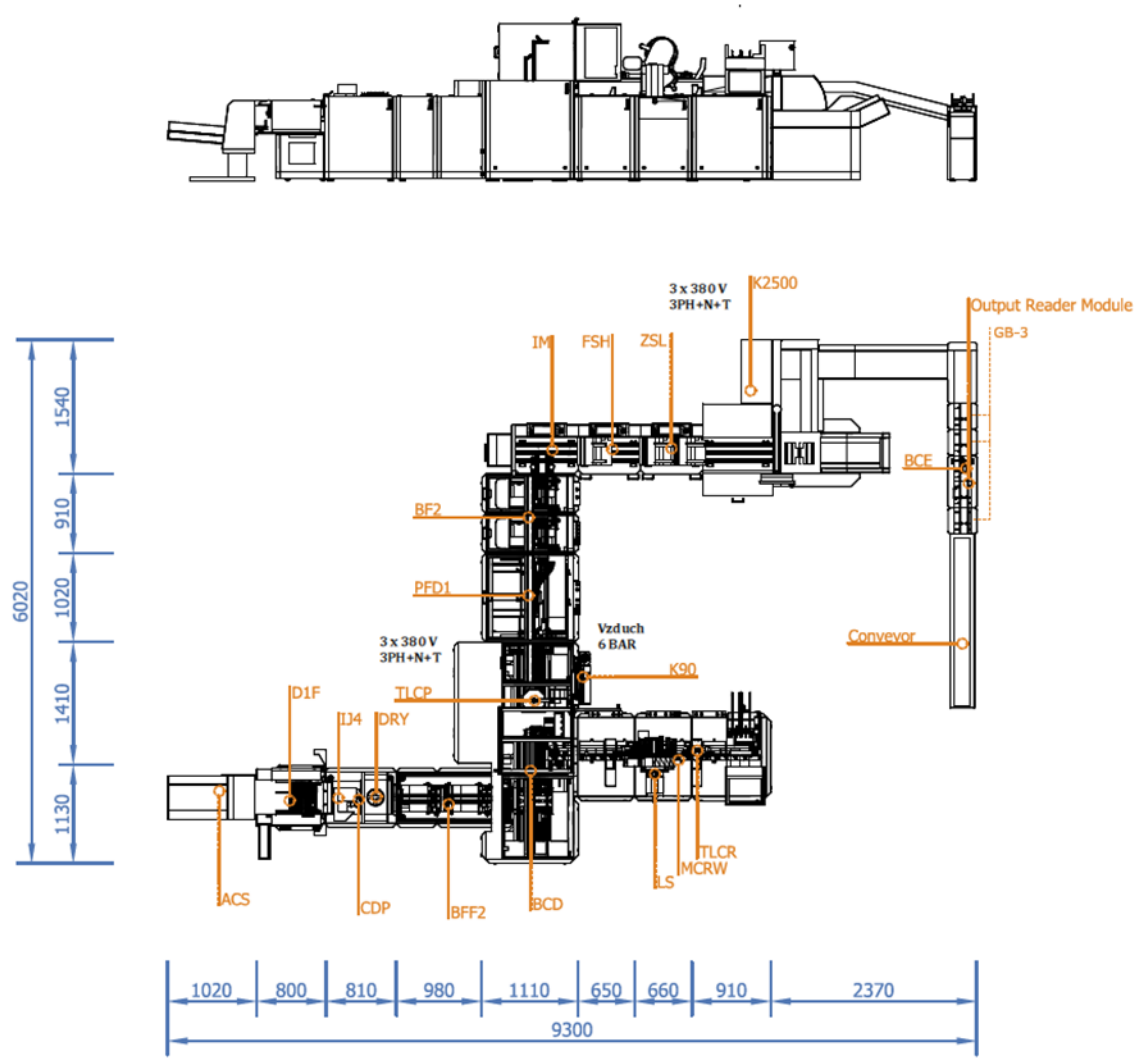
Otvorená architektúra, modulárny, rozšíriteľný systém

- Systém spĺňa

4.1.4 Hlavný obálkovací systém (OL1)



Obrázok č.6: Obálkovací systém KERN 90 + 2500 (OL1)



Obrázok č.7: Pôdorys obálkovacieho systému KERN 90 + 2500 (OL1)

OL1) Obálkovací systém KERN 90 + 2500		
Konfigurácia		
Sekcia kariet (pridávanie – identifikácia – priradenie)	2F	modul s N.02 podávačom kariet
	CC	transportný systém kariet
	MCR	kontaktné/bezkontaktné čítanie informácií priamo z mikročipu
	TLCR	kamera pre identifikáciu prednej časti plastových kariet
	LS	aplikátor obojstranne lepiacich nálepiek
	SPN	automatický modul na otáčanie karty
Sekcia pre A4 nosič (pridávanie a identifikácia)	1P4	Injekt ČB tlačiareň pre dotlač adresáta a čiarového kódu1D, 2D na nosič karty Nosič musí byť formátu A4 Šírka tlače 4“ Tento modul nie je možné použiť na potlač obálky na výstupe

	D1F	zásobník s podávačom a primárnym skladom na jednotlivé listy formátu A4 – nosič plastovej karty
	BCD	laserový snímač na čítanie barcode identifikácie A4 nosiča
	CD	dopravník dokumentov
	BYD	kôš na nespracované/vyradené dokumenty
Sekcia aplikácie karty na nosič	R1M1	robot SCARA s jedným ramenom pre podávanie kariet
	BYC	kôš na nespracované/vyradené karty
Výstupná časť	TLCP	telekamera s kontrolným systémom
	PFD1	primárne skladanie
	PFD2	sekundárne skladanie
	BF2	zbieranie a synchronizácia dokumentov na výstupe
Obálkovacia časť	IM	rozhranie medzi modulmi Kern 90 a Kern 2500
	D60	výstupné čítanie z modulu Kern 90
	FSHB	prídavný skladací modul pre A4 prílohy s čítaním barcode
	ZSL	stanica s 2 prídavnými zásobníkmi pre pridávanie príloh
	KV	obálkovací modul Kern 2500
	GB3	výstupný dopravník hotovej produkcie
	BCE	laserový snímač na identifikáciu bar kódu z obálky
	D90	výstupný pás s dĺžkou 2m pre hotovú produkciu
Softvér riadenia a kontroly	JBG RP	Job Manager – verzia na čítanie a tlač
	JBG PC	Job Manager – riadenie produkcie
Ostatné parametre		
Výkon	obálkovanie kariet 6 000 kariet/hod. Uvedený výkon je počet obálok na výstupnom páse, za predpokladu,že sa nanáša len 1 karta, na jeden nosič, prílohy idú bez obmedzenia. Plný výkon sa dosiahne za predpokladu,že nebude proces počas spracovávania kolácií prerušený.	
	obálkovanie dokumentov 8 000 obálok/hod. (bez obmedzenia pri vkladaní príloh do obálky)	
Veľkosť spracovávaných materiálov	Zásobník jednotlivých listov KERN 905 Formát: min. výška 70 mm x šírka 88 mm max. výška 430 mm x šírka 235 mm Váha: min. 70 g/m2 (pri neskladanom papieri) max. 180 g/m2	
	Prílohy od prídavnej a skladacej stanice FS: Formát: min. výška 70 mm x šírka 88 mm max. výška 430 mm x šírka 235 mm Váha: min. 70 g/m2 (pri neskladanom papieri) max. 180 g/m2	
	Prílohy od prídavnej stanice ZS (neskladané alebo predskladané do veľkosti použitej obálky): Formát: min. výška 70 mm x šírka 88 mm max. výška 150 mm x šírka 235 mm Váha: min. 70 g/m2 (pri neskladanom papieri) max. 240 g/m2 Hrúbka príloh: do 6 mm	

	Obálky: Formát: min. výška 80 mm x šírka 160 mm max. výška 178 mm x šírka 254 mm Váha: min. 80 g/m2 max.120 g/m2. Štandard formátu obálky: C6/5, resp. C5.
	Formát spracovávaných kariet 85,6 x 53,9 mm Hrúbka spracovávaných kariet od 0,3 do 0,82 mm.
Ostatné	Hlučnosť < 79 dB pod európskou normou
	Napájacie napätie 380 V, každá fáza istená pomalým ističom 30 A
	Príkon 17,5 kW
	Tepelný výkon 17,5 kJ/s,
	Váha 6000 kg
	Rozmery 9300 x 6020 mm

4.1.4.1. Popis jednotlivých sekcií OL1

Sekcia kariet Kern 90

Skladá sa z dvoch zásobníkov kariet, modulu pre transport kariet, čítacieho modulu pre čítanie OCR kódu a modulu pre aplikáciu obojstranne lapiacej pásky.

Sekcia pre A4 nosič

Skladá sa zo zásobníka pre 4000 ks A4 dokumentov s rýchlosťou podávania 20 000 dok./hod., modulu inkjet tlačiarne, modulu pre snímanie barcode a prívodného modulu pre A4 nosič.

Sekcia aplikácie kariet na nosič

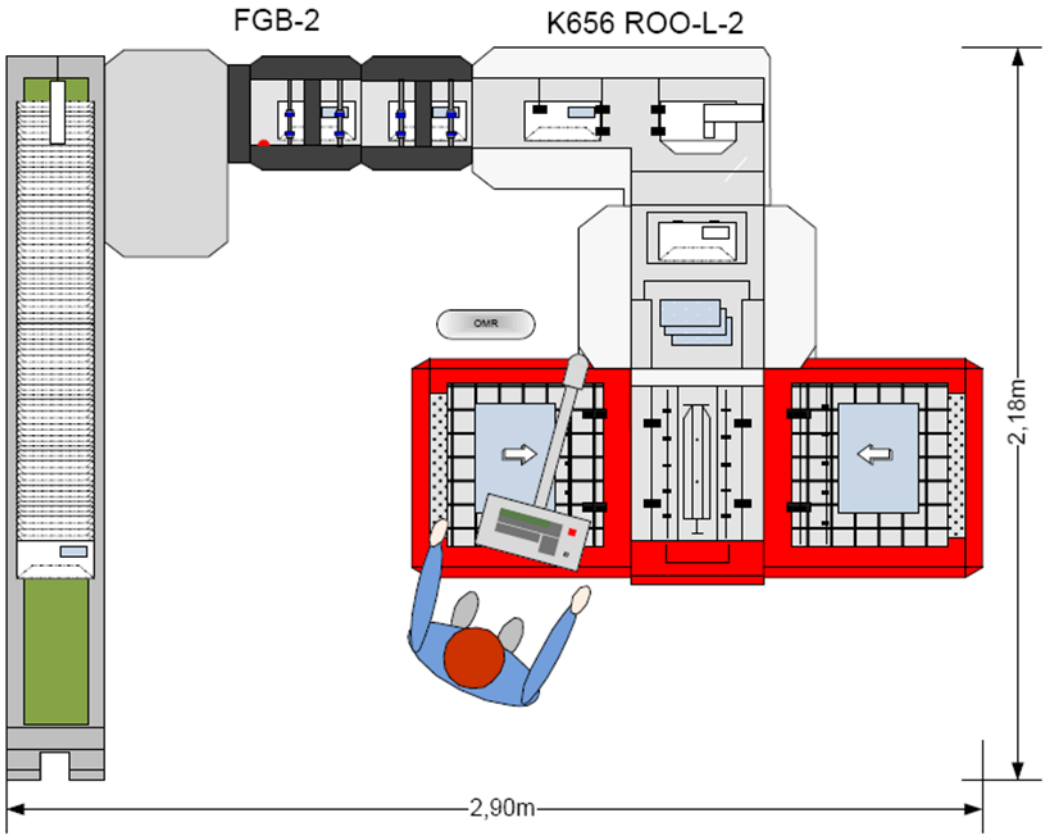
Skladá sa z modulu pre aplikáciu kariet a check boxu pre vyradené karty

Výst. časť sekcie pre spracovanie kariet sa skladá z kamerového modulu pre kontrolu nosiča s kartou, z modulov pre skladanie nosiča na formát obálky a z modulu pre zhromažďovanie a synchronizáciu produkcie.

Obálkovacia časť Kern 2500

Skladá sa z rozhrania medzi K90 a K2500, s modulov pre pridávanie 1 x A4 prílohy a 2 x príloh formátu obálky, s rýchlosťou podávania 30 000 príloh/hod., nasleduje samotný obálkovací modul pre vkladanie hotovej produkcie do obálky, na výstupe je laserový snímač barcode a pre hotovú produkciu je použitý 2 metrový výst. pás

4.1.5 Záložný obálkovací systém (OL2)

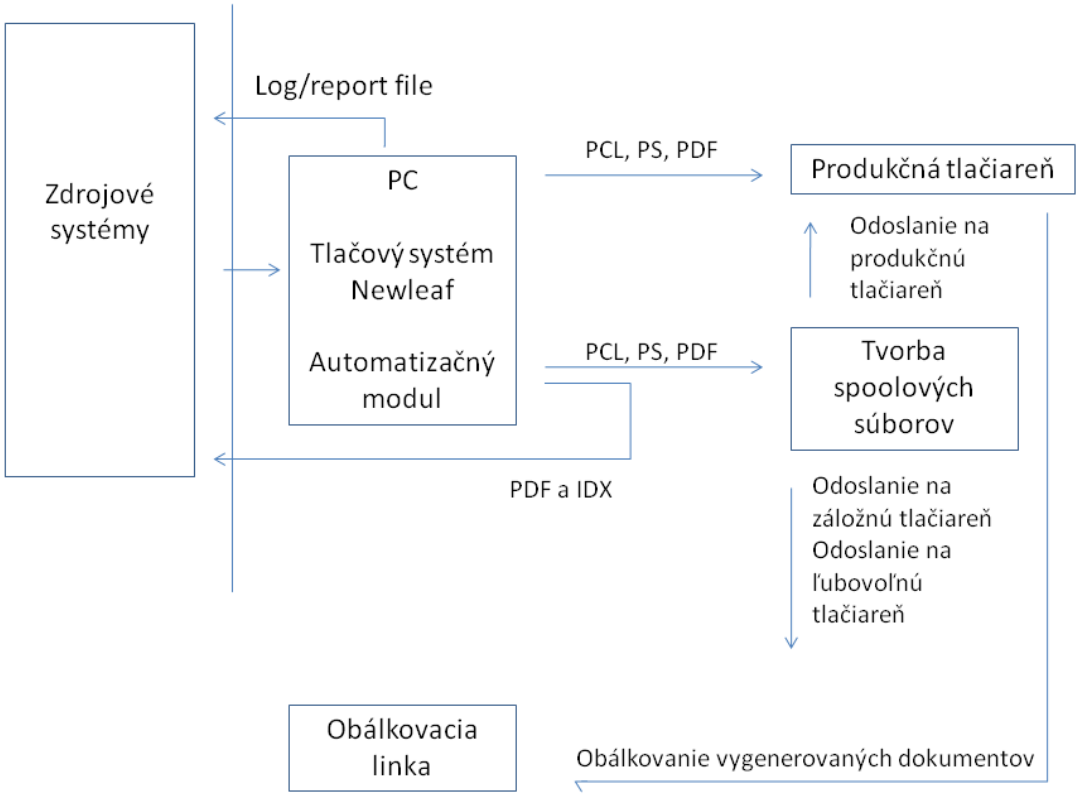


Obrázok č.8: Obálkovací systém KERN 686 LBO-RBO-3 (OL2)

OL2) Obálkovací systém Kern 686 LBO-RBO-3	
Popis	
Obálkovací systém v uvedenej konfigurácii spracováva hlavné dokumenty pozostávajúce z jednotlivých listov papiera s možnosťou pridávania príloh veľkosti A4 z druhého zásobníka a pridávanie jednej, dvoch alebo troch príloh veľkosti obálky, resp. príloh predskladaných do formátu obálky. Celý proces obálkovania môže byť riadený Barcode značkami, ktoré sú čítané z hlavných dokumentov.	
Konfigurácia	
Skladací a obálkovací systém KERN 686	skladacia a prídavná stanica ľavá pre skladanie a pridávanie formulárov veľkosti A4, resp. A3 s čítaním Barcode riadiacich znakov
	skladacia a prídavná stanica pravá pre skladanie a pridávanie formulárov veľkosti A4, resp. A3 s čítaním Barcode riadiacich znakov
	prídavná stanica KERN č.1 pre pridávanie príloh formátu obálky
	zoskupovací výstupný pás GB-1.
Výkon	menovitý: 8000 obálok/hod
	skutočný: 4000 - 7000 obálok/hod

Veľkosť spracovávaných materiálov	Zásobník jednotlivých listov KERN 905 Formát: min. výška 70 mm x šírka 88 mm max. výška 430 mm x šírka 235 mm Váha: min. 70 g/m^2 (pri neskladanom papieri) max. 180 g/m^2
	Prílohy od prídavnej a skladacej stanice FS: Formát: min. výška 70 mm x šírka 88 mm max. výška 430 mm x šírka 235 mm Váha: min. 70 g/m^2 (pri neskladanom papieri) max. 180 g/m^2
	Prílohy od prídavnej stanice ZS (neskladané alebo predskladané do veľkosti použitej obálky): Formát: min. výška 70 mm x šírka 88 mm max. výška 150 mm x šírka 235 mm Váha: min. 70 g/m^2 (pri neskladanom papieri) max. 240 g/m^2 Hrúbka príloh: do 6 mm
	Obálky: Formát: min. výška 80 mm x šírka 160 mm max. výška 178 mm x šírka 254 mm Váha: min. 80 g/m^2 max.120 g/m^2. Štandard formátu obálky: C6/5, resp. C5.
Ostatné parametre	Hlučnosť < 79 dB pod európskou normou
	Systém neprodukuje žiadne emisie, hlučnosť pod 77 dB
	Napájacie napätie 220 V, každá fáza istená pomalým ističom 30 A
	Príkon 1,5 kW
	Tepelný výkon 1,5 kJ/s,
	Váha 550 kg
	Rozmery 2900 x 2180 mm

5. Funkčný návrh systému



Obrázok č.9: Návrh architektúry pre riešenie centrálnej tlače

Dáta prichádzajúce zo zdrojového systému sú spracované na PC, na ktorom je nainštalovaný tlačový engine Newleaf. Tu dôjde ku spojeniu tlačových dát a šablóny dokumentu a tvorbe požadovaného tlačového výstupu.

Tlačový engine vygeneruje tlačový výstup, môže generovať (sériovo, nie paralelne) PCL, PS a PDF, ako aj tvorbu indexových výstupov. Tento výstup spolu s PDF umožňuje tvorbu tlačových výstupov pre archiváciu dokumentov, napr. v DMS alebo archivačnom systéme.

Tlačový engine môže odosielať súbory priamo na tlačiareň, prípadne vytvárať tlačový výstup spoolového súboru. Operátor sa potom môže rozhodnúť, na ktoré zariadenie odošle tlačový súbor pre potreby využitia kapacity viacerých tlačiarní a rozloženia load ballancingu tlačovej kapacity.

V prípade záujmu je možné nasadiť aj automatizačný modul, ktorý umožní automatizované spracovanie jobov, identifikáciu dátových položiek a spúšťanie tlačových jobov. Tento modul nemá vplyv na cenu licenčnej ani infraštruktúrnej zložky riešenia. V ponuke ho nenavrhujeme implementovať, nakoľko považujeme za praxou overené, že Operátorom riadené spracovanie je menej náchylné na chyby spôsobené nedodržaním všetkých potrebných podmienok pre automatizáciu zo strany zdrojových systémov a/alebo obsluhy. Jeho nasadenie, ale bude predmetom analýzy v etape zberu požiadaviek a na základe jej záverov prípadne implementované. Automatizačný modul vyžaduje nasadenie Java RealTime Environment na produkčnom PC.

5.1. Tlačový systém Newleaf

Newleaf je samostatne stojacou aplikáciou s grafickým používateľským rozhraním.

Newleaf software umožňuje tvorbu dokumentov a ich tlač na tlačiarňachi OCE vo formáte PCL, PS a PDF, rýchlosťou 160 strán za minútu.

Riešenie umožňuje vytváranie dokumentu, vkladanie textov, variabilných dátových premenných, vkladanie statickej aj dynamickej grafiky, ako aj čiarových kódov.

V grafickom WYSIWYG rozhraní používateľ vytvára dokument priamo vo formáte, v akom je generovaný na výstupe. V tomto rozhraní má možnosť prezerať náhľady dokumentov, tvoriť testovacie výstupy pre potreby vzorových tlačí aj na lokálnej tlačiarni bez potreby pripojenia na produkčnú tlač.

Ponúkané riešenie umožňuje generovať výstupy vo formátoch PCL, PS aj PDF, k nim generovať indexový súbor pre potreby archivácie vygenerovaných dokumentov.

Vygenerované súbory je možné odosielať na tlačiarne podporujúce tieto formáty, licencia nie je viazaná na danú konkrétnu tlačiareň alebo na konkrétne PC. Newleaf je licencovaný podľa rýchlosti generovania výstupov a počtu generovaných výstupov podľa kapacitných požiadaviek zadefinovaných pre zariadenia centrálnej, resp. záložnej tlače.

Všeobecne umožňuje vkladanie rôznych objektov na stránku, ako sú dynamická grafika, texty, čiarové kódy apod. Tieto objekty je možné podmienkovať a definovať logiku ich zobrazenia. Po vytvorení želaného layoutu je následne možné tento vygenerovať v želanom tlačovom výstupe, s možnosťou simplex/duplex tlače, N-UP tlače, definície rozmerov papiera apod. Jednoduchým pripojením dát je možné tieto vložiť drag & drop systémom priamo na dokument. Po načítaní dát umožňuje vkladanie objektov na stránky, ako sú statické a dynamické texty, grafika, grafy apod.Zároveň umožňuje vkladanie a definíciu čiarových kódov.

Jednotlivé objekty môžu mať definovanú logiku správania a ich variabilitu. Napríklad u grafického objektu je možné vložiť dva obrázky, a na základe vytvorenia podmienok definovať zobrazovanie danej grafiky. Po vytvorení dokumentu umožňuje jeho tlač a produkciu na tlačiarni zvolením typu výstupu (1up, 2up), veľkosť papiera, a voľby veľkosti tlačovej dávky.

5.2. Požiadavky na SW riešenie tlače a obálkovania

SW pre tvorbu personalizovaných dát a šablón tlačových zostáv s WYSIWYG rozhraním

- Newleaf je plne WYSIWYG.

Podpora čiarových kódov.

- Newleaf ponúka širokú škálu čiarových kódov.

Tvorba riadiaceho súboru pre obálkovaciu linku

- Tlačový systém Newleaf umožňuje tvorbu omr značiek pre riadenie obálkovacej linky, prípadne využitie čiarového kódu pre jej riadenie. Riešenie natívne podporuje funkčnosť tzv. mailera, ktorý umožňuje parsovanie tlačového súboru na obálkovanie.

SW na riadenie tlače personalizovaných údajov

- Riadenie tlače (umiestnenie adresy a sprievodného textu na nosič ku ktorému je prilepená ID 1 karta.
- Pri centrálnej tlači je potrebné uvažovať s použitím obálok s dvoma okienkami (kvôli spätnej adrese)

Integrácia do Dokument manažment systému (DMS) MV SR za účelom možnosti archivovania tlačových súborov

- Newleaf generuje výstupy do definovaného adresára, nedisponuje webservice alebo soap rozhraním. Vyššie uvedený automatizačný modul, ale umožní prenos výstupov na požadované miesto, odkiaľ bude prebraté middle-ware vrstvou.

Možnosť load balancingu tlačových úloh ktoré nemajú predpísanú výstupnú tlačiareň

- Operátor si môže zvoliť na ktorú tlačiareň odošle požadovaný výstup.

Správa dotlače

- Newleaf defaultne umožňuje definovanie rozsahu tlačených dokumentov, prípadne na základe logiky.

Možnosť náhľadu tlačovej/obálkovacej úlohy

- Default, na obrazovke prezeranie live dát, tlač na lokálnej tlačiarni.

Možnosť vyhľadávania v rámci tlačovej/obálkovacej úlohy

- Viď dotlač

Možnosť riadenia priorít

- Odporúčame manuálne spúšťanie tlačových aplikácií, s ohľadom na bezpečnosť a predídenie chyby nekorektného zaslania dátového súboru s inou tlačovou aplikáciou. Je potrebne adresovať spôsob ich splnia resp nesplnenia jednotivo po bulletoch.

Odporúčania z prevádzkového hľadiska

Na základe skúseností z návrhu a rozvoja tlačových stredísk u viacerých zákazníkov navrhujeme nižšie uvedené odporúčania:

- Vyhradiť samostatný sieťový segment pre tlačové riešenie – tzv. subnet mask. Toto zabezpečí oddelenie tlačovej časti riešenia od ostatného spracovania, a umožní zvýšenú ochranu dát proti zneužitiu. Obe lokality navzájom musia mať umožnené v segmente mapovanie sieťových tlačiarní a zdieľaných dátových úložísk.
- Záloha tlačového systému – tlačový systém Newleaf je licencovaný na základe USB HW kľúča. Pre potreby zálohovanie produkčného prostredia umožňuje tento systém inštaláciu produkčného prostredia na ľubovoľnom počte počítačov. V prípade poruchy HW produkčného prostredia je možné jednoducho prehodiť USB kľúč s licenciou na záložné PC, nakopírovať od zálohované tlačové aplikácie a pokračovať v tlači. Preto navrhujeme dodané záložné PC umiestniť na komplementárnu lokalitu ako je produkčný tlačový systém, t.j. do záložného personalizačného centra. Ako záložné riešenie pre prípad úplnej havárie (nebude použitý HW kľúč s dočasnou licenciou) bude e-mailom z definovanej supportnej adresy zaslaný objednávateľovi dočasná SW licencia, ktorá bude používaná až do doby, kým zhotoviteľ nedodá nový HW USB klúč.
- Zálohovanie tlačových aplikácií systému – využitím automatizačných zálohových modulov, ktoré sú natívne k dispozícii v inštalácii operačného systému Windows XP navrhujeme nastaviť automatizované zálohovanie adresára, v ktorom budú uložené jednotlivé tlačové aplikácie. V prípade havárie HW na produkčnom PC môžu prevádzkovatelia riešenia jednoducho nakopírovať odzálohované aplikácie a okamžite pokračovať v produkcii. Navrhujeme zálohovať na vyčlenený diskový priestor v komplementárnej lokalite.

6. Externé rozhrania

Tlačový systém predpokladá, že zdrojové systémy (alebo poskytnutý midleware systém objednávateľa, ak bude nejaký prevádzkovaný) bude schopný spúšťať Joby tlačového systému. Alternatívnou možnosťou je, že tlačový systém bude používať sprístupnené Webservisy zdrojových systémov na to, aby získal dáta pre jednotlivé tlačové požiadavky (pull) a rovnakým spôsobom vracal spätné informácie (log), resp. zapisoval tlačené dokumenty do DMS za účelom archivácie. Vo fáze špecifikácie požiadaviek bude v spolupráci s objednávateľom došpecifikované vhodné rozhranie (so zdrojovými systémami aj DMS) a následne sa stane záväzným pre všetky zdrojové systémy používajúce hromadnú tlač.

7. Dokumenty a dokumentácia

V rámci projektu budú dodané nasledovné dokumenty v slovenskom jazyku:

- Špecifikácia (analýza) požiadaviek
- Detailná špecifikácia rozhraní
- Plán testov vrátane návrhu testovacích procedúr

Dokumenty budú dodané v tlačenej forme v počte 1 kus ako aj v elektronickej forme v počte 1ks na CD nosiči.

V rámci projektu bude dodaná nasledovná dokumentácia:

Obálkovacie systémy	Používateľská dokumentácia • technický popis systému Kern 2500 + Kern 90 a jeho parametre • operátorskú príručku ku systému Kern 2500 • chybové oznamy systému Kern 2500 • pokyny pre vykonávanie základnej údržby
	Používateľská dokumentácia • technický popis systému Kern 686 a jeho parametre • operátorskú príručku ku systému Kern 686 • chybové oznamy systému Kern 686 • pokyny pre vykonávanie základnej údržby
Tlačové systémy	Bezpečnostná príručka

	Operátorský manuál VP4000 (zahŕňa používateľskú, technickú aj prevádzkovú dokumentáciu)
Software	Používateľský manuál

Pokiaľ nie je štandardná dokumentácia od výrobcov dostupná v slovenskom jazyku, táto bude dodaná v anglickom jazyku, vo formáte poskytovanom výrobcom.

8. Školenia

V rámci dodávky budú vykonané nasledovné školenia:

Názov	Počet účastníkov	Dĺžka trvania	Popis školenia	Čas vykonania
Školenie operátorov tlačových zariadení A1, B1 („školenie č.1“)	10	1 deň	Základné zaškolenie operátorov v rámci inštalácie v rozsahu 6 hodín pre 10 osôb. V rámci školenia budú vysvetlené vlastnosti zariadenia, jeho obsluha a všetky potrebné a pravidelné úkony operátora – vkladanie papiera, dopĺňanie tonera, riadenie a správa tlačových úloh, operátorské čistenie stroja.	V súlade s Harmonogramom
Školenie operátorov obálkovacích systémov A2, B2 („školenie č.2“)	10	2 dni	Ciele školenia: účastníci kurzu musia zvládnuť vykonanie základných obsluhujúcich činností potrebných pre prevádzkovanie obálkovacích systémov Kern, čítanie OMR a barcode značiek, zvládnutie základného mechanického nastavenia obálkovacích systémov Kern, vykonávanie denných profylaktických činností Obsah školenia: komunikačná konzola systému Kern, riadenie obálkovacieho systému, komunikácia so systémom, základné nastavenie systému Kern vykonávanie prevádzkových zmien programov, výber aplikácií, odstraňovanie jednoduchých prevádzkových porúch, vykonanie kontroly základného nastavenia systému a rezacieho automatu, lokalizácia porúch na základe oznamov, základná technická starostlivosť o systém, praktické cvičenia na systéme.	V súlade s Harmonogramom
Školenie operátorov, používateľov SW Newleaf	10	1-2 dni	Popis celého prostredia SW pre účely NPC. Zameranie sa na konkrétne úlohy v procesoch NPC.	V súlade s Harmonogramom

Školenie používateľov a operátorov tlačových a obálkovacích systémov za nasledujúcich podmienok:

- Operátori musia mať základné znalosti práce s PC.

Miesta školení:

- školiace pracoviská kupujúceho, ktoré budú oznámené predávajúcemu zo strany kupujúceho najneskôr 3 pracovné dni pred začatím príslušného školenia,

Jazyk školenia:

- slovenský a/alebo formou prekladu z anglického do slovenského jazyka

9. Podpora rutinnej prevádzky

Po nasadení riešenia do riadnej rutinnej prevádzky u objednávateľa bude poskytnutá podpora počas 2 týždňov.

Pre zvládnutie rutinnej prevádzky budú k dispozícii technickí pracovníci pre obálkovací i tlačový systém. Počas školenia budú operátori poučení o možnosti využívať helpdesk a hotline linku pre zvládnutie prevádzky systémov. Počas prvých 2 týždňov rozbehu oboch systémov budú technickí pracovníci držať pohotovosť priamo v mieste inštalácie a budú schopní zasiahnuť okamžite po nahlásení problému.

V rámci záručnej doby prebieha starostlivosť o zariadenia formou preventívnej starostlivosti. Okamih preventívnej prehliadky je určovaný servisným oddelením na základe pravidelnej informácie od objednávateľa ohľadne realizovanej produkcie. Nahlasovanie stavu počítadiel – mesačne - ako aj nahlasovanie prípadných porúch prebieha zo strany objednávateľa na definované číslo servisného dispečingu. V prípade servisného zásahu, ktorý vznikne na základe nedodržania prevádzkových podmienok, nedovolených zásahov, nevykonania predpísaných operátorských činností alebo používania papiera, ktorý nezodpovedá doporučeniu výrobcu bude takýto zásah spoplatnený v zmysle platného cenníka prác a dielov.

V prípade, ak je potrebné pre zabezpečenie prevádzky mimo bežnej pracovnej doby zabezpečiť dostupnosť servisného technika, objednávateľ môže takúto pohotovosť objednať na servisnom dispečingu. Pohotovosť je potrebné objednať minimálne 48 hodín pred jej predpokladaným začiatkom. Servisná pohotovosť bude spoplatnená podľa platného cenníka servisných služieb.

10. Rozšírená podpora nábehu rutinnej prevádzky

Po zahájení rutinnje prevádzky systémov Centrálen tlače a obálkovania bude zhotoviteľ zabezpečovať zvýšenú podporu prevádzky podľa potrieb objednávateľa. Počas rozšírenej podpory bude zabezpečená účasť zástupcov zhotoviteľa pre jednotlivé fázy nábehu priamo v priestoroch zákazníka.

V rámci rozšírenej podpory nábehu rutinnej prevádzka budú vykonávané činnosti:

- Príprava predproduktívnej prevádzky
- Retestovanie za účasti zhotoviteľa
- Dohľad nad nábehom systému
- Zvýšená konzultačná podpora – účasť implementačných tímov zhotoviteľa na mieste
- Koučovanie zamestnancov objednávateľa
- Podpora pri tvorbe ad-hoc požiadaviek objednávateľa na centrálnu tlač počas obdobia jedného roka

11. Zoznam použitých skratiek

Skratka	Popis
T1	Centrálny produkčný tlačový systém
OL1	Centrálna obálkovacia linka
T2	Záložný produkčný tlačový systém
OL2	Záložná obálkovacia linka
PEM	Tlačový engine
PIM	Veľkokapacitný zásobník
iHCS	Integrovaný veľkokapacitný stohovač
iMFS	Integrované multifunkčné dokončovacie zariadenie
MFD	Multifunkčný systém
DMS	Systém riadenia dokumentov

V Bratislave dňa .....28.08.2012.....

Za Zhotoviteľa

Hewlett-Packard Slovakia, s.r.o.

_____

Ing. Martin Kubala

Generálny riaditeľ a konateľ

V Bratislave dňa .....28.08.2012.....

Za Objednávateľa

Ministerstvo vnútra Slovenskej republiky

_____

Ing. Denisa Saková, PhD.

Vedúca služobného úradu Ministerstva vnútra

Príloha č.2 - Harmonogram

Časť I. Rozšírenie technického riešenia Personalizačného systému v Národnom personalizačnom centre Ministerstva vnútra Slovenskej republiky o personalizáciu elektronických eID kariet a vybudovanie technického riešenia pre Záložné personalizačné centrum pre personalizáciu dokladov v pôsobnosti MV na báze hrubého polykarbonátu podľa normy ISO 7810

Časť Diela	Podmienka/štart	Trvanie
Aktualizácia procesného modelu pre dokladu eID a DoPP	Podpis zmluvy	12 týždňov
Schválenie aktualizácie procesného modelu	Reštart projektu	3 týždne
Špecifikácia (analýza) požiadaviek na zmeny APV Personalizačného systému	Aktualizácia procesného modelu akceptovaná	5 týždňov
Návrh (dizajn) zmien APV	Špecifikácia (analýza) požiadaviek akceptovaná	11 týždňov
APV pre koordináciu NPC a ZNPC a podporu dokladov eID a eDoPP s kontaktným čipom	Návrh (dizajn) zmien APV akceptovaný	37,2 týždňov
Migrácia APV pre koordináciu NPC a ZNPC do rutinnej prevádzky v NPC	APV pre koordináciu NPC a ZNPC a podporu dokladov eID a eDoPP s kontaktným čipom	16 dní
Funkčná špecifikácia ePerso pre eID a eDoPP	Podpis zmluvy	10 týždňov
Funkčná špecifikácia ePerso pre eID a eDoPP (dokončenie)	Reštart projektu	6 týždňov
Dizajn ePerso pre eID a eDoPP	Funkčná špecifikácia zmien ePerso akceptovaná	8 týždňov
Implementácia ePerso	Dizajn zmien ePerso akceptovaný	16 týždňov
Funkčná špecifikácia Inšpekčného systému pre eID a eDoPP	Podpis zmluvy	12 týždňov
Funkčná špecifikácia Inšpekčného systému pre eID a eDoPP (dokončenie)	Reštart projektu	6 týždňov
Dizajn Inšpekčného systému	Funkčná špecifikácia Inšpekčného systému akceptovaná	8 týždňov
Implementácia Inšpekčného systému NPC	Dizajn Inšpekčného systému akceptovaný	16 týždňov
Integrácia Inšpekčného systému do JP	Implementácia Inšpekčného systému akceptovaná	4 týždňov
Testovanie	Ukončené časti: Implementácia APV pre eID a eDoPP Implementácia ePerso Integrácia Inšpekčného systému do JP	3 týždne
Spracovanie dokumentácie	Po ukončení implementácie	6 týždňov
Návrh pracovných rolí a procedúr	Po ukončení implementácie	6 týždňov
Špecifikácia logickej dátovej štruktúry (LDS) pre eID a eDoPP	Podpis zmluvy	16 týždňov
Špecifikácia logickej dátovej štruktúry (LDS) pre eID a eDoPP (dokončenie)	Reštart projektu	6 týždňov
Vývoj funkčného prototypu eID a eDoPP	Špecifikácia logickej dátovej štruktúry (LDS) akceptovaná	22 týždňov
Certifikácia prototypu eID a eDoPP	Vývoj funkčného prototypu eID a eDoPP akceptovaný	48 týždňov
Obstaranie testovacích čistopisov s čipom pre eID a eDoPP *	Nutná podmienka začiatku Akceptačných testov	0 týždňov
Akceptačné testy riešenia NPC pre eID a eDoPP s čipom	Čistopisy sú k dispozícii a Školenia sú ukončené	4 týždne

Príloha č.2 k Dodatku č.3 k Zmluve o dielo č. SE-OVO-13-050/2010

Časť Diela	Podmienka/štart	Trvanie
Školenia	Dokumentácia odovzdaná	2 týždne
Príprava rutinnej prevádzky. Personalizačný Systém pripravený na rutinnú prevádzku v NPC.	Integračné testovanie ukončené	1 týždeň
Podpora rutinnej prevádzky	Štart rutinnej prevádzky	2 týždne
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po vykonaní akceptačných testov	6 týždňov
Bezpečnostný zámer	Špecifikácia (analýza) požiadaviek na zmeny APV Personalizačného systému akceptovaná	7 týždňov
Analýza bezpečnosti	Bezpečnostný zámer akceptovaný	17 týždňov
Bezpečnostná smernica	Analýza bezpečnosti akceptovaná	14 týždňov
Vykonanie analýzy a návrh EAC PKI	Reštart projektu + 21 týždňov	14 týždňov
Dodávka HW a licencií pre EAC PKI infraštruktúru	Analýza a návrh EAC PKI akceptované	2 týždne
Implementácia EAC PKI infraštruktúry	Dodávka HW a licencií pre EAC PKI infraštruktúru	10 týždňov
Testovanie EAC PKI infraštruktúry	Dodávka HW a licencií pre EAC PKI infraštruktúru	3 týždne
Zaškolenie PKI administrátorov a operátorov	Testovanie EAC PKI infraštruktúry	6,5 týždňa
Akceptácia EAC PKI infraštruktúry	Zaškolenie PKI administrátorov a operátorov ukončené	4 týždne
Spracovanie dokumentácie	EAC PKI infraštruktúra akceptovaná	7 týždňov
Príprava EAC PKI infraštruktúry do rutinnej prevádzky a štart rutinnej prevádzky	Dokumentácia odovzdaná	6 týždňov
Podpora po nasadení riešenia do rutinnej prevádzky	Akceptácia nasadenie riešenia EAC PKI infraštruktúry do rutinnej prevádzky	2 týždne
Plán priestorového usporiadania	Reštart projektu	6 týždňov
Príprava priestorov ZNPC *	Plán priestorového usporiadania akceptovaný + 5 týždňov	23 týždňov
Dodávka HW/SW infraštruktúry pre APV do ZNPC	ZNPC pripravené na inštaláciu technológie	3 týždne
Inštalácia HW/SW infraštruktúry pre APV do ZNPC	Dodávka HW/SW infraštruktúry pre APV do ZNPC	4 týždne
Výroba personalizačnej technológie	Reštart projektu + 8 týždňov	9 týždňov
FAT testy	Výroba personalizačnej technológie ukončená	2 týždne
Inštalácia personalizačnej technológie	FAT testy ukončené ZNPC pripravené na inštaláciu technológie	3 týždne
SAT testy	Inštalácia personalizačnej technológie akceptovaná	3 týždne
Inštalácia APV a jeho súčasti pre všetky typy dokladov v ZNPC	ZNPC pripravené na inštaláciu technológie	3,4 týždna
Školenia	Inštalácia APV a jeho súčasti pre všetky typy dokladov v ZNPC ukončená	2 týždne
Akceptačné testy	SAT testy ukončené	2 týždne
Príprava rutinnej prevádzky ZNPC	Školenia ukončené	1 týždeň
Akceptácia uvedenia Personalizačného systému v ZNPC do rutinnej prevádzky	Príprava rutinnej prevádzky ZNPC akceptovaná	0 týždňov
Podpora rutinnej prevádzky	Akceptácia uvedenia Personalizačného systému v ZNPC do rutinnej prevádzky	2 týždne
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po vykonaní akceptačných testov	6 týždňov

* úloha v zodpovednosti Objednávateľa

Časť II. Rozšírenie IS SA agenda občianskych preukazov o funkčnosť realizujúcu vygenerovanie a spracovanie výrobných objednávok na personalizáciu elektronickej eID karty

Časť Diela	Podmienka/štart	Trvanie
Špecifikácia požiadaviek	Podpis zmluvy	6 týždňov
Schválenie Špecifikácie požiadaviek	Reštart projektu	3 týždne
Funkčný návrh systému	Špecifikácia požiadaviek akceptovaná	10 týždňov
Návrh (dizajn) APV	Funkčný návrh systému akceptovaný	9,5 týždňa
Implementácia rozšírenia APV (časť I.)	Návrh (dizajn) APV akceptovaný	25 týždňov
Návrh testovacích procedúr	Implementácia rozšírenia APV (časť I.) ukončená	4 týždne
Vykonanie školení a Akceptačné testovanie (časť I.)	Návrh testovacích procedúr ukončený	4 týždne
Dokumentácia (časť I.)	Návrh testovacích procedúr akceptovaný	4 týždne
Časť I. pripravená na PROD	Dokumentácia (časť I.) odovzdaná, Školenia ukončené, Aplikácia akceptovaná	0 týždňov
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po spustení produkčnej prevádzky	6 týždňov
Implementácia rozšírenia APV (časť II.)	Časť I. pripravená na PROD nasadená v PROD a Rozšírená podpora nábehu rutinnej prevádzky ukončená	7 týždňov
Školenie a dokumentácia	Implementácia rozšírenia APV (časť II.) ukončená	2 týždne
Akceptačné a Integračné testovanie	Školenie ukončené	3 týždne
Príprava rutinnej prevádzky	Akceptačné a Integračné testovanie ukončené	2 týždne
Uvedenie do rutinnej prevádzky	Príprava rutinnej prevádzky ukončená Personalizačný systém v ZNPC akceptovaný Certifikácia prototypu ukončená	0 týždňov
Podpora rutinnej prevádzky	Uvedenie do rutinnej prevádzky	2 týždne
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po vykonaní akceptačných testov	6 týždňov

Časť III. Rozšírenie technického riešenia pre Jednotné pracoviská MV pre zber žiadostí na vydávanie elektronických eID kariet

Časť Diela	Podmienka/štart	Trvanie
Procesný model	Podpis zmluvy	6 týždňov
Schválenie Procesného modelu	Reštart projektu	3 týždne
Špecifikácia (analýza) požiadaviek	Procesný model akceptovaný	6 týždňov
Dizajn rozhraní pre integráciu	Špecifikácia (analýza) požiadaviek akceptovaná	6 týždňov
Odovzdanie HW čítačiek na kontrolu elektronických ID kariet	Reštart projektu	15 týždňov
Dodanie HW a SW do výpočtového strediska OSK SITB MV SR	Špecifikácia (analýza) požiadaviek akceptovaná	20 týždňov
Dodania HW a SW na Oddelenia dokladov PPZ	Špecifikácia (analýza) požiadaviek akceptovaná	20 týždňov
Implementácia (časť I.)	Špecifikácia (analýza) požiadaviek a Dizajn rozhraní akceptované a nie skôr ako bude ukončená Integrácia Inšpekčného systému do JP	24 týždňov
Odovzdanie dokumentácie (časť I.)	8 týždňov po ukončení Implementácie časti I.	4 týždne
Vykonanie školení a Akceptačné testovanie	8 týždňov po ukončení Implementácie časti I.	4 týždne
Príprava a nasadzovanie (časť I.)	Školenia a akceptačné testy ukončené	0 týždňov
Časť I. pripravená na PROD	Aplikácia akceptovaná	0 týždňov

Časť Diela	Podmienka/štart	Trvanie
Implementácia (časť II.)	Implementácia (časť I.) ukončená a riešenie v produkcii Dokumentácia (časť I.) odovzdaná	20 týždňov
Školenie a dokumentácia	2 týždne pred začiatkom Integračných a Akceptačných testov	2 týždne
Akceptačné a Integračné testovanie	Školenie ukončené	3 týždne
Príprava rutinnej prevádzky	Integračné a akceptačné testovanie ukončené	1 týždeň
Uvedenie do rutinnej prevádzky	Príprava rutinnej prevádzky a Akceptácia uvedenia Personalizačného systému v ZNPC do rutinnej prevádzky a Certifikácia prototypu ukončená	0 týždňov
Podpora rutinnej prevádzky	Uvedenie do rutinnej prevádzky	2 týždne

Časť IV. eGovernment služby poskytujúce občanom možnosť realizácie vybraných služieb pre vydávanie elektronických eID prostredníctvom Internetu

Časť Diela	Podmienka/štart	Trvanie
Procesný model eGovernment služieb	4,5 týždňa po akceptácii Návrhu (dizajnu) APV v časti II.	6 týždňov
Riešenie zmeny eGov služieb a rozhodnutie na strane Zákazníka *	Rozhodnutie zákazníka	0 týždňov
Dokončenie Procesného modelu na základe rozhodnutia Zákazníka	Rozhodnutie zákazníka	6 týždňov
Špecifikácia požiadaviek na eGovernment služby	Procesný model eGovernment služieb akceptovaný	6 týždňov
Funkčný návrh pre eGovernment služieb	Špecifikácia požiadaviek akceptovaná	9,5 týždňa
Technický návrh eGovernment služieb	Špecifikácia požiadaviek akceptovaná	9,5 týždňa
Implementácia Webových služieb	Technický návrh eGovernment služieb akceptovaný	16 týždňov
Implementácia formulárov pre Web portál MV SR	Technický návrh eGovernment služieb akceptovaný	16 týždňov
Návrh testovacích procedúr	Technický návrh eGovernment služieb akceptovaný	16 týždňov
Dokumentácia	Technický návrh eGovernment služieb akceptovaný	16 týždňov
Riešenie portálu (UPVS) je pripravené a je zabezpečená aj integrácia služieb na portál *	Technický návrh eGovernment služieb akceptovaný	0 týždňov
Školenia	Dokumentácia akceptovaná a Implementácia ukončená Portál pripravený a služby zaintegrované *	3 týždne
Integračné a akceptačné testy	Školenia ukončené Riešenie IAM pripravené	3 týždne
Inštalácia a príprava rutinnej prevádzky	Týždeň pred ukončením Integračných a akceptačných testov	2 týždne
Uvedenie do rutinnej prevádzky	Inštalácia a príprava rutinnej prevádzky akceptovaná	0 týždňov
Podpora rutinnej prevádzky	Uvedenie do rutinnej prevádzky	2 týždne
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po vykonaní akceptačných testov	6 týždňov

* úloha v zodpovednosti Objednávateľa

Časť V. Technické riešenie pre zabezpečenie centralizovaného riadenia prístupu k implementovaným eGovernment službám

Časť Diela	Podmienka/štart	Trvanie
Procesný model	Podpis zmluvy	8 týždňov

Časť Diela	Podmienka/štart	Trvanie
Schválenie Procesného modelu	Reštart projektu	2,5 týždňa
Funkčný model	Procesný model akceptovaný	6 týždňov
Detailná funkčná špecifikácia	Funkčný model akceptovaný	6 týždňov
Dodávka hardvérového vybavenia	Reštart projektu	10 týždňov
Dodávka SW licencií	Reštart projektu	10 týždňov
Implementácia riešenia	Detailná funkčná špecifikácia akceptovaná a dodávka SW licencií akceptovaná	20 týždňov
Príprava a Akceptácia dokumentu Technická Architektúra *	V rámci Implementácie riešenia	21 týždňov
Dokončenie Implementácie riešenia	Dokument Technická Architektúra akceptovaný	10 týždňov
Školenia administrátorov	Implementácia riešenia ukončená	8 týždňov
Dokumentácia	Implementácia riešenia ukončená	8 týždňov
Integračné a akceptačné testy	Školenia ukončené	4 týždne
Inštalácia a príprava rutinnej prevádzky	Integračné a akceptačné testy ukončené	6 týždňov
Uvedenie do rutinnej prevádzky	Inštalácia a príprava rutinnej prevádzka školenia ukončené	0 týždňov
Podpora rutinnej prevádzky	Uvedenie do rutinnej prevádzky	2 týždne
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po vykonaní akceptačných testov	6 týždňov
Dodávka licencií podpory interných užívateľov	Podpis zmluvy	4 týždne
Implementácia podpory interných používateľov pre integráciu externých dodávok a riešenie znalostnej databázy	Reštart projektu	6 týždňov
Implementácia podpory interných používateľov pre riadenie prístupových oprávnení	Implementácia podpory interných používateľov pre integráciu externých dodávok a riešenie znalostnej databázy akceptované	24 týždňov
Vykonanie používateľských testov	Pred ukončením Implementácie podpory interných používateľov pre riadenie prístupových oprávnení	4 týždne
Integrácia web služieb interných systémov	6 týždňov od začiatku Implementácie riešenia	29 týždňov
Vykonanie testov integrácie web služieb interných systémov	Integrácia web služieb interných systémov akceptovaná	2 týždne

Časť VI. Rozšírenie technického riešenia pre Jednotné pracoviská MV o Mobilné pracoviská na zber žiadostí pre vydávane elektronických eID kariet

Časť Diela	Podmienka/štart	Trvanie
Procesný model	Podpis zmluvy	6 týždňov
Schválenie Procesného modelu	Reštart projektu	2,5 týždňa
Špecifikácia (analýza) požiadaviek	Procesný model akceptovaný	7 týždňov
Dizajn rozhraní pre integráciu	Špecifikácia (analýza) požiadaviek akceptovaná	7,5 týždňa
Dodanie HW a SW mobilných pracovísk	Špecifikácia (analýza) požiadaviek akceptovaná	20 týždňov
Implementácia	Dizajn rozhraní pre integráciu a špecifikácia požiadaviek akceptované	24 týždňov
Odovzdanie dokumentácie	Implementácia ukončená	2 týždne
Inštalácia	Implementácia ukončená	4 týždne
Školenie	Inštalácia dokončená	2 týždne
Akceptačné a Integračné testy	Školenia ukončené	3 týždne

Príprava rutinnej prevádzky	Akceptačné a Integračné testovanie ukončené	1 týždeň
Uvedenie do rutinnej prevádzky	Príprava rutinnej prevádzky akceptovaná	0 týždňov
Podpora rutinnej prevádzky	Uvedenie do rutinnej prevádzky	2 týždne

Časť VII. Technické riešenie pre vybudovanie Centrálnej tlače pre hromadnú tlač dokumentov v pôsobnosti MV SR

Časť Diela	Podmienka/štart	Trvanie
Dodávka hlavnej obálkovacej linky do NPC	Podpis zmluvy	1 týždeň
Inštalácia hlavnej obálkovacej linky v NPC	Dodávka hlavnej obálkovacej linky do NPC akceptovaná	2 týždne
Špecifikácia požiadaviek na riešenie centrálnej tlače a obálkovanie tlačových dokumentov	Podpis zmluvy	12 týždňov
Schválenie špecifikácie požiadaviek na riešenie centrálnej tlače a obálkovanie tlačových dokumentov	Reštart projektu	6 týždňov
Dodávka a inštalácia zariadení pre centrálnu tlač do NPC	Reštart projektu	1 týždeň
Dodávka a inštalácia obálkovacej linky do ZNPC	ZNPC pripravené na inštaláciu technológie	16 týždňov
Dodávka a inštalácia zariadení pre centrálnu tlač do ZNPC	Ku ukončeniu dodávky a inštalácie obálkovacej linky do ZNPC	14 týždňov
Implementácia riešenia centrálnej tlače v NPC	Dodávka a inštalácia zariadení pre centrálnu tlač do NPC a akceptovaná špecifikácia požiadaviek na riešenie centrálnej tlače a obálkovanie tlačových dokumentov	16 týždňov
Akceptačné testy	Implementácie riešenia centrálnej tlače ukončená	13 týždňov
Odovzdanie dokumentácie	4 týždne pred ukončením akceptačných testov	4 týždne
Školenie	Dokumentácia odovzdaná	2 týždne
Príprava rutinnej prevádzky a uvedenie do rutinnej prevádzky	Spolu s ukončením Školení	2 týždne
Podpora rutinnej prevádzky	Uvedenie do rutinnej prevádzky	2 týždne
Rozšírená podpora nábehu rutinnej prevádzky	Podľa potrieb objednávateľa po vykonaní akceptačných testov	6 týždňov

Spustenie eID s čipom

Časť Diela	Podmienka/štart	Trvanie
Ostré čistopisy pripravené	Rozhodnutie zákazníka	0 týždňov
Príprava produkčnej prevádzky dokladu s čipom	Ostré čistopisy sú pripravené	8 týždňov
Vykonanie zmeny prepínača na produkcii	Produkčná prevádzka pripravená	1 týždeň
Riešenie eID s čipom pripravené na PROD	Zmena v prepínači vykonaná	0 týždňov
Podpora nábehu rutinnej prevádzky systémov NPC, IS SA, JP a MP	Riešenie v produkcii	2 týždne

Harmonogram čiastkových plnení

Míľnik / Bod Zmluvy	Názov plnenia	Termín Dodania	Poznámka
1 / 3.1	Aktualizácia procesného modelu	-	Akceptované
2 / 3.2	Špecifikácia (analýza) požiadaviek	-	Akceptované
3 / 3.3	Návrh (dizajn) zmien APV	-	Akceptované
4 / 3.4	Funkčná špecifikácia Inšpekčného systému pre eID a eDoPP	-	Akceptované
5 / 3.5	Rozšírenie bezpečnostného projektu NPC - Bezpečnostný zámer	-	Akceptované
6 / 3.6	Rozšírenie bezpečnostného projektu NPC - Analýza bezpečnosti	-	Akceptované
7 / 3.7	Rozšírenie bezpečnostného projektu NPC - Bezpečnostná smernica	-	Akceptované
8 / 3.8	Implementácia a testovanie APV, ePerso a Inšpekčného systému pre eID a eDoPP	-	Akceptované
9 / 3.9	Spracovanie dokumentácie	-	Akceptované
10 / 3.10	Návrh pracovných rolí a procedúr	-	Akceptované
11 / 3.11	Školenia administrátorov, operátorov a používateľov NPC	-	Akceptované
12 / 3.12	Špecifikácia logickej dátovej štruktúry (LDS) pre eID a eDoPP	-	Akceptované
13 / 3.13	Vývoj funkčného prototypu eID a eDoPP	-	Akceptované
14 / 3.14	Integračné a akceptačné testy	19.10.2012	
15 / 3.15	Príprava rutinnej prevádzky NPC	26.10.2012	
16 / 3.16	Podpora rutinnej prevádzky NPC	18.3.2013	
17 / 3.17	Rozšírená podpora nábehu rutinnej prevádzky NPC	30.4.2013	
18 / 3.18	Vykonanie analýzy a návrh EAC PKI	-	Akceptované
19 / 3.19	Dodávka HW pre EAC PKI infraštruktúru	-	Akceptované
20 / 3.20	Dodávka licencií pre EAC PKI infraštruktúru	-	Akceptované
21 / 3.21	Implementácia EAC PKI infraštruktúry	-	Akceptované
22 / 3.22	Testovanie EAC PKI infraštruktúry	-	Akceptované
23 / 3.23	Spracovanie dokumentácie EAC PKI	28.9.2012	
24 / 3.24	Zaškolenie PKI administrátorov a operátorov	-	Akceptované
25 / 3.25	Príprava EAC PKI infraštruktúry do rutinnej prevádzky	26.10.2012	
26 / 3.26	Podpora rutinnej prevádzky EAC PKI	18.3.2013	
27 / 3.27	Plán priestorového usporiadania	-	Akceptované
28 / 3.28	Dodávka HW infraštruktúry pre APV do ZPC	-	Akceptované
29 / 3.29	Dodávka SW infraštruktúry pre APV do ZPC	-	Akceptované
30 / 3.30	Dodávka HW personalizačnej technológie - MX6000	-	Akceptované
31 / 3.31	Dodávka HW personalizačnej technológie - MX2000	-	Akceptované
32 / 3.32	Dodávka SW personalizačnej technológie	-	Akceptované
33 / 3.33	Inštalácia personalizačnej technológie a vykonanie SAT testov	-	Akceptované
34 / 3.34	Školenia administrátorov, operátorov a používateľov ZPC	-	Akceptované
35 / 3.35	Akceptačné testovanie riešenia ZPC	-	Akceptované
36 / 3.36	Príprava rutinnej prevádzky ZPC	-	Akceptované
37 / 3.37	Podpora prevádzky ZPC	-	Akceptované

38 / 3.38	Rozšírená podpora nábehu rutinnej prevádzky ZPC	31.1.2013	
39 / 3.39	Špecifikácia požiadaviek	-	Akceptované
40 / 3.40	Funkčný návrh	-	Akceptované
41 / 3.41	Technický návrh	-	Akceptované
42 / 3.42	Implementácia riešenia	28.9.2012	
43 / 3.43	Integračné a akceptačné testy	19.10.2012	
44 / 3.44	Technická a používateľská dokumentácia	-	Akceptované
45 / 3.45	Inštalácia a príprava rutinnej prevádzky	26.10.2012	
46 / 3.46	Podpora rutinnej prevádzky	18.3.2013	
47 / 3.47	Rozšírená podpora nábehu rutinnej prevádzky IS SA	31.3.2013	
48 / 3.48	Tréningy a školenia	28.9.2012	
49 / 3.49	Procesný model	-	Akceptované
50 / 3.50	Špecifikácia požiadaviek	-	Akceptované
51 / 3.51	Dizajn rozhraní pre integráciu	-	Akceptované
52 / 3.52	Dodanie HW - čítačky	-	Akceptované
53 / 3.53	Dodanie HW pre Inšpekčný systém eID	-	Akceptované
54 / 3.54	Dodanie HW pre Kontrolný systém biometrie	-	Akceptované
55 / 3.55	Dodanie HW pre hraničnú kontrolu	-	Akceptované
56 / 3.56	Dodanie SW pre Inšpekčný systém eID	-	Akceptované
57 / 3.57	Dodanie SW licencií pre hraničnú kontrolu	-	Akceptované
58 / 3.58	Obstaranie SW - Kontrolný systém biometrie	-	Akceptované
59 / 3.59	Implementácia riešenia	28.9.2012	
60 / 3.60	Integračné a akceptačné testy	19.10.2012	
61 / 3.61	Technická a používateľská dokumentácia	28.9.2012	
62 / 3.62	Inštalácia a príprava rutinnej prevádzky	26.10.2012	
63 / 3.63	Rollout a štart rutinnej prevádzky	26.10.2012	
64 / 3.64	Podpora rutinnej prevádzky	18.3.2013	
65 / 3.65	Tréningy a školenia	28.9.2012	
66 / 3.66	Procesný model	26.10.2012	
67 / 3.67	Špecifikácia požiadaviek	7.12.2012	
68 / 3.68	Funkčný návrh	8.2.2013	
69 / 3.69	Technický návrh (dizajn)	8.2.2013	

70 / 3.70	Implementácia riešenia	17.5.2013	
71 / 3.71	Integračné a akceptačné testy	14.6.2013	
72 / 3.72	Technická a používateľská dokumentácia	17.5.2013	
73 / 3.73	Inštalácia a príprava rutinnej prevádzky	24.6.2013	
74 / 3.74	Podpora rutinnej prevádzky	8.7.2013	
75 / 3.75	Rozšírená podpora nábehu rutinnej prevádzky eGov	31.7.2013	
76 / 3.76	Školenia	27.5.2013	
77 / 3.77	Procesný model	-	Akceptované
78 / 3.78	Špecifikácia požiadaviek	-	Akceptované
79 / 3.79	Detailná funkčná špecifikácia	-	Akceptované
80 / 3.80	Dodávka hardvérového vybavenia	-	Akceptované
81 / 3.81	Dodávka SW licencií - aplikačný SW	-	Akceptované
82 / 3.82	Dodávka SW licencií - infraštruktúrny SW	-	Akceptované
83 / 3.83	Implementácia riešenia	26.10.2012	
84 / 3.84	Integračné a akceptačné testy	14.1.2013	
85 / 3.85	Technická a používateľská dokumentácia	20.12.2012	
86 / 3.86	Inštalácia a príprava rutinnej prevádzky	25.2.2013	
87 / 3.87	Školenia	14.1.2013	
88 / 3.88	Podpora rutinnej prevádzky	15.3.2013	
89 / 3.89	Rozšírená podpora nábehu rutinnej prevádzky IAM	31.3.2013	
90 / 3.90	Dodávka licencií interných používateľov	-	Akceptované
91 / 3.91	Implementácia podpory interných používateľov pre integráciu externých dodávateľov a riešenie znalostnej databázy	-	Akceptované
92 / 3.92	Implementácia podpory interných používateľov pre riadenie prístupových oprávnení	-	Akceptované
93 / 3.93	Vykonanie používateľských testov podpory interných používateľov pre riadenie prístupových oprávnení	-	Akceptované
94 / 3.94	Integrácia a testovanie web služieb interných systémov do architektúry eGovernment služieb	-	Akceptované
95 / 3.95	Procesný model	-	Akceptované
96 / 3.96	Špecifikácia požiadaviek	-	Akceptované
97 / 3.97	Dizajn rozhraní pre integráciu	-	Akceptované
98 / 3.98	Dodanie HW mobilných pracovísk	-	Akceptované
99 / 3.99	Dodanie SW mobilných pracovísk	-	Akceptované

100 / 3.100	Implementácia riešenia a jeho otestovanie	-	Akceptované
101 / 3.101	Integračné a akceptačné testy	19.10.2012	
102 / 3.102	Technická a používateľská dokumentácia	-	Akceptované
103 / 3.103	Inštalácia a príprava rutinnej prevádzky	26.10.2012	
104 / 3.104	Rollout a štart rutinnej prevádzky	26.10.2012	
105 / 3.105	Podpora rutinnej prevádzky	18.3.2013	
106 / 3.106	Školenia	28.9.2012	
107 / 3.107	Špecifikácia požiadaviek na centrálnu tlač	-	Akceptované
108 / 3.108	Dodávka zariadenia pre obálkovanie v NPC	-	Akceptované
109 / 3.109	Dodávka zariadenia pre centrálnu tlač v NPC	-	Akceptované
110 / 3.110	Dodávka zariadenia pre obálkovanie v ZPC	-	Akceptované
111 / 3.111	Dodávka zariadenia pre centrálnu tlač v ZPC	-	Akceptované
112 / 3.112	Dodávka SW na riadenie a formátovanie centrálnej tlače	-	Akceptované
113 / 3.113	Implementácie riešenia centrálnej tlače	-	Akceptované
114 / 3.114	Akceptačné testy	-	Akceptované
115 / 3.115	Technická a používateľská dokumentácia	-	Akceptované
116 / 3.116	Podpora rutinnej prevádzky	-	Akceptované
117 / 3.117	Školenia	-	Akceptované
118 / 3.118	Rozšírená podpora nábehu rutinnej prevádzky CT	31.1.2013	

V Bratislave dňa .....28.08.2012.....

Za Zhotoviteľa

Hewlett-Packard Slovakia s.r.o.

Ing. Martin Kubala
Generálny riaditeľ a konateľ

V Bratislave dňa .....28.08.2012.....

Za Objednávateľa

Ministerstvo vnútra Slovenskej republiky

Ing. Denisa Saková, PhD.
Vedúca služobného úradu Ministerstva vnútra