

Výzva na predkladanie ponúk pre účely určenia predpokladanej hodnoty zákazky (ďalej len „Výzva“)

1. Verejný obstarávateľ:

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI)
Pribinova 25
811 09 Bratislava
IČO: 50 349 287
Kontaktná osoba: JUDr. Zuzana Rusnáková, Mgr. Melinda Vargová
E-mail: zuzana.rusnakova@mirri.gov.sk; melinda.vargova@mirri.gov.sk
Adresa hlavnej stránky verejného obstarávateľa /URL/: <https://www.mirri.gov.sk/>

2. Zatriedenie obstarávacieho subjektu podľa zákona:

Verejný obstarávateľ podľa § 7 ods. 1 písm. a) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“)

3. Názov zákazky podľa verejného obstarávateľa:

„Digitálny onboarding do aplikácie Slovensko v mobile“

4. Druh zákazky (tovary/služby/stavebné práce):

Zákazka na poskytnutie služieb.

5. Hlavné miesto dodania tovaru/poskytnutia služieb/uskutočnenia stavebných prác:

Sídlo verejného obstarávateľa – Pribinova 4195/25, 811 09 Bratislava.

6. Výsledok verejného obstarávania:

Výsledkom verejného obstarávania bude zmluva, ktorej predmetom bude dodávka softvérového diela s integrovaním biometrickej technológie overenia identity a poskytnutie služieb prevádzkovej podpory po dobu 24 mesiacov (s možnosťou opcie na ďalších 24 mesiacov).

7. Stručný opis zákazky:

Predmetom zákazky je dodávka softvérového diela s integrovaním biometrickej technológie overenia identity v rozsahu softvérových komponentov, licencií, integračnej podpory, produkčnej podpory a zabezpečenia prevádzky systému zo strany dodávateľa za účelom **vytvorenia možnosti aktivácie používateľských účtov do mobilných aplikácií (Slovensko v mobile - SvM) a iných špecializovaných portálov VS prostredníctvom služieb digitálneho onboardingu (DO)**, ktorých prínosom bude zjednodušenie, zrýchlenie a zmodernizovanie prístupu občanov k elektronickým službám štátu implementovaním možnosti overenia identity a aktivácie používateľských účtov so zvýšenou mierou garancií bez nutnosti použitia externej čítačky čipových kariet a bezpečnostného osobného kódu (BOK).

8. Spoločný slovník obstarávania:

72000000-5 – Služby informačných technológií: konzultácie, vývoj softvéru, internet a podpora
48810000-9 - Informačné systémy
72250000-2 - Služby týkajúce sa podpory systému
72263000-6 - Implementácia softvéru
72253200-5 - Systémové podporné služby

9. Celkový rozsah predmetu zákazky:

Podrobná špecifikácia predmetu zákazky je uvedená v „Prílohe č. 1 – Opis predmetu zákazky“ tejto Výzvy.

10. Predpokladaná hodnota zákazky v EUR bez DPH

Predpokladaná hodnota zákazky bude určená týmto prieskumom trhu, v súlade s ustanovením § 6 ods. 1 zákona o verejnom obstarávaní.

11. Spôsob určenia ceny a hlavné podmienky financovania a platobné dojednania:

Navrhovaná zmluvná cena musí byť stanovená podľa zákona NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky MF SR č. 87/1996 Z. z., ktorou sa vykonáva zákon Národnej rady Slovenskej republiky č. 18/1996 Z. z. o cenách v znení neskorších predpisov.

Hospodárskym subjektom navrhovaná cenová ponuka bude vyjadrená ako maximálna v EUR s presnosťou na dve desatinné miesta.

Financovanie bude prebiehať na základe doručených faktúr poskytovateľa služieb. Lehota splatnosti faktúry, ktorá bude mať náležitosti daňového a účtovného dokladu v zmysle osobitných právnych predpisov, bude **60 dní** odo dňa jej riadneho doručenia verejnému obstarávateľovi.

Verejný obstarávateľ neposkytuje preddavky ani zálohovú platbu na predmet zákazky. Platba bude realizovaná formou bezhotovostného platobného styku v eurách na základe predloženej faktúry.

12. Podmienky účasti:

Z dôvodu, že aktuálna Výzva na predkladanie ponúk sa týka určenia predpokladanej hodnoty zákazky, tak v tejto fáze hospodársky subjekt, ktorý bol oslovený so žiadosťou o predloženie cenovej ponuky, nepredkladá žiadne doklady za účelom preukázania splnenia podmienok účasti, a teda verejný obstarávateľ bude požadovať preukázať splnenie podmienok účasti až v rámci riadne vyhláseného verejného obstarávania.

Verejný obstarávateľ v rámci vyhláseného verejného obstarávania bude požadovať splnenie podmienok účasti osobného postavenia podľa § 32 a technickej alebo odbornej spôsobilosti podľa:

- A. § 34 ods. 1 písm. a) zákona o verejnom obstarávaní** – zoznamom poskytnutých služieb, prostredníctvom ktorého preukáže realizáciu služieb rovnakého alebo podobného charakteru ako je požadovaný predmet zákazky za predchádzajúce obdobie štyroch (4) rokov od vyhlásenia verejného obstarávania,
- B. § 34 ods. 1 písm. d) zákona o verejnom obstarávaní** – opisom technického vybavenia, študijných a výskumných zariadení a opatrení použitých uchádzačom alebo záujemcom na zabezpečenie kvality

Verejný obstarávateľ požaduje predložiť doklady preukazujúce splnenie tejto podmienky účasti:

1. Uchádzač predloží platný certifikát o zavedení systému manažérstva v oblasti IT služieb v zmysle požiadaviek **normy ISO/IEC 20000-1** vo vzťahu k predmetu zákazky vydaný nezávislou inštitúciou, prípadne jeho ekvivalent osvedčujúci zavedenie rovnocenných opatrení podľa požiadaviek na vydanie tohto certifikátu, pričom verejný obstarávateľ uzná ako rovnocenný certifikát vydaný príslušnými orgánmi členských štátov Európskej únie.

Odôvodnenie: Verejný obstarávateľ vyžaduje, aby uchádzač garantoval, že prostredie, v ktorom sú služby poskytované, je na základe implementácie procesov v oblasti riadenia

služieb a bezpečnosti IT, riadené a kontrolované, a teda sú vytvorené organizačné a technické predpoklady pre kvalitu poskytovaných služieb.

2. Uchádzač predloží platný certifikát kvality vývoja v zmysle požiadaviek **normy ISO/IEC 25000 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE** vydaný nezávislou inštitúciou, prípadne jeho ekvivalent osvedčujúci zavedenie rovnocenných opatrení podľa požiadaviek na vydanie tohto certifikátu, pričom verejný obstarávateľ uzná ako rovnocenný certifikát vydaný príslušnými orgánmi členských štátov Európskej únie.

Odôvodnenie: Verejný obstarávateľ vyžaduje, aby uchádzač garantoval (i) vysokú mieru bezpečného vývoja softvéru a (ii) vysokú mieru bezpečnosti vývojového prostredia, v ktorom bude prebiehať vývoj predmetného diela.

3. Uchádzač predloží minimálne jeden platný certifikát v oblasti informačnej bezpečnosti v zmysle požiadaviek normy:

- **ISO/IEC 22301** - Security and resilience - Business continuity management systems – Requirements a/alebo
- **ISO/IEC 27001** - Information security, cybersecurity and privacy protection - Information security management systems – Requirements a/alebo
- **ISO/IEC 27002** - Information security, cybersecurity and privacy protection - Information security controls a/alebo
- **ISO/IEC 27017** - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services a/alebo
- **ISO/IEC 27018** - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,

vydaný nezávislou inštitúciou, prípadne jeho ekvivalent osvedčujúci zavedenie rovnocenných opatrení podľa požiadaviek na vydanie tohto certifikátu, pričom verejný obstarávateľ uzná ako rovnocenný certifikát vydaný príslušnými orgánmi členských štátov Európskej únie.

Odôvodnenie: Verejný obstarávateľ vyžaduje, aby uchádzač garantoval (i) vysokú mieru bezpečnosti prevádzky infraštruktúry a (ii) vysokú mieru bezpečnosti prevádzky samotného diela.

- C. § 34 ods. 1 písm. g) zákona o verejnom obstarávaní** - údajmi o vzdelaní a odbornej praxi alebo o odbornej kvalifikácii osôb určených na plnenie zmluvy alebo riadiacich zamestnancov, ak nie sú kritériom na vyhodnotenie ponúk, a to vo vzťahu k nasledovným pozíciám:

Verejný obstarávateľ požaduje od uchádzača údaje o odbornej praxi alebo odbornej kvalifikácii osôb zodpovedných za poskytnutie služby formou predloženia profesijných životopisov podpísaných dotknutou osobou a predložením dokladu/dokladov, ktorý/ktoré je/sú uvedené pri jednotlivých kľúčových odborníkoch.

Uchádzač predloží za každého kľúčového odborníka profesijný životopis alebo ekvivalentný doklad podpísaný dotknutou osobou (kľúčovým odborníkom), ktorý musí poskytovať minimálne nasledovné informácie:

- meno a priezvisko príslušného kľúčového odborníka,

- história zamestnania/odbornej praxe príslušného Kľúčového odborníka (zamestnávateľ, trvanie pracovného pomeru/trvanie odbornej praxe, rok a mesiac od – do, pozícia, ktorú príslušný Kľúčový odborník zastával),
- praktické skúsenosti príslušného Kľúčového odborníka (názov projektu/zákazky, pozícia na projekte/zákazke, stručný opis projektu/predmetu zákazky; popis činnosti/pracovnej pozície Kľúčového odborníka, obdobie rok a mesiac od – do; kontaktné údaje odberateľa – názov, sídlo, emailový a telefonický kontakt, kde si bude môcť verejný obstarávateľ overiť informácie),
- certifikácie odbornej spôsobilosti súvisiace s predmetom projektu/zákazky,
- dátum a vlastnoručný podpis príslušného kľúčového odborníka.

Uchádzač predloží údaje o vzdelaní a odbornej praxi za všetkých požadovaných Kľúčových odborníkov (s výnimkou pozícií Kľúčových odborníkov „Projektový manažér“ a „Service Manager“, ktoré môžu byť preukázané aj jednou fyzickou osobou, nemôže uchádzač jednou fyzickou osobou preukázať splnenie podmienky účasti pre viacero z požadovaných pozícií a pre dotknuté pozície uchádzač predloží požadovaný počet rôznych Kľúčových odborníkov, čiže 1 Kľúčový odborník = 1 osoba), čím nie je dotknutá možnosť výmeny Kľúčového odborníka počas plnenia predmetu zákazky v zmysle Zmluvy, pričom verejný obstarávateľ predpokladá súbežný výkon činností Kľúčových odborníkov.

Kľúčový odborník, ktorý bude uvedený v ponuke uchádzača sa musí reálne podieľať na plnení predmetu Zmluvy, ktorá bude výsledkom tohto verejného obstarávania. V prípade, že Kľúčový odborník nie je zamestnancom uchádzača, musí uchádzač verejnému obstarávateľovi preukázať, že pri plnení Zmluvy bude skutočne používať odborné kapacity tejto osoby (Kľúčového odborníka), čo uchádzač preukáže zmluvou uzavretou s touto osobou, z ktorej musí vyplývať záväzok osoby, že poskytne plnenie počas celého trvania zmluvného vzťahu. V prípade, že počas plnenia Zmluvy dôjde k nahradeniu Kľúčového odborníka inou osobou, nový Kľúčový odborník musí spĺňať minimálnu požadovanú úroveň nahradeného Kľúčového odborníka vyžadovanú verejným obstarávateľom pri preukazovaní danej podmienky účasti technickej alebo odbornej spôsobilosti.

Verejný obstarávateľ požaduje predložiť doklady preukazujúce splnenie tejto podmienky účasti na nasledovných pozíciách:

Kľúčový odborník č. 1 – Projektový manažér:

- 1 osoba zodpovedná za riadenie a koordináciu IT projektu,
- minimálne 3 roky odbornej praxe v oblasti riadenia a koordinácie IT projektov,
- minimálne 2 praktické skúsenosti s riadením a koordináciou projektu rovnakého alebo obdobného charakteru ako predmet zákazky,
- platný certifikát PRINCE 2 - minimálne na úrovni Practitioner, vydaný v súlade s aktuálnymi certifikačnými požiadavkami, t. j. nie starší ako 3 roky od vydania, alebo ekvivalentný certifikát zameraný na projektové riadenie vydaný príslušnou medzinárodne uznávanou certifikačnou/akreditačnou autoritou.

Kľúčový odborník č. 2 – Service Manager:

- 1 osoba zodpovedná za riadenie prevádzky a rozvoja dodávaných služieb rovnakého alebo obdobného charakteru ako predmet zákazky,
- minimálne 3 roky odbornej praxe v oblasti riadenia prevádzky a rozvoja služieb IT projektov rovnakého alebo obdobného charakteru ako predmet zákazky,
- platný certifikát ITIL V4 - minimálne na úrovni Managing Professional (MP), vydaný v súlade s aktuálnymi certifikačnými požiadavkami, t. j. nie starší ako 3 roky od vydania, alebo

ekvivalentný certifikát zameraný na riadenie prevádzky a rozvoj IT služieb, vydaný príslušnou medzinárodne uznávanou certifikačnou/akreditačnou autoritou.

Kľúčový odborník č. 3 – Bezpečnostný architekt v oblasti IKT:

- 1 osoba zodpovedná za návrh celkovej architektúry riešenia,
- minimálne 3 roky odbornej praxe v oblasti architektúry IKT zameranej na minimálne jednu z oblastí: šifrovanie a/alebo autentifikáciu a/alebo autorizáciu,
- minimálne 1 praktická skúsenosť s implementáciou digitálneho onboardingu,
- minimálne 1 praktická skúsenosť s implementáciou HSM¹,
- platný certifikát CISSP – ISSAP a/alebo CISSP - ISSEP a/alebo ekvivalentný certifikát zameraný na bezpečnostnú architektúru v IKT vydaný príslušnou medzinárodne uznávanou certifikačnou/akreditačnou autoritou.

Kľúčový odborník č. 4 – Senior Developer:

- 1 osoba zodpovedná za oblasť back-end,
- minimálne 3 roky odbornej praxe v oblasti zameranej na prácu s biometrickými údajmi štandardizovaných formátov,
- minimálne 2 praktické skúsenosti s bezpečnostnými protokolmi TLS, OAuth 2.0, OpenID Connect, SAML a W3C WebAuthn²,
- platný certifikát CSSLP a/alebo S-CSSD a/alebo ekvivalentný certifikát zameraný na vývoj v IT oblasti (oblasť bezpečnosti) vydaný príslušnou medzinárodne uznávanou certifikačnou/akreditačnou autoritou.

Kľúčový odborník č. 5 – Senior Developer:

- 1 osoba zodpovedná za oblasť front-end,
- minimálne 3 roky odbornej praxe v oblasti zameranej na prácu s biometrickými údajmi štandardizovaných formátov,
- minimálne 2 praktické skúsenosti s bezpečnostnými protokolmi TLS, OAuth 2.0, OpenID Connect, SAML a W3C WebAuthn³,
- platný certifikát CSSLP a/alebo S-CSSD a/alebo ekvivalentný certifikát zameraný na vývoj v IT oblasti (oblasť bezpečnosti) vydaný príslušnou medzinárodne uznávanou certifikačnou/akreditačnou autoritou.

Kľúčový odborník č. 6 – Test Manager:

- 1 osoba zodpovedná za vypracovanie stratégie testovania a riadenie jeho vykonávania,
- minimálne 3 roky odbornej praxe v oblasti riadenia a koordinácie testovania diela na projekte rovnakého alebo obdobného charakteru ako predmet zákazky,
- minimálne 2 praktické skúsenosti s riadením a koordináciou testovania funkčnosti diela na projekte rovnakého alebo obdobného charakteru ako predmet zákazky,

¹ Verejný obstarávateľ uvádza, že vo vzťahu k požiadavkám v znení „*minimálne 1 praktická skúsenosť s implementáciou digitálneho onboardingu*“ a „*minimálne 1 praktická skúsenosť s implementáciou HSM*“ je prípustné preukazovať splnenie predmetných požiadaviek aj identickou praktickou skúsenosťou.

² V súvislosti s požiadavkou vo vzťahu ku „Kľúčovému odborníkovi č. 4 – Senior Developer“ (oblasť back-end) týkajúcou sa praktickej skúsenosti, a to konkrétne požiadavky na minimálne 2 praktické skúsenosti s bezpečnostnými protokolmi TLS, OAuth 2.0, OpenID Connect, SAML a W3C WebAuthn, je postačujúce predloženie minimálne 2 praktických skúsenosti, ktoré budú kumulatívne preukazovať skúsenosti daného kľúčového odborníka so všetkými požadovanými bezpečnostnými protokolmi.

³ V súvislosti s požiadavkou vo vzťahu ku „Kľúčovému odborníkovi č. 5 – Senior Developer“ (oblasť front-end) týkajúcou sa praktickej skúsenosti, a to konkrétne požiadavky na minimálne 2 praktické skúsenosti s bezpečnostnými protokolmi TLS, OAuth 2.0, OpenID Connect, SAML a W3C WebAuthn, je postačujúce predloženie minimálne 2 praktických skúsenosti, ktoré budú kumulatívne preukazovať skúsenosti daného kľúčového odborníka so všetkými požadovanými bezpečnostnými protokolmi.

- platný certifikát ISTQB Certified Tester Advanced Level a/alebo ekvivalentný certifikát zameraný na oblasť manažmentu testovania vydaný príslušnou medzinárodne uznávanou certifikačnou/akreditačnou autoritou.

13. Lehota na predkladanie aktualizovaných ponúk uplynie dňa:

22. 08. 2025 o 13:00 hod.

14. Miesto na predloženie ponúk:

Cenovú ponuku je potrebné doručiť výlučne elektronicky, do uplynutia lehoty na predkladanie ponúk pre účely určenia PHZ, a to na emailovú adresu: zuzana.rusnakova@mirri.gov.sk a patrik.simo@mirri.gov.sk.

15. Ponuka musí obsahovať:

1. Doplnenú „Prílohu č. 2 – Cenová ponuka a rozpočet“ Výzvy v „.xlsx“ formáte,
2. Doplnenú a podpísanú „Prílohu č. 2 – Cenová ponuka a rozpočet“ Výzvy v „.pdf“ formáte

16. Jazyk, v ktorom možno predložiť ponuky:

Ponuky, návrhy a ďalšie doklady a dokumenty vo verejnom obstarávaní sa predkladajú v štátnom jazyku a môžu sa predkladať aj v českom jazyku. Ak je doklad alebo dokument vyhotovený v inom ako štátnom jazyku alebo českom jazyku, predkladá sa spolu s jeho úradným prekladom do štátneho jazyka. Ak sa zistí rozdiel v obsahu dokladu alebo dokumentu predloženom podľa druhej vety, rozhodujúci je úradný preklad do štátneho jazyka.

17. Zákazka sa týka projektu / programu financovaného z fondov EÚ:

Zákazka bude financovaná z Plánu obnovy a odolnosti SR a štátneho rozpočtu SR.

18. Dátum zaslania výzvy na predkladanie ponúk pre účely určenia PHZ:

15. 08. 2025

Prílohy:

Príloha č. 1 – Opis predmetu zákazky

Príloha č. 2 – Cenová ponuka a rozpočet

Príloha č. 3 – Katalóg požiadaviek



Príloha č. 1 - Opis predmetu zákazky

Názov zákazky: Digitálny onboarding do aplikácie Slovensko v mobile

Základný opis predmetu zákazky

1. Skratky

Skratka	Popis
DO	Digitálny onboarding
RPO	Recovery point objectives; Bod obnovy systému zo zálohy
RTO	Recovery time objective; za aký čas je možné obnoviť systém po výpadku
DKVI	Doba konečného vyriešenia incidentu
IS	Informačný systém
SvM	Slovensko v mobile
MV SR	Ministerstvo vnútra Slovenskej republiky
SLA	Prevádzková podpora systému
eID	Elektronický občiansky preukaz
OP	Občiansky preukaz

2. Predmet zákazky

Predmetom zákazky je dodávka softvérového diela s integrovaním biometrickej technológie overenia identity v rozsahu softvérových komponentov, licencií, integračnej podpory, produkčnej podpory a zabezpečenia prevádzky systému zo strany dodávateľa za účelom **vytvorenia možnosti aktivácie používateľských účtov do mobilných aplikácií (Slovensko v mobile - SvM) a iných špecializovaných portálov VS prostredníctvom služieb digitálneho onboardingu (DO)**, ktorých prínosom bude zjednodušenie, zrýchlenie a zmodernizovanie prístupu občanov k elektronickým službám štátu implementovaním možnosti overenia identity a aktivácie používateľských účtov so zvýšenou mierou garancií bez nutnosti použitia externej čítačky čipových kariet a bezpečnostného osobného kódu (BOK).

Digitálny onboarding (DO) zahŕňa technológie a postupy pre registráciu účtu používateľa využitím technológií na overenie identity bez nutnosti jeho fyzickej prítomnosti na úrade určenom na registráciu a so zachovaním požadovanej miery garancií overenia identity osoby. Tento spôsob aktivácie aplikácie musí byť v súlade s požiadavkami vykonávacieho nariadenia Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úroveň zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (eIDAS) v konsolidovanom znení a nariadenia Európskeho parlamentu a Rady (EÚ) č. 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity, a to pre úroveň identifikácie a autentifikácie aspoň „pokročilá“. Digitálny onboarding tak rozšíri súčasné možnosti aktivácie používateľský účtov v mobilných aplikáciách a špecializovaných portáloch.

Digitálny onboarding bude určený **pre občanov SR** s dokladom vydaným po 01. 07. 2008¹ a to primárne pre občanov s OP s čipom bez znalosti BOK (sekundárne pre občanov s OP bez čipu). Ďalším nevyhnutným predpokladom aktivácie používateľského účtu prostredníctvom digitálneho onboardingu bude okrem uvedených dokladov aj smartfón s podporovaným operačným systémom (Android alebo iOS) alebo počítačom s webovým prehliadačom v podporovanej verzii, s pripojením na internet a vybavený kamerou. Verejný obstarávateľ predpokladá, že počet nových jedinečných používateľov digitálneho onboardingu na najbližších 12 mesiacov (od začiatku nasadenie tejto funkcionality do prevádzky) bude 100 000 občanov. Odhadovaný maximálny počet predpokladaných aktivácií v špičkách je cca 2000 denne.

¹ <https://www.minv.sk/?vzory-dokladov-obcianske-preukazy>



3. Rozsah zákazky

Z hľadiska povahy predmetu zákazky verejný obstarávateľ plánuje predmet zákazky obstarat' nasledovne:

- Dodávka technológie digitálneho onboardingu (dostupné vo forme dodávky softvérových komponentov). Digitálny onboarding umožní overenie identity použitím dokladu totožnosti (s čipom alebo aj bez čipu) a biometrických znakov osoby.
- Zabezpečenie licencií pre technológiu digitálneho onboardingu na najbližších 12 mesiacov pre 100 000 aktívnych overených užívateľov
- Implementácia podporných integračných služieb digitálneho onboardingu pre umožnenie integrácie viacerým klientskym aplikáciám a integráciou na IS MV SR pre overenie identity občana predložením dát z dokladu totožnosti.
- Integračná podpora a produkčná podpora (uvedená nižšie).
- Zabezpečenie prevádzky.

Cieľom verejného obstarania bude dodanie softvérového diela s integrovaním biometrickej technológie overenia identity (popísaných v nasledujúcich odstavcoch) v rozsahu potrebných softvérových komponentov, licencií, integračnej podpory, produkčnej podpory a zabezpečenia prevádzky systému.

Implementácia integračných služieb a integrácie IS MV SR bude zahŕňať implementácie integračných služieb digitálneho onboardingu, ktoré umožnia spravovať integrácie klientskych aplikácií a webových portálov na poskytované služby so samostatným riadením politik pre vyhodnocovanie vstupov ako aj integráciu na IS MV SR pre vyhodnocovanie súladu predkladaných údajov z dokladov totožnosti o identitách s registrami MV SR. Vyhodnocovanie súladu a zhodnotenie politik pre vyhodnocovanie vstupov má umožniť zapojenie kontrol aj dodatočných IS.

Integračná podpora bude zahŕňať konzultácie poskytované integrátorovi počas procesu integrácie softvérového vývojového kit-u (Software development kit; SDK) obstarávaného od dodávateľa do mobilných aplikácií a špecializovaných portálov VS. Integračná podpora bude prebiehať formou konzultačných stretnutí, na ktorých budú prerokúvané problémy, s ktorými sa integrátor stretne v procese integrácie. Dodávateľ poskytne súčinnosť v zmysle dohodnutej SLA.

Zároveň verejný obstarávateľ uvádza, že predmetom tohto verejného obstarávania nie je integrácia technológie digitálneho onboardingu do existujúcej aplikácie verejného obstarávateľa.

4. Požadované riešenie

Požiadavky verejného obstarávateľa na funkcionality digitálneho onboardingu:

Vizuálne komponenty technológie bude možné upraviť v súlade s aktuálne platnými dizajn manuálmi, predovšetkým v súlade s Jednotným dizajn manuálom elektronických služieb a webových sídiel ID-SK Frontend (<https://idsk.gov.sk/>). Zároveň verejný obstarávateľ vyžaduje riešenie, ktoré bude možné dizajnovo personalizovať pre potreby konkrétnych špecializovaných portálov.

Proces samoobslužnej aktivácie aplikácie, ktorého súčasťou je vytvorenie a registrácia používateľského účtu, využitím služieb digitálneho onboardingu dôjde k overeniu identity vyhodnotením biometrických údajov a údajov z predložených dokladov totožnosti (občiansky preukaz) poskytnutých v procese v nasledovných krokoch:

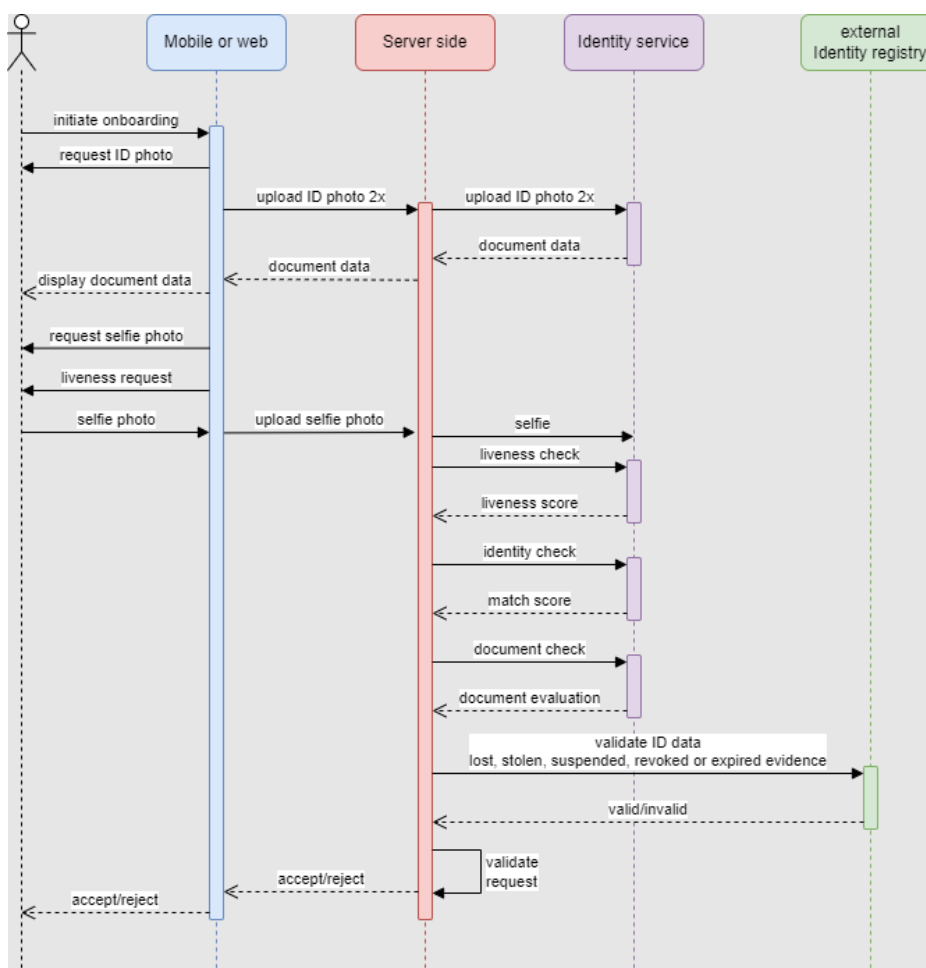
1.	Občan po otvorení aplikácie vyberie spôsob aktivácie, ktorý umožní aktivovať aplikáciu pomocou tvárovej biometrie	Ak smartfón občana disponuje funkcionalitou NFC, priloží OP (eID) k smartfónu, ktorý z čipu OP vytiahne textové údaje a fotografiu do aplikácie (túto funkcionalitu zabezpečí softvérové riešenie poskytovateľa technológie digitálneho onboardingu s využitím integrovanej funkcionality SDK pre digitálny onboarding) Ak klient nedisponuje funkcionalitou NFC alebo má OP bez NFC rozhrania, nasníma pomocou kamery prednú a zadnú stranu svojho OP, pričom služba z fotografie OP vyčíta textové údaje do aplikácie
2.	Občan je vyzvaný, aby si pomocou kamery vytvoril fotografiu vlastnej tváre (selfie).	
3.	Získané textové údaje nasnímané z OP občana pošle aplikácia na overenie voči registrom Ministerstva vnútra	Požiadavka na funkcionality SDK pre sprístupnenie údajov načítaných z OP pre ďalšie spracovanie.



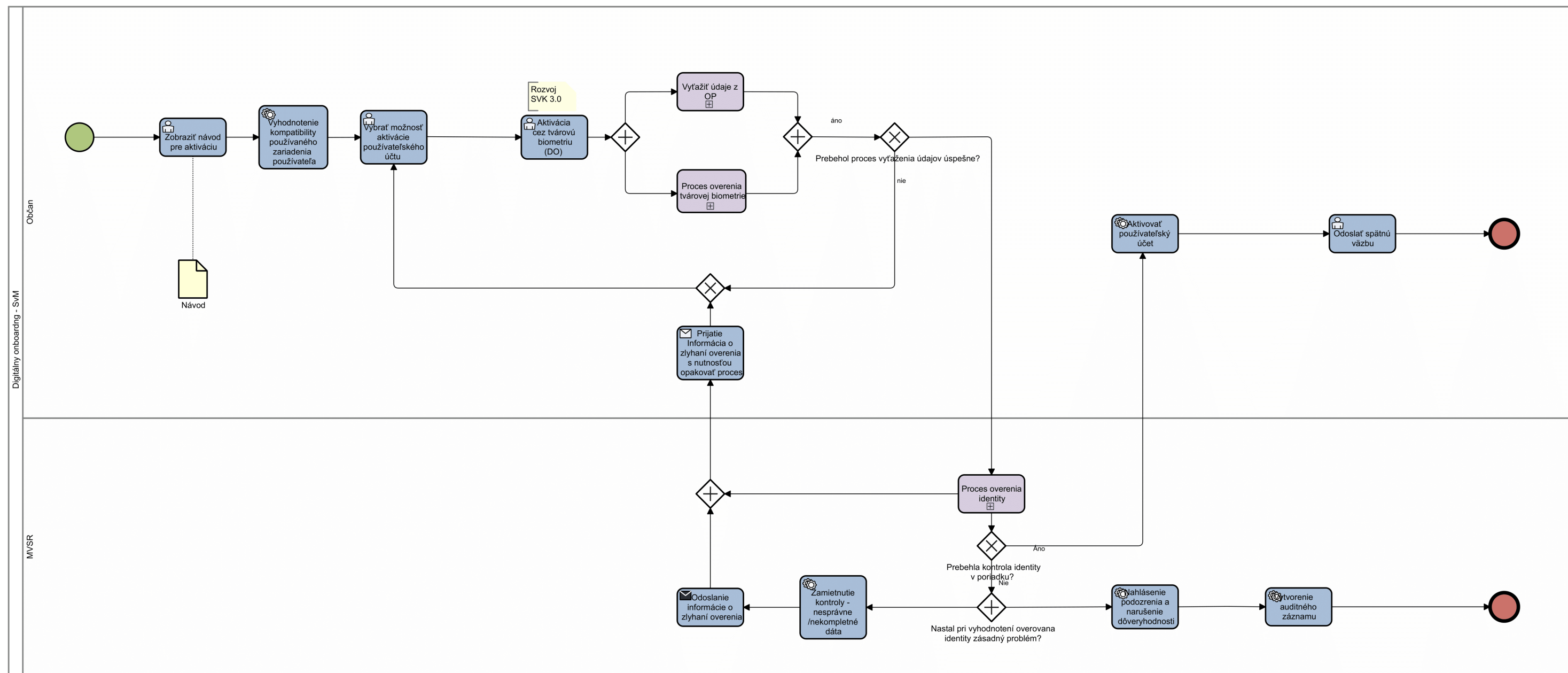
	Slovenskej republiky (MV SR). V prípade eID (teda občianskeho preukazu bez NFC), dôjde aj k overeniu fotografie voči registrom MV SR. V prípade eID 2.0 (teda občianskeho preukazu s NFC) overenie voči registrom MV SR nie je potrebné, keďže fotografia bude načítaná priamo z údajov uložených na príslušnom eID 2.0.	
4.	Služba porovná fotografiu z OP so selfie fotografiou a vyhodnotí, či sa jedná o rovnakú osobu. Zároveň v procese vyhodnotí, či selfie fotografia občana nie je podvrhnutým obrazom (kontrola živosti).	V tejto fáze prebehne kontrola dokladu totožnosti na jeho dodatočné zneplatnenie nahlásením straty, zničenia alebo krádeže, prípadne smrťou alebo stratou občianstva, či inou situáciou. Bude vykonaná kontrola súladu údajov z predloženého dokladu totožnosti s registrami MV SR. Kontrola platnosti dokladu je kľúčovou položkou v procese vyhodnocovania predkladanej identity, ktorá prináša garancie požadované vykonávacím nariadením Komisie (EÚ) 2015/1502 z 8. septembra 2015 . Integrácia na registre MV SR je predmetom implementácie softvérového diela.
5.	pozitívny výsledok overenia negatívny výsledok overenia (niektorý z krokov bude neúspešný)	zriadenie prístupu do aplikácie/specializovaného portálu zobrazenie dôvodu , z akého nebola aktivácia úspešná a tiež tipy, že občan môže proces zopakovať resp. sa mu zobrazí odporúčanie, že môže využiť iný spôsob aktivácie aplikácie alebo poslanie spätnej väzby.

Vyššie uvedené jednotlivé kroky môžu byť v konečnom riešení usporiadané v inom poradí, resp. niektoré z nich prebiehajú súčasne.

Verejný obstarávateľ informatívne z dôvodu prehľadnosti uvádza predbežný uvažovaný návrh sekvenčného diagramu a procesného toku, ktoré sú uvedené v nasledujúcich diagramoch, pričom uvádza, že integrácia na registre MV SR je predmetom implementácie softvérového diela formou štandardných SOAP API rozhraní s mTLS autorizáciou:

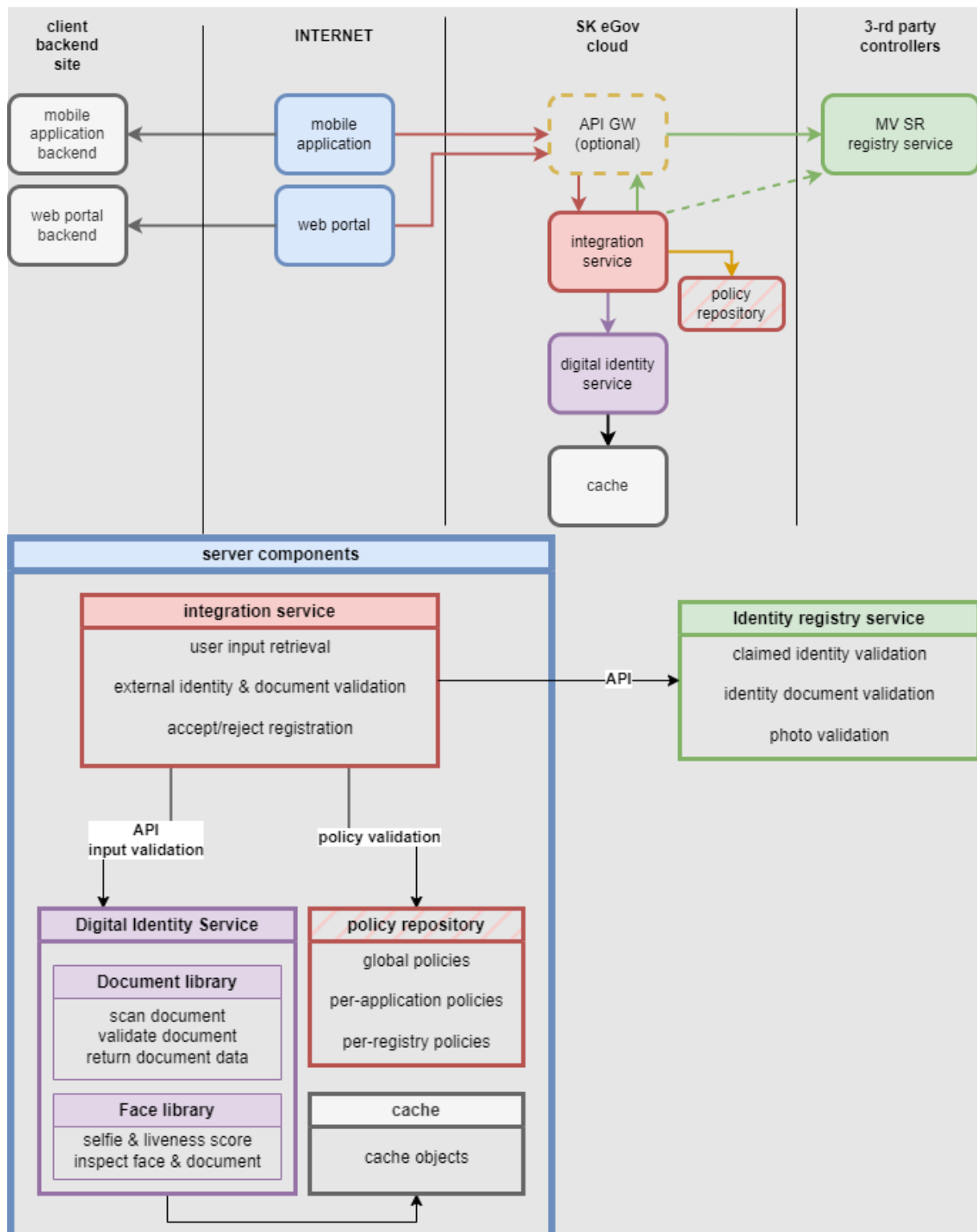


Obrázok 1 Sekvenčný diagram DO



Obrázok 2 Procesný diagram DO

Predpokladaná architektúra modulov digitálneho onboardingu



Na strane klientskej aplikácie je technológia digitálneho onboardingu integrovaná cez softvérový komponent SDK, ktorý je súčasťou dodávky technológie DO. SDK sprostredkuje klientskej aplikácii volania integračnej služby, ktorá zabezpečuje vyhodnocovanie predložených fotografií a dát z klientskej aplikácie v procese digitálneho onboardingu. Táto služba predkladané dáta posielajú na vyhodnotenie na službu digitálnej identity a treťostranné validácie vstupov a následne vyhodnotí



návratové hodnoty s definíciami politík na parametre akceptácie vstupov z repozitára politík. Po vyhodnotení všetkých požadovaných podmienok politík pre integrovanú klientsku aplikáciu je výsledok predložený klientskej aplikácii.

SDK klientskych platforiem musia podporovať

- priamu integráciu natívneho kódu oboch platforiem Apple iOS a Google Android
- integráciu webových portálov s vysokými garanciami integrity vykonávaného kódu (ideálne technológiou WebAssembly alebo alternatívou s dostatočnými garanciami)

Technológia musí podporovať flexibilitu toku procesu digitálneho onboardingu a obrazoviek UX rozhrania pri integrácii do mobilnej aplikácie, resp. webového portálu. Čas prechodu celým procesom onboardingu nepresiahne 3 min.

Verejný obstarávateľ požaduje od dodávanej technológie ďalej nasledovné vlastnosti/funkcionality:

Dodávaná technológia musí umožniť získavanie prehľadu o počte úspešných a neúspešných aktivácií aplikácie potrebných pre vyhodnotenie kvality služieb DO. O dôvode neúspešnosti procesu aktivácie bude občan v procese aktivácie informovaný, zároveň bude inštruovaný vykonať aktiváciu opakovane s cieľom úspešne aktivovať aplikáciu, prípadne s využitím ostatných foriem aktivácie.

Požiadavky na kvalitu a bezpečnosť

Verejný obstarávateľ vyžaduje, aby biometrické technológie a možnosti ich zapojenia do procesu aktivácie používateľských účtov napĺňali požiadavky definované nasledovnými normami:

- ISO/IEC 39794 „Extensible biometric data interchange formats“, ktorá definuje rozšírenia formátov ISO/IEC 19794 v súlade s ASN.1 normatívou
- ISO/IEC 29794 „Biometric sample quality“, ktorá definuje rámec hodnotenia kvality vzoriek biometrických údajov
- ISO/IEC 19794 „Biometric data interchange formats“, ktorá definuje formáty pre výmenu biometrických dát
- ISO/IEC 19785 „Common Biometric Exchange Formats Framework“, ktorá definuje štandardy formátov pre výmenu biometrických údajov

Kvalita technológie vyhodnocovania biometrie tváre musí byť preukázaná testom v certifikovanom testovacom laboratóriu s hodnotami „False Non-Match Rate“ menšou ako 0,0040 (podľa NIST FRTE 1:1 Verification)².

Kvalita technológie vyhodnocovania biometrie tváre musí napĺňať garancie „ISO/IEC 30107-3 Information technology — Biometric presentation attack detection, Part 3: Testing and reporting“ úrovne 2, čo verejný obstarávateľ vyžaduje preukázať skúšobným protokolom alebo certifikátom vydaným akreditovaným orgánom posudzovania zhody.

Vzhľadom na spracúvanie osobných údajov musí technológia digitálneho onboardingu umožňovať adekvátnu ochranu týchto dát v súlade s legislatívnymi predpismi platnými v Slovenskej republike:

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

V prípade použitia technológií šifrovania musí technológia digitálneho onboardingu umožniť konfiguráciu šifrovacieho modulu s možnosťou konfigurácie použitých šifrovacích algoritmov a jeho rozhrania, ktoré musia byť implementované v súlade s štandardmi PKCS (Public Key Cryptography Standards), prípadne umožniť integráciu s externým HSM (Hardware Security Module) modulom spôsobom, ktorý flexibilne umožní navýšenie garancií šifrovania zmenou konfiguračných parametrov.

5. Technologická architektúra a požiadavky na cloudové služby

Riešenie bude umiestnené a prevádzkované vo vládnom cloude v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Verejný obstarávateľ (MIRRI) poskytne úspešnému uchádzačovi cloudové prostredie vo verejnej časti vládneho cloudu, ktoré je súčasťou prostredia eSKa Cloudu. Toto prostredie je zabezpečované prostredníctvom cloudových prostredí Microsoft Azure a Oracle OCI zapísaných v katalógu vládnych cloudových služieb. Víťazný uchádzač navrhne technologickú architektúru

² Požiadavku na kvalitu technológie vyhodnocovania biometrie tváre, ktorú verejný obstarávateľ požaduje preukázať testom v certifikovanom testovacom laboratóriu s hodnotami „False Non-Match Rate“ menšou ako 0,0040 (podľa NIST FRTE 1:1 Verification) je postačujúce preukázať zápisom ponúkanej technológie v zozname vedenom „National Institute of Standards and Technology“ (NIST) na nasledujúcej webovej adrese: <https://pages.nist.gov/frvt/html/frvt11.html>, v súvislosti s čím uchádzač uvedie údaje v rozsahu podľa „Prílohy č. 5 – Návrh na plnenie kritérií na vyhodnotenie ponúk“ „Súťažných podkladov na predmet zákazky: Digitálny onboarding do aplikácie Slovensko v mobile“.



využitím cloudových služieb podľa vlastnej technologickej preferencie v prostredí eSKA Cloud. Žiadosť o poskytnutie cloudových služieb a súvisiace informácie a dokumenty sú dostupné na adrese: <https://mirri.gov.sk/sekcie/ziadost-pre-poskytnutie-cloudovych-sluzieb/>. Prípadné ďalšie informácie je možné nájsť vo forme zodpovedaných najčastejších otázok dostupných na adrese: <https://mirri.gov.sk/sekcie/informatizacia/dokumenty/vladny-cloud/faq/>.

Verejný obstarávateľ poskytne infraštruktúru využitím služieb vládneho cloudu na úrovni IaaS a/alebo PaaS a/alebo SaaS. Verejný obstarávateľ požaduje poskytovať služby s úrovňou zabezpečenia U3.

Verejný obstarávateľ (MIRRI) požaduje, aby uchádzač v rámci ponuky predložil dokument, v ktorom špecifikuje požadované služby v eSKA cloude³ (link: [Katalóg cloudových služieb | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR](#)), ktoré použije na vývoj Diela a následnú prevádzku.

6. Požiadavky na prevádzkovú podporu systému (SLA)

Predmet SLA

Predmetom SLA je zabezpečenie podpory prevádzky technológie digitálneho onboardingu (DO).

Týka sa všetkých backendových komponentov a integrácií na externé systémy. V súčasnosti bude vyžadovaná integrácia na služby overenia identity MV SR. Do budúcnosti predpokladáme integráciu aj na iné externé služby.

SLA sa netýka frontendovej integrácie do klientských aplikácií a portálov, kde je využitá technológia DO.

Úrovně podpory prevádzky systému

Verejný obstarávateľ požaduje, aby poskytovateľ služby realizoval Help Desk nasledovnej úrovne podpory, s nasledujúcim označením:

- **L1 podpora:** (Level 1) – Jednotný priamy kontakt pre používateľov nového riešenia. Zabezpečené zamestnancami objednávateľa (verejného obstarávateľa) a/alebo ním určenými osobami.
- **L2 podpora:** (Level 2) – Postúpenie požiadaviek od L1 podpory. Zabezpečené Poskytovateľom služby na základe zmluvy.
- **L3 podpora:** (Level 3) – Postúpenie požiadaviek od L2, prípadne L1 podpory. Zabezpečené Poskytovateľom služby na základe zmluvy.

Pre prevádzkovú podporu sú definované takéto SLA:

- Dostupnosť L1 podpory pre IS je 8x5 (8 hodín x 5 pracovných dní v týždni od 8:00 h do 16:00 h, dostupnosť nie je vyžadovaná počas dní pracovného pokoja).
- Dostupnosť L2 a L3 podpory pre IS je 8x5 (8 hodín x 5 pracovných dní v týždni od 8:00 h do 16:00 h, dostupnosť nie je vyžadovaná počas dní pracovného pokoja).

Zabezpečenie bezpečnostného monitoringu:

- Vykonáva prevádzkovateľ DO
- Zabezpečuje monitoring 24x7 (sledovanie stavu, vykonanie ad-hoc bezpečnostných opatrení)

Riešenie incidentov – SLA parametre

Za incident je považované neplánované narušenie služby, alebo zníženie jej kvality. **Označenie naliehavosti incidentu:**

Označenie incidentu	Naliehavosť incidentu	Popis naliehavosti incidentu
A	Kritická	Incidenty, ktoré majú veľký dopad na biznis a vyžadujú okamžitú pozornosť, pretože spôsobujú úplné výpadky alebo významne obmedzujú hlavné biznisové procesy.

³ Vzor dokumentu, v ktorom uchádzač špecifikuje požadované služby v eSKA cloude je „Prílohou č. 11 – Cloud služby“ „Súťažných podkladov na predmet zákazky: Digitálny onboarding do aplikácie Slovensko v mobile“



B	Vysoká	Incidenty s významným dopadom na biznis, ale s menej závažným dopadom ako kritické incidenty. Vyžadujú rýchle riešenie, ale nie sú okamžitou hrozbou.
C	Stredná	Incidenty, ktoré ovplyvňujú určitú časť biznisu, ale majú menej závažný dopad a nevyžadujú okamžitú reakciu.
D	Nízka	Incidenty s malým alebo žiadnym dopadom na biznis. Sú menej urgentné a môžu byť riešené v bežnom pracovnom čase.

- možný dopad:

Označenie závažnosti incidentu	Dopad	Popis dopadu
1	katastrofický	katastrofický dopad, priamy finančný dopad alebo strata dát,
2	značný	značný dopad alebo strata dát
3	malý	malý dopad alebo strata dát

- výpočet priority incidentu je kombináciou dopadu a naliehavosti v súlade s best practices ITIL V4 uvedený v nasledovnej matici:

Matica priority incidentov		Dopad		
		Katastrofický - 1	Značný - 2	Malý - 3
Naliehavosť	Kritická - A	1	2	3
	Vysoká - B	2	3	3
	Stredná - C	2	3	3
	Nízka - D	3	3	4

- vyžadované reakčné doby:

Označenie priority incidentu	Reakčná doba ⁽¹⁾ od nahlásenia incidentu po začiatok riešenia incidentu	Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) ⁽²⁾
1	Do 15 min.	Do 4 hodín
2	Do 30 min.	Do 8 hodín
3	Do 4 hodín	Do 2 dní
4	Do 8 hodín	Do 5 dní

- Za vyriešenie incidentu sa považuje aj nasadenie dočasného náhradného riešenia umožňujúceho pokračovať v prevádzke.

(1) Reakčná doba je čas medzi nahlásením incidentu a jeho prevzatím na riešenie v dohodnutom čase dostupnosti.



(2) Doba konečného vyriešenia incidentu (DKVI) je čas medzi nahlásením incidentu a jeho vyriešením poskytovateľom služby do doby, kedy je dostupnosť služby obnovená v plnom rozsahu. Doba konečného vyriešenia incidentu od jeho nahlásenia sa počíta počas celého dňa. Do tejto doby sa nezaráta čas potrebný na nevyhnutnú súčinnosť Objednávateľa alebo tretích strán, ak je potrebná pre vyriešenie incidentu.

Incidenty nahlásené Objednávateľom (verejným obstarávateľom) Poskytovateľovi služby v rámci testovacieho prostredia:

- Majú prioritu 3 a nižšiu.
- Vzťahujú sa výhradne k dostupnosti testovacieho prostredia.
- Za incident na testovacom prostredí sa nepovažuje incident vzťahujúci sa k práve testovanej funkcionalite.

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

- Služby systémovej podpory na požiadanie (nad paušál).
- Služby realizácie zmenových požiadaviek (nad paušál).

Výkonnosť a dostupnosť služieb

Popis	Parameter	Poznámka
Prevádzkové hodiny	24 hodín	24 hodín x 7 dní od 00:00 h do 24:00 h vrátane sviatkov
Servisné okno	8 hodín	- Plánovaný výpadok je oznámený minimálne 15 pracovných dní vopred. - Plánovaný výpadok nie je dlhší ako 8 hodín a je medzi 22:00 h – 06:00 h
Dostupnosť produkčného prostredia IS	95%	95 %, t. j. max. výpadok je 1,24 hodiny (1 hodina 12 minút) denne 8,8 hodín (8 hodín 24 minút) týždenne 1 deň, 12 hodín 13 minút mesačne 18 dní 2 hodiny 41 minút ročne - Nedostupnosť IS sa počíta počas prevádzkových hodín od momentu zaevidovania udalosti, ktorá ju spôsobila (zaevidovanie formou incidentu monitorovacím nástrojom, auditným záznamom alebo inou formou preukazujúcou zdroj, typ a čas udalosti). Do nedostupnosti IS sa nezarátavajú plánované výpadky IS.
RPO	Od 8 do 24 hodín	Poskytovateľ služby vie zabezpečiť riešenia tak, aby boli minimalizované straty dát v rámci zálohovania a obnovy dát
RTO	Do 1 hodiny	Poskytovateľ služby vie zabezpečiť riešenia tak, aby bola minimalizovaná doba výpadku.
Zálohovanie	V súlade s RPO a RTO	Záloha dát bude vykonávaná pravidelne, garantovaná zálohovacou stratégiou, ktorá bude zohľadňovať RPO a RTO
Odozva služieb	n/a	50% z všetkých volaní má odozvu kratšiu alebo rovnú 0,2 sekundy, 90% z všetkých volaní má odozvu kratšiu alebo rovnú 0,5 sekundy, 95% z všetkých volaní má odozvu najviac 0,7 sekundy, 99% z volaní má odozvu najviac 1 sekundu - Odozva synchrónneho volania integrovaných externých služieb sa nezaráta do odozvy služby DO

Služby riadenia systémovej a aplikačnej podpory (paušál)

Servisné služby vzťahujúce sa na produkčné aj testovacie prostredie systému, ktoré je prevádzkované v infraštruktúre vládneho cloudu, medzi ktoré patria: činnosti správy a údržby systémového softvéru a systému vrátane kontroly príslušných operačných systémov, kontroly logov, naplnenosti diskového priestoru, operačnej pamäte, správy komunikačnej matice pre jednotlivé služby produktov, sledovania informácií výrobcov a dodávateľov zariadení, príslušných bezpečnostných riešení, patchov a nutných aktualizácií, správa služieb infraštruktúry, monitorovanie vyťaženia systému, monitorovanie sieťovej komunikácie, monitorovanie naplnenosti databáz, správa certifikátov interných/externých, pridelovanie systémových

prostriedkov, vytváranie záloh, nasadzovanie nových verzií, riešenie úloh, vykonávanie preventívnej údržby, udržiavanie systému v súlade s bezpečnostnou dokumentáciou, súčinnosť a odstraňovanie zistení z bezpečnostného auditu.

Servisné služby budú realizované so zámerom:

- Uvedenie systému do plne funkčného stavu alebo poskytnutie náhradného riešenia (po poruchách, chybách) podľa definovaných parametrov pre produkčné prostredie pre nové riešenie DO.
- Podpora systémového softvéru a aplikačného softvéru v produkčnom aj testovacom prostredí (vrátane riešenia vzniknutých problémov).
- Nasadzovanie nových verzií aplikačného programového vybavenia do testovacieho a produkčného prostredia.
- Lokalizácia potenciálnych problémov pri používaní prostredia.
- Optimalizácia prevádzky na základe odsúhlasených návrhov riešení.
- Aktualizácia prevádzkovej, používateľskej a bezpečnostnej dokumentácie vyplývajúcej z aktuálneho nastavenia systému.
- Poskytovanie podpory pri integrácii DO s inými systémami a aplikáciami používanými Objednávateľom.

Činnosti správy a údržby systémového softvéru a aplikačného softvéru vykonávané priebežne

Priebežná správa a údržba DO

Tieto činnosti sa vykonávajú v pravidelných intervaloch s cieľom preventívne identifikovať možné problémy. Ide zväčša o monitorovanie a kontrolovanie definovaných parametrov na základe vopred definovaného profylaktického plánu. Výsledky kontrol budú evidované v reporte s návrhom preventívnych akcií na elimináciu neštandardných stavov systému. Priebežná správa a údržba DO ďalej zahŕňa pravidelné činnosti v oblastiach:

- **Administrácia a manažment**
- **Zálohovanie a obnova**
- **Monitoring prevádzky**
- **Monitoring bezpečnosti**

Monitoring prevádzky služieb, komponentov a infraštruktúry je implementovaný v súlade so stratégiou monitoringu, v rozsahu a spôsobom, ktorý

- zabezpečí podklady pre adresovanie možných výpadkov alebo zníženia kvality služieb
- poskytne podporné informácie pre dodatočnú analýzu a hľadanie príčin výpadkov alebo zníženia kvality služieb,
- zabezpečí bezodkladné automatizované informovanie tímov technickej podpory o výpadkoch alebo zníženiach kvality služieb.

Monitoring bezpečnosti je implementovaný v súlade s bezpečnostným projektom, v rozsahu a spôsobom, ktorý umožní priebežné vyhodnocovanie udalostí s možným dopadom na bezpečnosť.

Evidencia a reportovanie

- **Spracovávanie požadovaných reportov a operatívnych informácií:** O stave prevádzky, poskytovaní služieb, výsledkoch monitoringu, kontrol a auditov v súlade s [Požiadavkami na kvalitu a bezpečnosť](#) uvedené v kapitole 4. tohto dokumentu.
- **Vedenie technických a prevádzkových evidencií:** Vráťane technickej dokumentácie, nastavení parametrov, evidencie technických prostriedkov, používateľských príručiek, evidencie dodávateľov a kontaktných osôb.
- **Poskytovanie štatistických informácií:** Pre Objednávateľa a ním určené osoby.

Zabezpečovanie kvality služieb

Predkladanie návrhov opatrení na zlepšenie kvality služieb prevádzky a implementáciu schválených opatrení:

- **Plánovanie a riadenie preventívnej údržby**
- **Riadenie preventívnej údržby a opráv:** Vráťane prevádzkových a bezpečnostných auditov.
- **Riadenie vnútorných procesov:** A spolupráce s ostatnými zložkami.



Požiadavky služby systémovej podpory na požiadanie (nad paušál)

Prevádzkové činnosti, ktoré budú poskytované nad rámec služieb v rámci systémovej a aplikačnej podpory (SLA):

- Riešenie systémových a prevádzkových chýb súvisiacich s potrebou funkčnej úpravy nastavených procesov;
- Školenia garantov a používateľov;
- Poskytovanie služieb odborných a technických konzultácií nad rámec činností uvedených v rámci SLA (uvedených v časti **Služby riadenia systémovej a aplikačnej podpory (paušál)**);
- Ďalšie činnosti a služby aplikačnej podpory súvisiace so zabezpečením prevádzky systému;
- Aktualizácia používateľskej a technickej dokumentácie po každej zmene systému;

Požiadavky služby realizácie zmenových požiadaviek (nad paušál)

Činnosti súvisiace s rozvojom systému. Tieto činnosti zahŕňajú implementáciu schválených požiadaviek objednávateľa na zmenu funkčnosti systému najmä:

- Rozširovanie funkcionality systému - Analýza, návrh a vývoj rozšírenia, vylepšenia a/alebo modifikácie aplikačného softvéru;
- Vykonanie úprav v nastavení modulov systému voči implementovanej funkčnosti a existujúcim nastaveniam;
- Programovanie nových funkcií v rámci existujúcich modulov systému;
- Vykonávanie úprav do existujúcich integračných rozhraní;
- Programovanie a implementácia nových integračných rozhraní;
- Realizácia testov podľa testovacích scenárov;
- Projektové riadenie zmien v zmysle Vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 z 9. októbra 2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v znení neskorších predpisov;
- Aktualizácia používateľskej a technickej dokumentácie po každej zmene systému.

Zmena funkčnosti zahŕňa pridanie, modifikáciu alebo zrušenie akejkoľvek časti systému a súvisiacej dokumentácie. Zmena funkčnosti môže byť vyvolaná legislatívnou požiadavkou a/alebo požiadavkou používateľov na zlepšenie existujúcej funkcionality alebo zavedenie novej funkcionality v novom riešení DO.

ID POŽIADAVKY (zvoľte si konvenciu označovania)	KATEGÓRIA POŽIADAVKY _funkčná požiadavka _nefunkčná požiadavka _technická požiadavka	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	DETAILNÝ POPIS POŽIADAVKY
1	Ne-Funkcna požiadavka	Procesy	Integrácia flow DO v procese registrácie používateľského účtu	DO je plne integrovaný v procese registrácie používateľského účtu s ohľadom na zrozumiteľnosť pre občana.
2	Funkcna požiadavka	Externé integrácie	Integrácia biometrie MVSR	Integračná služba DO umožňuje voľiteľnú validáciu fotografií využitím integrácie biometrie MVSR.
3	Funkcna požiadavka	Správa konfigurácie a politík	Auditné záznamy o zmenách konfigurácie	Každá zmena konfigurácie a politík DO musí byť zaznamenaná, rozsah auditného záznamu musí umožniť zaznamenanie celého kontextu požiadavky na zmenu aj zmeny samotnej
4	Funkcna požiadavka	Správa konfigurácie a politík	Definícia politík	Modul umožňuje definíciu špecifických politík pre všetky prípady použitia služieb digitálneho onboardingu. Definícia politiky obsahuje zoznam požadovaných a voľiteľných vstupov pre overenie ako aj hodnoty pre ich vyhodnocovanie.
5	Funkcna požiadavka	Správa konfigurácie a politík	Riadenie politík	Modul umožňuje riadenie zmien v politikách, podporuje verzionovanie politík, schvaľovanie ich nasadenia.
6	Technicka požiadavka	Správa konfigurácie a politík	Garancie úložiska politík	Úložisko politík implementuje vysokú mieru garancií integrity uložených záznamov a riadenia prístupu k nim. Úložisko politík chráni pred neželaným zásahom do záznamov.
7	Technicka požiadavka	Správa konfigurácie a politík	Garancie úložiska politík	Úložisko politík implementuje vysokú mieru garancií dostupnosti uložených záznamov a riadenia prístupu k nim.
8	Funkcna požiadavka	Správa konfigurácie a politík	Garancie záznamov politík	Modul umožňuje overiť integritu každého záznamu politiky samostatne.
9	Funkcna požiadavka	Správa konfigurácie a politík	Overenie integrity úložiska politík	Modul umožňuje overiť integritu úložiska a všetkých záznamov v úložisku politík.
10	Technicka požiadavka	Integrácie: Webové portály	Nástroje pre integráciu webových portálov	Modul integračnej služby DO poskytuje softvérové nástroje (SDK) pre zjednodušenú integráciu webových portálov.
11	Ne-Funkcna požiadavka	Integrácie: Webové portály	Vzhľad obrazoviek DO	SDK technológie DO umožňuje upraviť vzhľad obrazoviek DO v súlade so vzhľadom integrovanej aplikácie a štandardom ID-SK
12	Ne-Funkcna požiadavka	Integrácie: Webové portály	Optimálny flow DO	SDK technológie DO umožňuje implementovať flow procesov DO s ohľadom na potrebu opakovať len niektorý z krokov DO
13	Technicka požiadavka	Integrácie: Webové portály	Podpora integrácie webových portálov	SDK technológie DO implementuje integráciu webových portálov technológiou s vysokou mierou garancií - napr. WebAssembly https://webassembly.org/ alebo alternatívou.
14	Technicka požiadavka	Integrácie: Webové portály	Podpora webových prehliadačov	Riešenie umožňuje prípravu webovej aplikácie pre prehliadače s WebKit jadrom (Apple Safari)

15	Technická požiadavka	Integrácie: Webové portály	Podpora webových prehliadačov	Riešenie umožňuje prípravu webovej aplikácie pre prehliadače s Gecko jadrom (Firefox)
16	Technická požiadavka	Integrácie: Webové portály	Podpora webových prehliadačov	Riešenie umožňuje prípravu webovej aplikácie pre prehliadače s Blink jadrom (Chromium)
17	Technická požiadavka	Integrácie: Webové portály	Podpora webových prehliadačov	Riešenie umožňuje prípravu webovej aplikácie pre prehliadače so SpiderMonkey JavaScript enginom (Firefox)
18	Technická požiadavka	Integrácie: Webové portály	Podpora webových prehliadačov	Riešenie umožňuje prípravu webovej aplikácie pre prehliadače so V8 JavaScript enginom (Chromium)
19	Technická požiadavka	Integrácie: Webové portály	Podpora webových prehliadačov	Riešenie umožňuje prípravu webovej aplikácie pre prehliadače so WebKit JavaScript enginom (Apple Safari)
20	Technická požiadavka	Integrácie: Mobilná aplikácia	Nástroje pre integráciu mobilných platforiem	Modul integračnej služby DO poskytuje softvérové nástroje (SDK) pre zjednodušenú integráciu mobilných platforiem.
21	Ne-Funkčná požiadavka	Integrácie: Mobilná aplikácia	Vzhľad obrazoviek DO	SDK technológie DO umožňuje upraviť vzhľad obrazoviek DO v súlade so vzhľadom integrovanej aplikácie a štandardom ID-SK
22	Ne-Funkčná požiadavka	Integrácie: Mobilná aplikácia	Optimálny flow DO	SDK technológie DO umožňuje implementovať flow procesov DO s ohľadom na potrebu opakovať len niektorý z krokov DO
23	Technická požiadavka	Integrácie: Mobilná aplikácia	Podpora mobilných operačných systémov	SDK technológie DO podporuje Apple iOS 18 a novšie
24	Technická požiadavka	Integrácie: Mobilná aplikácia	Podpora mobilných operačných systémov	SDK technológie DO podporuje Google Android 12 a novšie
25	Technická požiadavka	Integrácie: Webové portály	Vyhodnotenie schopnosti vykonať DO	SDK technológie DO umožňuje vyhodnotiť, či mobilný telefón používateľa je schopný zrealizovať digitálny onboarding (kamera s dostatočným rozlíšením, verziu NFC rozhrania)
26	Technická požiadavka	Integrácie: Mobilná aplikácia	Vyhodnotenie schopnosti vykonať DO	SDK technológie DO umožňuje vyhodnotiť, či mobilný telefón používateľa je schopný zrealizovať digitálny onboarding (kamera s dostatočným rozlíšením, verziu NFC rozhrania)
27	Technická požiadavka	Integrácie: Webové portály	Podpora načítania elektronického dokladu cez NFC rozhranie	SDK technológie DO umožňuje načítanie údajov z elektronického dokladu cez NFC rozhranie v rozsahu, ktorý umožňuje garantované overenie jeho pravosti bezpečnostnými mechanizmami samotného NFC rozhrania
28	Technická požiadavka	Integrácie: Mobilná aplikácia	Podpora načítania elektronického dokladu cez NFC rozhranie	SDK technológie DO umožňuje načítanie údajov z elektronického dokladu cez NFC rozhranie v rozsahu, ktorý umožňuje garantované overenie jeho pravosti bezpečnostnými mechanizmami samotného NFC rozhrania
29	Funkčná požiadavka	Politiky	Poskytnutie politík klientskej strane	Služba integrácie DO umožní klientskej aplikácii prístup k politikám integrovanej aplikácie tak, aby tieto mohli byť použité v procese DO. Napr. minimálne/optimálne/maximálne rozlíšenie fotografie pre jednotlivé kroky DO (doklady, selfie), prípadne iné politiky.

30	Funkcna požiadavka	Politiky	Vyhodnotenie požiadaviek na vstupy	Služba integrácie DO prijme vstupy a vyhodnotí ich porovnaním s požiadavkami na vstupné dáta v jednotlivých krokoch procesu DO
31	Funkcna požiadavka	Spracovanie dokladov	Príjem fotografií dokladov na spracovanie	Služba integrácie DO prijme fotografie dokladu totožnosti a pošle ich na spracovanie Službe Overenia Digitálnej Identity (DI). Po vyhodnotení sa údaje získané od užívateľa nesmú ukladať na strane MIRRI, dáta majú slúžiť len na spracovanie overenia dokladov a následne zmazať.
32	Funkcna požiadavka	Spracovanie dokladov	Vyhodnotenie fotografií dokladov	Služba Overenia Digitálnej Identity vyhodnotí integritu a dôveryhodnosť fotografií dokladu a vydoluje z nich údaje o osobe. Parametre vyhodnotenia fotografií dokladu aj údaje o osobe pošle v odpovedi integračnej služby DO.
33	Funkcna požiadavka	Spracovanie dokladov	Vyhodnotenie výstupu spracovania fotografií dokladov	Služba integrácie DO prijme výstup spracovania fotografií dokladu, vykoná porovnanie s parametrami politik pre akceptáciu v procese DO a výstup pošle klientovi.
34	Funkcna požiadavka	Spracovanie dokladov	Vyhodnotenie dôveryhodnosti v registroch MVSR	Služba integrácie DO údaje z dokladu pošle na služby overenia identity MVSR.
35	Funkcna požiadavka	Spracovanie dokladov	Vyhodnotenie výstupu služby overenia identity MVSR	Služba integrácie DO prijme výstup overenia identity MVSR, vykoná porovnanie s parametrami politik pre akceptáciu v procese DO a výstup pošle klientovi.
36	Funkcna požiadavka	Procesy	Vynútenie opakovania krokov DO	V prípade nesúladu výstupu spracovania vstupov DO od klienta s politikami pre akceptáciu vstupov, integračná služba DO zabezpečí, že klientovi nebude umožnené pokračovať v ďalšom kroku. V mobilnej aplikácii bude logika pre opakovanie kroku alebo presmerovanie na alternatívy onboardingu, ale samotná služba bude riadiť dostupnosť volaní ďalších krokov v procese DO.
37	Funkcna požiadavka	Logovanie	Hlásenia o podozreniach a vážnych narušeniach	Služba integrácie DO akékoľvek závažné podozrenia a narušenia dôveryhodnosti služby nahlási do auditného záznamu.
38	Technicka požiadavka	Ochrana údajov	Bezpečné zmazanie a dočasné ukladanie citlivých dát	Citlivé dáta, ktoré si vyžadujú dočasné uloženie pri spracúvaní, sú po spracovaní zmašané spôsobom, ktorý znemožní získať tieto dáta forenznými nástrojmi
39	Technicka požiadavka	Ochrana údajov	Bezpečné zmazanie a dočasné ukladanie citlivých dát	Citlivé dáta, ktoré si vyžadujú dočasné uloženie pri spracúvaní, sú po spracovaní zmašané spôsobom, ktorý znemožní získať tieto dáta forenznými nástrojmi
40	Technicka požiadavka	Ochrana údajov	Bezpečné zmazanie a dočasné ukladanie citlivých dát	Citlivé dáta, ktoré si vyžadujú dočasné uloženie pri spracúvaní, sú po spracovaní zmašané spôsobom, ktorý znemožní získať tieto dáta forenznými nástrojmi

41	Technická požiadavka	Ochrana údajov	Bezpečné zmazanie a dočasné ukladanie citlivých dát	Citlivé dáta, ktoré si vyžadujú dočasné uloženie pri spracúvaní, sú po spracovaní zmazané spôsobom, ktorý znemožní získať tieto dáta forenznými nástrojmi
42	Ne-Funkčná požiadavka	Ochrana osobných údajov a súkromia	Analytický nástroj neumožní identifikáciu a sledovanie	Spôsob zapojenia analytického nástroja nesmie umožniť identifikovať občana alebo zariadenie alebo inak umožniť sledovanie jeho správania sa.
43	Technická požiadavka	Ochrana osobných údajov a súkromia	Ochrana pred sledovaním	Riešenie DO implementuje maximálnu možnú mieru ochrany pred sledovaním a identifikáciou prehliadača a zariadenia (fingerprinting). Spôsob ochrany zabráni sledovaniu aj integrovaným kódom tretej strany.
44	Funkčná požiadavka	Spracovanie fotografií tváre	Vyhodnotenie fotografií tváre	Služba overenia DI vyhodnotí integritu a dôveryhodnosť fotografií tváre a overí ich s fotografiou z predloženého dokladu. Parametre vyhodnotenia fotografií tváre pošle v odpovedi integračnej služby DO.
45	Funkčná požiadavka	Spracovanie fotografií tváre	Vyhodnotenie výstupu spracovania fotografií tváre	Služba integrácie DO prijme výstup spracovania fotografií tváre, vykoná porovnanie s parametrami politík pre akceptáciu v procese DO a výstup pošle klientovi.
46	Funkčná požiadavka	Spracovanie fotografií tváre	Vyhodnotenie dôveryhodnosti v registroch MVSR	V prípade fotografie tváre získanej z dokladu bez použitia NFC (s nízkym rozlíšením) pošle Služba integrácie DO fotografiu tváre na služby overenia identity MVSR.
47	Funkčná požiadavka	Spracovanie fotografií tváre	Vyhodnotenie výstupu služby overenia identity MVSR	Služba integrácie DO prijme výstup overenia identity MVSR, vykoná porovnanie s parametrami politík pre akceptáciu v procese DO a výstup pošle klientovi.
48	Technická požiadavka	Podpora používateľa	Nápoveda digitálneho onboarding	SDK technológie DO podporuje tvorbu nápovedy procesu digitálneho onboarding
49	Technická požiadavka	Podpora používateľa	Nápoveda digitálneho onboarding	SDK technológie DO podporuje tvorbu nápovedy procesu digitálneho onboarding
50	Funkčná požiadavka	Procesy	Opakovanie neúspešného scenára	Integračná služba DO v kontexte nastavenia politík umožní 2x zopakovať každý z krokov v prípade, že daný krok bol neúspešný. Používateľ je informovaný o dôvode neúspešnosti daného kroku. Po 3. neúspešnom nasnímaní dokladu alebo tváre sú používateľovi zobrazené všetky možnosti aktivácie.
51	Funkčná požiadavka	Procesy	Nasnímanie tváre a overenie živosti	Služba Overenia Digitálnej Identity vyhodnotí živosť používateľa. Po vyhodnotení sa údaje získané od užívateľa nesmú ukladať, dáta majú slúžiť len na spracovanie overenia a následne bezpečne zmazať.
52	Ne-Funkčná požiadavka	Integrácie: Mobilná aplikácia	Zabezpečenie SK a EN jazykovej verzie	SDK technológie DO umožní sprístupnenie slovenskej a anglickej jazykovej mutácie podľa globálneho nastavenia aplikácie pri spustení.

53	Ne-Funkcna poziadavka	Integrácie: Webové portály	Zabezpečenie SK a EN jazykovej verzie	SDK technológie DO umožní sprístupnenie slovenskej a anglickej jazykovej mutácie podľa nastavenia preferencií používateľa v prehliadači.	
54	Technicka poziadavka	Integrácie: Mobilná aplikácia	Zber analytických údajov	SDK technológie DO umožní integrovať obrazovky DO do spracovania analytických dát	
55	Technicka poziadavka	Integrácie: Webové portály	Zber analytických údajov	SDK technológie DO umožní integrovať obrazovky DO do spracovania analytických dát	
56	Ne-Funkcna poziadavka	Výkon a dostupnosť služieb	Počet Používateľov	Na základe štatistických údajov o počtoch používateľov aplikácie SVM očakávame za prvých 12 mesiacov cca 100 000 unikátnych nových používateľov aplikácie, ktorí sa onboardujú prostredníctvom digitálneho onboarding, pričom bude potrebné zvoliť architektúru tak, aby sa výkon systému dal zvyšovať podľa potreby.	
57	Technicka poziadavka	Výkon a dostupnosť služieb	Odozva grafického rozhrania	Maximálna doba odozvy grafického rozhrania do 2 sekúnd, v prípade načítavania dát z externého IS upozorniť používateľa, že prebieha načítanie.	DO v mobilnej aplikácii
58	Technicka poziadavka	Výkon a dostupnosť služieb	Odozva grafického rozhrania	Maximálna doba odozvy grafického rozhrania do 2 sekúnd, v prípade načítavania dát z externého IS upozorniť používateľa, že prebieha načítanie.	DO vo webovom portále
59	Ne-Funkcna poziadavka	Výkon a dostupnosť služieb	Správa systému a prevádzková podpora	Help Desk bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením: - L1 podpory IS (Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa – IS Solution manager, ktorý je v správe verejného obstarávateľa a v prípade jeho nedostupnosti Centrum podpory používateľov (zabezpečuje prevádzkovateľ IS a DataCentrum). - L2 podpory IS (Level 2, postúpenie požiadaviek od L1) - vybraná skupina dodávateľom riadne zaškolených garantov, so znalosťou funkcionality diela alebo jeho časti riadne uvedeného do prevádzky. - L3 podpory IS (Level 3, v režime 8x5, postúpenie požiadaviek od L2) - na základe zmluvy o službách a podpore IS (zabezpečuje víťazný uchádzač) v súlade s procesmi ITILv4 a podľa pravidiel určených v budúcej SLA.	

60	Ne-Funkcna poziadavka	Výkon a dostupnosť služieb	Klasifikácia väd pre Akceptačné testovanie	Požiadavka na klasifikáciu väd pre akceptačné testovanie: A- Kritická - Kritické vady, ktoré spôsobia úplné zlyhanie diela ako celku a nie je možné používať ani jednu jeho časť. B – Vysoká - Vady a nedostatky, ktoré zapríčinia čiastočné zlyhanie diela a neumožňuje používať časť diela. C- Stredná - Vady a nedostatky, ktoré spôsobia čiastočné obmedzenia používania diela. D – Nízka - Kozmetické a drobné vady.
61	Ne-Funkcna poziadavka	Výkon a dostupnosť služieb	Kvalita služieb pri testovaní	Požiadavka na kvalitu služieb pri vykonaní testov a vykonanie rozhodnutia o spustení pilotnej prevádzky a tiež finálnej akceptácie – platí pre všetky služby, funkcie a API spoločne (počet väd je určený ako súčet identifikovaných väd): A - Kritická - Kritické vady, ktoré spôsobia úplné zlyhanie diela ako celku a nie je možné používať ani jednu jeho časť (0 väd). B – Vysoká - Vady a nedostatky, ktoré zapríčinia čiastočné zlyhanie diela a neumožňuje používať časť diela (maximálne 1 vada). C- Stredná - Vady a nedostatky, ktoré spôsobia čiastočné obmedzenia používania diela (maximálne 2 vady). D – Nízka - Kozmetické a drobné vady (nie je obmedzené).

62	Technická požiadavka	Požiadavka na infraštruktúru	Architektonické princípy	Prí technickej a systémovej architektúre budú dodržané všetky definované priority informatizácie VS a tiež všetky technologické a dátové princípy, ako sú najmä: - Technologická interoperabilita – softvér a hardvér vo verejnej správe musí byť v súlade s definovanými štandardami, ktoré podporujú interoperabilitu údajov, aplikácií a technológií. - Otvorené štandardy – prednostne sa budú používať otvorené štandardy a formáty a dôraz bude na zabezpečení technologickej neutrálnosti. - Vládny cloud prednostne – informačné systémy a technológie, ktoré sa v rámci verejnej správy rozvíjajú alebo modifikujú, musia byť budované v kooperácii s poskytovateľmi cloudových služieb v zmysle ich nasadenia do Vládneho cloudu. - Otvorenosť údajov – údaje otvorenej vlády musia byť dostupné a prehľadné. Vybrané množiny údajov nebudú podliehať princípom otvorených údajov. Tento princíp však nesmie byť v rozpore s princípom „jeden krát a dost“. - Údaje sú dostupné a zdieľané – používatelia majú prístup ku všetkým údajom, na ktoré majú legitímny nárok, či už pre informatívne účely alebo pre potreby naplnenia svojich povinností. Údaje sú a budú zdieľané naprieč verejnou správou v súlade s platnou legislatívou. - Jednoduché používanie aplikácií – aplikácie VS musia byť jednoduché na použitie pre koncového používateľa, či už z technického alebo z obsahového hľadiska. - Bezpečnosť údajov – údaje budú chránené najmä pred neoprávneným prístupom, manipuláciou, použitím a zverejnením (zachovanie dôvernosti údajov), ich úmyselnou alebo neúmyselnou modifikáciou (zachovanie integrity údajov) a budú dostupné v požadovanom čase a v požadovanej kvalite (zachovanie dostupnosti údajov). - Pravosť údajov – používateľ bude pracovať len s údajmi, ktorých hodnotnosť a pôvod sú zabezpečené napr. ich autorizáciou. - Auditovateľnosť – riadenie informačnej bezpečnosti, rovnako ako aj iných aktivít vo VS, musí používať princípy a pravidlá, ktoré umožňujú
63	Ne-Funkčná požiadavka	Požiadavka na UX / UI / UCD	Vykonanie UX prieskumov	Vykonanie UX prieskumov pre digitálny onboarding prostredníctvom tvárovej biometrie, zapracovanie pripomienok a kontinálny zber spätnej väzby do ukončenia projektu.
64	Ne-Funkčná požiadavka	Požiadavka na UX / UI / UCD	Analýza a návrh procesu z hľadiska UX	Analýza a návrh UI/UX/procesov portálu pre digitálny onboarding

65	Ne-Funkcna poziadavka		Testovanie portálu	Testovanie na QA a UAT prostredí v súlade s požiadavkami a v rozsahu podľa detailného časového plánu testovania funkcionalít DO, podľa popisov testov a testovacích procedúr s cieľom overiť dosiahnutie akceptačných kritérií: _ Funkčné testy (FAT) _ Súčinnosť pre vykonanie Bezpečnostných testov _ Regresné testy / Závažové testy _ Systémové integračné testy (SIT) _ UX testy _ UAT testy
66	Ne-Funkcna poziadavka		Nasadenie služieb a PIP	Súčinnosť pri nasadení riešenia na UAT a PROD prostredia a riadne uvedenie riešenia do riadnej produkčnej prevádzky vrátane aktualizácie požadovanej prevádzkovej dokumentácie a používateľských manuálov.
67	Ne-Funkcna poziadavka	Dokumentácia	Dokumentácia pre služby DO	Vytvorenie dokumentácie pre backend služby DO, integračných manuálov a príručiek pre vývojárov.
68	Ne-Funkcna poziadavka	Dokumentácia	Aktualizácia dokumentácia pre release	Vytvorenie aktualizovanej dokumentácie pre release. Vytvorenie a udržiavanie DNR k riešeniu vo všetkých fázach realizácie projektu v súlade s vyhláškou MIRRI č. 401/2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v znení neskorších predpisov. DNR môže vznikať priebežne s ohľadom na agilný spôsob vývoja a jeho finálna verzia bude zafixovaná najneskôr 1 mesiac pred začatím UAT testov na prostredí prevádzkovateľa modulu.

69	Ne-Funkcna poziadavka	Všeobecné požiadavky	Implementácia PZ	Požiadavky na implementáciu Projektového zámeru v rozsahu minimálne: • Príprava a prevádzkovanie technologických prostredí potrebných v procese návrhu, implementácie, testovania a dodania PZ do riadnej prevádzky, • Zabezpečenie a dodanie funkcionality podľa detailnej funkčnej a technickej špecifikácie podľa funkčných celkov (Objednávateľom a Dodávateľom vzájomne odsúhlasené VOB - voice of business a VOC - voice of customer), • Definovanie pravidiel pre organizáciu jednotlivých vrstiev zdrojového kódu (Dodržať § 15 ods. 2 písm. d) bod 2. zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov), • Vývoj príslušných SW objektov a tried, • Vývoj integračných rozhraní, • Zabezpečenie kvality kódu prijatím príslušných opatrení, • Integrácia častí diela v súlade s popísanými cieľovými Biznis procesmi, ktoré predloží Objednávateľ • Zabezpečenie finálnej compatibility jednotlivých dodávok ako funkčného celku
70	Ne-Funkcna poziadavka	Dátová architektúra	Testovacie dáta	Testovacie dáta budú pripravované v spolupráci so zástupcami zdrojových IS VS, ktoré budú využívať funkcionality Slovensko v mobile (testovacie OP resp. identity z MV SR).
71	Ne-Funkcna poziadavka	Bezpečnostné požiadavky	Ochrana údajov	Systém bude obsahovať bezpečnostné opatrenia zabezpečujúce ochranu údajov používaných pri prihlásení do sietí a informačných systémov, ktoré zabráňujú zneužitiu týchto údajov neoprávnenou osobou
72	Ne-Funkcna poziadavka	Ochrana osobných údajov a súkromia	GDPR	Ak bude v súvislosti s prevádzkovaním aplikácie dochádzať ku spracovaniu osobných údajov fyzických osôb, ktoré budú využívať aplikáciu. Dodávateľ na základe tejto skutočnosti musí zabezpečiť implementáciu všetkých požiadaviek v zmysle príslušných ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES

73	Ne-Funkcna poziadavka	Ochrana osobných údajov a súkromia	GDPR	V súvislosti s prevádzkovaním aplikácie bude dochádzať ku spracovaniu osobných údajov fyzických osôb, ktoré budú využívať aplikáciu. Projekt/dodávateľ na základe tejto skutočnosti musí zabezpečiť implementáciu všetkých požiadaviek v zmysle príslušných ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES. Osobné údaje je potrebné spracovávať iba pre odôvodnené účely spracúvania osobných údajov, po obmedzenú dobu a s využitím maximálnej možnej miery zabezpečenia. Pre dodržanie všetkých legislatívnych požiadaviek Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 je potrebné realizovať vo fáze vývoja a implementácie aplikácie analýzu organizačných a IT procesov, ktoré pokrývajú spracovateľské činnosti osobných údajov. Aplikácia Slovensko v mobile sa bude riadiť národnou legislatívou, kde je ochrana osobných údajov fyzických osôb upravená: • Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • Vyhláška Úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
74	Ne-Funkcna poziadavka	Všeobecné požiadavky	Súlad s internými smernicami MIRRI	Požiadavka na súlad s internými smernicami MIRRI o riadení projektov, s ktorými Objednávateľ Dodávateľa riadne a preukázateľne oboznámi pred začiatkom analýzy.
75	Ne-Funkcna poziadavka	Všeobecné požiadavky	Aplikovanie dokumentu NKIVS	Požiadavka na primerané aplikovanie dokumentu - Národná koncepcia informatizácie verejnej správy Slovenskej republiky (NKIVS) počas návrhu a uvedenia nových alebo rozšírených služieb do prevádzky.
76	Ne-Funkcna poziadavka	Všeobecné požiadavky	Aplikovanie dokumentu Strategické priority NKIVS	Požiadavka na súlad a primerané aplikovanie v čase návrhu a implementácia platného dokumentu Strategické priority NKIVS.
77	Ne-Funkcna poziadavka	Všeobecné požiadavky	Aplikovanie dokumentu PZ k projektu DO	Požiadavka na súlad a aplikáciu dokumentu Projektový zámer k projektu DO (dostupné na https://metais.slovensko.sk/ci/Projekt/db386237-166d-485d-8d9b-f28aad52565b/documents) primerane aplikovaný počas návrhu, implementácie a uvedenia PZ do prevádzky.
78	Ne-Funkcna poziadavka	Všeobecné požiadavky	Aplikovanie dokumentu Metodika pre systematické zabezpečenie org. VS	Aplikovanie dokumentu Metodika pre systematické zabezpečenie org. VS

79	Ne-Funkcna poziadavka	Bezpečnostné požiadavky	Riadenie prístupov	Systém zachová riadenie prístupov používateľov k sieťam a IS podľa zásady povolenia minimálneho prístupu nutného len pre realizovanie úlohy
80	Ne-Funkcna poziadavka	Reporting	Tvorba reportu pre sledovanie KPIs projektu	Ako biznis vlastník/projektový manažér chcem mať k dispozícii reporty pre vyhodnotenie KPIs stanovených v PZ
81	Funkcna poziadavka	Reporting	Hlásenia o zlyhaniach sú zbierané centrálné	Hlásenia o zlyhaniach sú posielané do centrálného repozitára na ďalšie spracovanie
82	Ne-Funkcna poziadavka	Reporting	Hlásenia o zlyhaniach obsahujú kontext modulu	Hlásenia o zlyhaniach obsahujú kontext kódu pre identifikáciu konkrétneho modulu, v ktorom došlo k zlyhaniu.
83	Ne-Funkcna poziadavka	Reporting	Hlásenia o zlyhaniach obsahujú úroveň výnimky	Hlásenia o zlyhaniach obsahujú kontext úrovne výnimky, pri ktorej došlo k zlyhaniu.
84	Funkcna poziadavka	Reporting	Spracovanie hlásení o zlyhaniach	Riešenie zahŕňa vyhodnocovanie chybovosti všetkých integrovaných aplikácií a portálov tak, aby bolo možné vyhodnocovať kvalitu ich integrácie a mieru garancií deklarovaných v požiadavkách na integráciu a akceptovaných integrujúcou sa stranou.
85	Funkcna poziadavka	Reporting	Prístup analytickým dátam	Riešenie umožní prístup k analytickým dátam správcovi/vlastníkovi integrovanej aplikácie v minimálnej miere potrebnej na vyhodnocovanie kvality a vylepšení funkcionality integrácie.
86	Ne-Funkcna poziadavka	Školenia	Realizácia školení	Dodávateľ riešenia zabezpečí vyšškolenie koncových používateľov/administrátorov v rozsahu 2 školení po 8 hodín.
87	Ne-Funkcna poziadavka	Školenia	Realizácia školení	Dodávateľ riešenia zabezpečí dokumentáciu pre vývojárov integrujúcich sa aplikácií a portálov.
88	Ne-Funkcna poziadavka	Prevádzka	Nasadenie a PIP	Súčinnosti pri nasadení riešenia a uvedenia do riadnej produkčnej prevádzky vrátane aktualizácie požadovanej prevádzkovej dokumentácie minimálne v rozsahu školiace materiály, integračná príručka, príručka používateľa vrátane realizácie školení
89	Ne-Funkcna poziadavka	Bezpečnostné požiadavky	Dodanie podkladov k Bezpečnostnému projektu	Požiadavky na dodanie podkladov k vykonaniu nezávislého bezpečnostného projektu vrátane kontroly zdrojového kódu integrácií, podľa aktuálnych bezpečnostných štandardov v čase odovzdávania predmetu zákazky, tak aby bolo možné vykonanie auditu komponentov, ktoré sú výstupom plnenia diela. Dodávateľ musí zapracovať zistenia a nálezy bezpečnostného projektu brániace riadnemu užívaniu predmetu dodávky. Požiadavky na dodanie podkladov k overeniu zapracovania pripomienok a odstránenia nálezov brániacich riadnemu používaniu predmetu diela.

90	Ne-Funkcna požiadavka	Dokumentácia	Vypracovanie Bezpečnostného projektu	Súčasťou dodávky diela bude vypracovanie Bezpečnostného projektu v zmysle legislatívnych požiadaviek, ktorého prvá verzia musí byť dodaná najneskôr s Detailným návrhom riešenia (DNR), pričom Bezpečnostný projekt musí byť aktualizovaný Dodávateľom počas celej realizačnej fázy projektu, aj na základe nálezov z bezpečnostného testovania
91	Ne-Funkcna požiadavka	Výkon a dostupnosť služieb	Dostupnosť služieb	Dostupnosť všetkých služieb digitálneho onbardingu bude v režime 24/7, resp.95 %, t. j. max. výpadok je: - 1,24 hodiny (1 hodina 12 minút) denne - 8,8 hodín (8 hodín 24 minút) týždenne - 1 deň, 12 hodín 13 minút mesačne - 18 dní 2 hodiny 41 minút ročne Nedostupnosť IS sa počíta počas prevádzkových hodín od momentu zaevidovania udalosti, ktorá ju spôsobila (zaevidovanie formou incidentu monitorovacím nástrojom, auditným záznamom alebo inou formou preukazujúcou zdroj, typ a čas udalosti). Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS.
92	Technicka požiadavka	Požiadavka na infraštruktúru	Dostupné prostredia	IS bude využívať minimálne nasledovné prostredia: • Vývojové 1x (zabezpečuje Dodávateľ) • Testovacie 1x (zabezpečuje Objednávateľ) • Produkčné 1x (zabezpečuje Objednávateľ)
93	Legislatívna požiadavka	Legislatívne požiadavky	Súlad s nariadením EU 910/2014	Súlad s Nariadením Európskeho parlamentu a rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
94	Ne-Funkcna požiadavka	Dokumentácia	Analýza a dizajn	Úvodná analýza a výskum zákazníckych skupín
95	Ne-Funkcna požiadavka	Dokumentácia	Analýza a dizajn	Návrh funkčného riešenia (MVP verzia)
96	Ne-Funkcna požiadavka	Dokumentácia	Analýza a dizajn	Návrh používateľského rozhrania, UI flowov a prototypu
97	Ne-Funkcna požiadavka	Dokumentácia	Analýza a dizajn	Používateľské testovanie prototypu a jeho optimalizácia (pred implementáciou alebo v priebehu UAT testovania/pred spustením do produkčnej verzie)
98	Ne-Funkcna požiadavka	Dokumentácia	Požiadavky na testovacie prostredia	Detailný časový rámec testovania
99	Ne-Funkcna požiadavka	Dokumentácia	Požiadavky na testovacie prostredia	Popis testov a testovacích procedúr
100	Ne-Funkcna požiadavka	Dokumentácia	Požiadavky na testovacie prostredia	Zodpovednosti počas testovania
101	Ne-Funkcna požiadavka	Dokumentácia	Požiadavky na testovacie prostredia	Testovacie fázy

102	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	Funkčné testy (FAT)
103	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	Bezpečnostné testy
104	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	Regresné testy / Závažové testy
105	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	Systémové integračné testy (SIT)
106	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	UX testy a testy naplnenie štandardov prístupnosti
107	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	UAT testy
108	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	Monitoring systémov
109	Ne-Funkcna poziadavka	Dokumentácia	Poziadavky na testovacu	Ako súčasť výstupov bude dodaná kompletná dokumentácia na základe hore uvedeného zoznamu aj s príslušnými výstupmi/reportami (platí pre jednotlivé fázy testovania)
110	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej	Aplikačná príručka
111	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej	Konfiguračná príručka
112	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej	Inštalčná príručka
113	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej	Integračná príručka
114	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej dokumentácie	Používateľská príručka (resp. doplnenie existujúcich príručiek o nové komponenty/funkcie)
115	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej dokumentácie	Prevádzkový opis a pokyny pre servis a údržbu vrátane pokynov pre obnovu v prípade výpadku alebo havárie (Havarijný plán)
116	Ne-Funkcna poziadavka	Dokumentácia	Príprava produktovej dokumentácie	Detailný návrh riešenia (aktualizovať aj všetku príslušnú, t.j. bezpečnostný, software, atď, dokumentáciu)
117	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Kvalita zdrojových kódov	Každý zdrojový kód (aj preexistentný) musí napĺňať požiadavky kvality podľa článku 15 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru. - zdrojový kód musí byť čitateľný a komentovaný priamo v kóde - zdrojový kód nesmie byť modifikovaný spôsobom, ktorý obmedzuje čitateľnosť a spracovanie
118	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Obsah zdrojových kódov	Každý zdrojový kód (aj preexistentný) musí napĺňať požiadavky obsahu podľa článku 14 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru. - Zdrojový kód musí obsahovať všetky komponenty, ktoré umožnia jeho preklad, spustenie alebo vytvorenie inštalčného balíka. - Zdrojový kód nesmie obsahovať citlivé a dôverné údaje

119	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Štruktúra zdrojových kódov	Každý zdrojový kód, ktorý je predmetom vývoja, musí napĺňať požiadavky obsahu podľa článku 16 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru. - súčasťou Zdrojového kódu musí byť informácia o licencií, spôsobe označovania verzií, postupoch kompilácie a inštalácie a spôsobe hlásenia bezpečnostných zraniteľností - štruktúra repozitára zdrojových kódov zohľadňuje oddelenie zdrojových kódov, dátových súborov, podporných a treťostranných knižníc, konfiguračných súborov a dokumentácie
120	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Závislosti softvéru	Každý zdrojový kód, ktorý je predmetom vývoja, musí doložiť úplný zoznam priamych závislostí podľa článkov 21-23 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru.
121	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Statická analýza kvality a bezpečnosti	Každý zdrojový kód, ktorý je predmetom vývoja, a každé jeho vydanie, musí byť predmetom kontroly kvality a bezpečnosti podľa článkov 26 a 27 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru.
122	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Dynamická analýza kvality a bezpečnosti	Každý zdrojový kód, ktorý je predmetom vývoja, a každé jeho vydanie, musí byť predmetom kontroly kvality a bezpečnosti podľa článkov 28 a 29 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru.
123	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Určenie názvu	Každý zdrojový kód (aj preexistentný), musí mať definované označenie menom podľa článku 6 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru.
124	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Určenie verzionovania	Každý zdrojový kód, ktorý je predmetom vývoja, musí mať definované pravidlá označovania verzií podľa článku 7 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru.
125	Ne-Funkcna poziadavka	Zdrojové kódy a balíky softvéru	Určenie licencie	Každý zdrojový kód, ktorý je predmetom vývoja, musí mať určenú licenciu podľa článku 8 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru. V prípade pre-existentného zdrojového kódu musí byť určená licencia pre využitie v kontexte jeho začlenenia do výstupov projektu (výrobca môže umožniť viacero typov licencií).
126	Ne-Funkcna poziadavka	Procesy vývoja a nasadenia	Proces testovania vydania	Každý zdrojový kód má zdokumentovaný proces testovania nového vydania na kontrolu kvality a bezpečnosti (statickú aj dynamickú) podľa článkov 24-29 metodiky 024007/2023 o kvalite zdrojových kódov a balíkov softvéru.

[illegible]