Národné centrum zdravotníckych informácií

Dohoda o integračnom zámere Ministerstva investícií regionálneho rozvoja a informatizácie Slovenskej republiky, Ministerstva vnútra Slovenskej republiky a Národného centra zdravotníckych informácií (ďalej aj len „Dohoda“)

Subjekt	Národné centrum zdravotníckych informácií	**Subjekt**	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Meno	Ing. Pavol Capek	**Meno**	Ing. Mgr. Andrej Kramár
Funkcia	generálny riaditeľ	**Funkcia**	Vedúci sekcie informačných technológií verejnej správy
Dátum	29.6.2021	**Dátum**	
Podpis		**Podpis**	
		Subjekt	Ministerstvo vnútra Slovenskej republiky
		Meno	Rastislav Rejdovian
		Funkcia	Generálny riaditeľ sekcie informatiky, telekomunikácií a bezpečnosti MV SR
		Dátum	
		Podpis	

Projekt:	Integrácia aplikácie IS GreenPass na SmartCertApp
Dokument:	DIZ-MVSR-NCZI-VerifierApp-OverPassSpecial-v1.0.docx
Verzia:	1.0
Dátum:	29.06.2021
Autor:	
Vlastník:	Národné centrum zdravotníckych informácií

História dokumentu

Verzia	Dátum verzie	Popis zmien	Vypracoval
0.1	7.6.2021	Iniciálny dokument	
0.2	21.6.2021	Doplnený popis GreenPass a integračných procesov a scenárov.	
0.3	24.6.2021	Doplnenia dokumentu	
0.4	25.6.2021	Pripomienkovanie a doplnenia dokumentu	
0.5	25.6.2021	Doplnenia dokumentu	
0.6	27.06.2021	Pripomienkovanie a doplnenia dokumentu	
0.7	27.06.2021	Doplnenia dokumentu	
0.8	28.6.2021	Doplnenia dokumentu	
0.9	29.6.2021	Opravy	
0.10	29.06.2021	Zapracovanie pripomienok	
1.0	29.6.2021	Finálny dokument	

Obsah

Použité pojmy a skratky

Skratka	Popis
NCZI	Národné centrum zdravotníckych informácií
DIZ	Dohoda o integračnom zámere
SCA	Informačný systém Smart Cert App
IS	Informačný systém
API	Application programming interface alebo skratkou API (rozhranie pre programovanie aplikácií)
CA	Certifikačná autorita.
IP	Internetový protokol.
mTLS	Mutual authentication.
MOA	Mobilná aplikácia.
BE	Backend, serverová časť informačného systému.
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.
MV SR	Ministerstvo vnútra Slovenskej republiky.
PZ SR	Policajný zbor Slovenskej republiky.
PZS	Poskytovateľ zdravotnej starostlivosti
EÚ	Európska únia.
SR	Slovenská republika.
digitálny COVID preukaz EÚ alebo DCC alebo DGC	potvrdenia obsahujúce informácie o držiteľovom očkovaní, výsledku testu alebo prekonaní ochorenia vydané v súvislosti s pandémiou ochorenia COVID-19
Zmluva o spolupráci	Zmluva o bezodplatnej spolupráci pri sprístupňovaní digitálneho COVID preukazu EÚ medzi NCZI a MV SR

1 Úvodné ustanovenia

1.1 Identifikácia subjektov integračného zámeru

Subjektmi Dohody o integračnom zámere sú Národné centrum zdravotníckych informácií (NCZI), Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI) ako integrujúci sa subjekt a Ministerstvo vnútra Slovenskej republiky (MV SR) ako koncový konzument poskytovaných údajov. Koncovým IS v rámci integrácie bude IS GreenPass, poskytovateľom riešenia bude IS SmartCertApp. Postavenie subjektov Dohody z pohľadu ochrany osobných údajov budú predmetom samostatných zmlúv o spolupráci.

Subjekty Dohody	Rola	Správca (Gestor)	IS spadajúce pod Dohodu
	Konzument	MV SR	*IS GreenPass isvs_10804*
	Prevádzkovateľ	MIRRI	*IS GreenPass isvs_10804*
	Poskytovateľ	NCZI	*SmartCertApp*

1.2 Zdôvodnenie a ciele integračného zámeru

Projekt implementácie slovenskej verzie Digital Covid Certificate (DCC) vyplýva z požiadaviek EÚ na harmonizáciu procesov pre vydávanie a preukazovanie sa dokladmi o vakcinácii osoby, vykonaných testov na COVID-19 a potvrdení o prekonaní ochorenia COVID-19. Návrh a implementácia riešenia umožní občanom využívať štandardné riešenie digitálnej verzie DCC a pomôže automatizovať procesy v súlade s usmerneniami EÚ, primárne platnou legislatívou, nižšími právnymi normami a internými metodikami SR.

Na základe analýzy v prípravnej fáze, kde boli posúdené alternatívy z pohľadu biznisovej, aplikačnej a technologickej vrstvy, sa ako vybraná alternatíva stanovilo riešenie vývoj natívnej mobilnej aplikácie (verifier app) OverPassSpecial. Backend aplikácie OverPassSpecial s názvom IS GreenPass pre prístup k neverejným rozhraniam NCZI bude umiestnený vo vládnom cloude.

IS GreenPass poskytuje rozhrania pre OverPassSpecial, ktoré sú vytvorené v súlade s Projektovým zámerom a Projektový prístupom a príslušným katalógom požiadaviek, ktorý je prílohou Projektového zámeru:

- Mobilná aplikácia pre policajtov a iné oprávnené osoby koncového konzumenta na overenie existencie certifikátov vydaných v rámci EU (**OverPass Special** / verifier app / iba OS Android 6+) v rozsahu:
    - získanie verejného kľúča členských štátov EU poskytnutého cez SCA, jeho uloženie v lokálnom úložisku BE a použitie pre overenie naskenovaného QR kódu v online režime,
    - verifikovanie certifikátov v offline režime načítaním QR kódu a overením platnosti podľa príslušného verejného kľúča národnej autority,
    - online overenie platnosti a pravosti certifikátu na základe unikátneho identifikátora certifikátu (ak bude dostupné API a pripojenie na Internet),
    - online overenie a zobrazenie certifikátov osoby na základe kombinácie údajov o osobe (rodné číslo, identifikačný doklad + dátum narodenia,...) (ak bude dostupné API a pripojenia na Internet),
    - zobrazenie informácie o overení certifikátu pre obsluhu (v rozsahu a v súlade s platnou metodikou),

1.3 Rozpočet

Náklady na integráciu informačných systémov SCA a IS GreenPass sú hradené na každej strane zvlášť zo samostatných rozpočtových položiek projektov obidvoch subjektov Dohody.

2 Rozsah integrácie

Sekcia zachytáva rozsah integrácie z pohľadu komplexnosti integrovaných biznis procesov a požiadaviek na funkcionalitu/služby. IS GreenPass a v rámci IS aplikácie OverPassSpecial bude:

Názov API rozhrania Smart Cert App
Smart Cert App verified check services api

V prípade zmeny rozsahu integrácie sa táto Dohoda bude dopĺňať dodatkami.

2.1 Architektúra riešenia SCA

Nižšie je zobrazená aplikačná architektúra SCA, vrátane zakreslených aktuálne plánovaných komunikačných kanálov.

2.2 Biznis architektúra digitálneho COVID preukazu

Nasledujúci diagram znázorňuje architektúru biznis služieb DCC. Občan používa natívnu mobilnú aplikáciu (Wallet app), prostredníctvom ktorej bude môcť občan uložiť digitálnu verziu DCC vo svojom mobilnom zariadení a následne ju použiť na preukázanie sa oprávnenej osobe. PZ SR, ako osoba oprávnená vykonávať overovanie platnosti a pravosti certifikátov používa aplikáciu OverPassSpecial na overenie (Verifier app) platnosti a pravosti DCC predložených v papierovej alebo elektronickej podobe. Predmetom integrácie aplikácie OverPass Special sú farebne zvýraznené (žltou) časti architektúry.

2.3 Aplikačná architektúra digitálneho COVID preukazu

Nasledovný diagram znázorňuje aplikačnú architektúru, jej štruktúru a nevyhnutné integrácie v rámci komplexného pohľadu.

Aplikačné komponenty sú rozdelené do 3 skupín.

- **Koncové služby** – do tejto skupiny patrí aplikácia **OverPassSpecial** je vytvorená tak, aby nebolo používanie dát a procesov DCC možné spojiť s inými procesmi, ktoré nesúvisia s riadením boja proti pandémii spôsobenej koronavírusom,
- **Externé systémy eGOV** – ide o systém, ktoré cez API rozhranie poskytuje služby na získanie a overenie dát. Aplikácia **OverPassSpecial** je integrovaná na:
    - Greenpass service API (DCC MOA BackEnd)
    - Smart Cert App verified check services api (Privátne API SCA)
- **Externé systémy** – systémy tretích strán, ktoré sú dôležité v procese publikovania aplikácií a ich sprístupneniu koncovým používateľom.

2.4 Technologická architektúra Greenpass service API

Technologická architektúra bude postavená na technológii vládneho cloudu a projekt využije open-source SW jednak pre lepšiu ekonomickú bilanciu projektu a tiež z dôvodu stratégie plánovania štátnych IT projektov.

Z pohľadu technologických požiadaviek sú všetky definované v prílohe Katalóg požiadaviek, ktorý tvorí Prílohu č. 1 Projektového zámeru. Technologické požiadavky vychádzajú z povahy diela a sú detailne nadefinované.

Pre projekt DCC boli definované nasledovné komponenty:

- vládny cloud - servery, dátové úložiská, sieťové a komunikačné prvky, zálohovacie stanice, pracovné stanice a periférne zariadenia, kabeláž, inštalačné skrine,
- systémový a VM Softvér,
- databázový Softvér – PostgreSQL (ak bude potrebné perzistovať údaje),
- nástroje pre monitoring, logovanie prevádzky a vzdialenú správu Komponentov DCC,
- nástroje pre pravidelné prevádzkové zálohovanie DCC.

Nasledujúci diagram zobrazuje Technologickú architektúru DCC:

Pri budovaní aplikačných komponentov v rámci navrhovaného riešenia sa predpokladá využitie služieb vládneho cloudu. Pôjde minimálne o model využívania dostupných služieb IaaS (teda využitie virtuálneho dátového centra), pri ktorom cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry ako serverov, úložísk údajov a sieťovej infraštruktúry. Zároveň sa okrem vlastnej fyzickej lokality predpokladá aj využitie housingových služieb z DC vládneho cloudu.

- Predpokladá sa využitie najmä nasledujúcich služieb typu IaaS:
    - virtuálny server,
    - diskový priestor,
    - sieťové pripojenie,
- Predpokladá sa využitie najmä nasledujúcich služieb typu PaaS:
    - služby aplikačnej vrstvy,
    - služby bezpečnosti,
    - služby monitoringu a manažmentu.
- Predpokladá sa využitie nasledujúcich služieb typu SaaS
    - aplikácia pre správu webového obsahu,
    - aplikácia pre zálohu a archiváciu dát Služby vládneho cloudu.

2.5 Popis hlavných služieb využívaných v procesoch

OVM definovaný legislatívou bude pristupovať cez dedikované neverejné API (Smart Cert App verified check) prostredníctvom ktorých off-line / online overí DCC vygenerovaný na SR prostredníctvom SCA.

Zároveň bude kontrolná aplikácia (verifier app) pristupovať k Trust listu verejných kľúčov členských štátov EÚ prostredníctvom samostatného API, ktorých doručovanie zabezpečí SCA medzi EU a SK riešeniami, ktorá je ako jediný zdroj aktuálne platných verejných kľúčov členských štátov EÚ na Slovensku.

Procesy a dátové toky sú navrhnuté v súlade s Nariadením Európskeho parlamentu a rady (EÚ) 2021/953 a technickými špecifikáciami publikovanými sieťou elektronického zdravotníctva (https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v4_en.pdf) s cieľom umožniť overenie pravosti, platnosti a integrity potvrdenia v zmysle požiadaviek nariadenia (EÚ) 2021/953, odsek (15, 16, 17, 32 a 51) a plne rešpektovali pravidlá, politiky, špecifikácie, protokoly, formáty údajov a digitálnu infraštruktúru definované v rámci čl.2, bod 11.

API Smart Cert App verified check je realizované ako samostatný host na jednej verejnej IP adrese s definovanými mTLS pravidlami nezávisle od iných hostov na rovnakom API (samostatná CA, samostatný server cert pre daný host, samotné klientské prístupy).

Ako dodatočná ochrana je designovaný IP whitelisting na úrovni cloud providera pre verejnú IP.

Prostredia: DEV, TEST, PREPROD, PROD

Samotný popis rozhrania je cez “Swagger” dokumentáciu, zaslanú separátne mimo DIZ.

2.6 Popis procesov

V tejto kapitole sú popísané procesy súvisiace s poskytnutím údajov zo SCA pre IS Greenpass service API alebo jeho komponenty v súlade s príslušnou časťou riešenie verifikácie digitálneho COVID preukazu autorizovanou osobou, ktorá používa aplikáciu OverPassSpecial.

Pri integrácii ide primárne o získanie dát o DCC zo zdrojovej aplikácie cez SCA API. Výmena dát medzi aplikáciami a zdrojmi dát bude prebiehať vo formáte JSON na REST rozhraní podľa štandardu OpenAPI 3+. Riešenie bude integrované na rozhrania NCZI, ktoré NCZI v čase zverejní vrátane príslušnej dokumentácie a budú potrebné pre realizáciu riešenia podľa odsúhlasených procesných scenárov.

Dáta majú formát podľa dokumentácie eHN.

2.6.1 Synchronizácia verejných kľúčov

Cieľom procesu je pravidelne aktualizovať verejné kľúče na strane OverPass Special aplikácie.

Aktéri:

- OverPassSpecial,
- IS Greenpass service API

Vstup procesu:

- Dostupnosť dátovej siete a funkčné prepojenie medzi SCA a BE IS Greenpass service API,
- Systém zistí neaktuálnosť kľúčov v rámci aplikácia a nastaveného cyklu pre synchronizáciu kľúčov voči SCA a BE IS Greenpass service API,

Výstup procesu:

- Aktualizované klúče na BE IS Greenpass service API.

2.6.2 Overenie digitálneho covid preukazu

Cieľom procesu je overenie covid preukazu príslušníkom Policajného Zboru SR.

Aktéri:

- OverPassSpecial,
- Greenpass service API
- NCZI BE (BackEnd)
- Príslušník MV SR

- Držiteľ covid preukazu

Vstup procesu:

- Covid preukaz obsahujúci QR kód
- Verejné kľúče štátov EU
- Rodné číslo

Výstup procesu:

- Overenie covid preukazu

2.7 Architektúra riešenia IS Greenpass service API

Návrh požiadaviek vychádza z potrieb služieb realizovaných ako MVP. Predpokladaná doba životnosti navrhovanej verzie je 12 mesiacov s ohľadom najmä na pandemickú situáciu spôsobnú koronavírusom.

Detailný popis riešenia bude dostupný v dokument DNR v súlade s pravidlami riadenia kvality QA v súlade s platnou legislatívnou SR a to najmä legislatívnymi úpravami pre riadenia štátnych IT projektov a primerane podľa charakteru projektu:

- Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS (od 1.5.2020),
- Vyhláška č.85/2020 Z.z. o riadení projektov (od 1.5.2020),
- Vyhláška č.179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS (od 30.6.2020).

2.7.1 Produkčné prostredie dgc-api.gov.sk

IS bude využívať infraštruktúrne služby (IaaS) Vládneho cloudu podľa možností Katalógu služieb Vládneho cloudu.

- Služby pripojenia do siete: Sieťové služby
- Služby výpočtového výkonu: Virtuálny server, 3x
- Architektúra CPU: x86-64, RISC
- Počet virtuálnych CPU: 4, 2x
- Veľkosť RAM: 8GB
- Systémový diskový priestor: 20 GB
- Server OS (navrhované verzie OS musia byť podporované výrobcom v čase nasadenia projektu do produkčnej prevádzky min. 2 roky podľa oficiálneho „End-of-support“ plánu dodávateľa):
- CentOS 8.3 (64-bit)

Prostredie	ID	Služba Vládneho cloudu (výber z katalógu služieb)	OS a verzia	Počet CPU	RAM (GB)	IS/modul
Produkčné	dgc-api-01	IaaS	Centos 8.3	2	8	DGC_BE
Produkčné	dgc-api-02	IaaS	Centos 8.3	2	8	DGC_BE
Produkčné	dgc-api-03	IaaS	Centos 8.3	2	8	DGC_BE
Produkčné	Dgc-mgmt-01	IaaS	Centos 8.3	1	4	DGC_BE

2.7.2 Testovacie a integračné prostredie dgc-api-fix.gov.sk

IS bude využívať infraštruktúrne služby (IaaS) Vládneho cloudu podľa možností Katalógu služieb Vládneho cloudu:

- Služby pripojenia do siete: Sieťové služby
- Služby výpočtového výkonu: Virtuálny server, 3x
- Architektúra CPU: x86-64, RISC
- Počet virtuálnych CPU: 4, 2x
- Veľkosť RAM: 8GB
- Systémový diskový priestor: 20 GB

- Server OS (navrhované verzie OS musia byť podporované výrobcom v čase nasadenia projektu do produkčnej prevádzky min. 2 roky podľa oficiálneho „End-of-support“ plánu dodávateľa):
- CentOS 8.3 (64-bit)

Prostredie	ID	Služba Vládneho cloudu (výber z katalógu služieb)	OS a verzia	Počet CPU	RAM (GB)	IS/modul
Testovacie	dgc-api-01	IaaS	Centos 8.3	2	8	DGCT_BE
Testovacie	dgc-api-02	IaaS	Centos 8.3	2	8	DGCT_BE
Testovacie	dgc-api-03	IaaS	Centos 8.3	2	8	DGCT_BE
Testovacie	Dgc-mgmt-01	IaaS	Centos 8.3	1	4	DGC_BE

2.7.3 Dátový model

Aplikácia v súlade s Nariadením Európskeho parlamentu a rady (EÚ) 2021/953 a technickými špecifikáciami publikovanými sieťou elektronického zdravotníctva ukladá v lokálnom úložisku mobilného zariadenia, kde natívna mobilná aplikácie beží, iba verejné kľúče.

Ukladanie verejných kľúčov v rámci v lokálnom úložisku mobilného zariadenia je nutnou podmienkou, aby aplikácia OverPassSpecial umožňovala off-line verifikáciu COVID preukazu.

Backend neukladá dáta o certifikátoch. Backend ukladá iba verejné kľúče potrebné na overenie pravosti certifikátov.

2.8 Komunikácia medzi IS GreenPass a SCA

2.8.1 Synchronizácia verejných kľúčov

Proces synchronizácie verejných kľúčov na úrovni IS Greenpass service API a SCA verified check services API.

2.8.2 Overenie covid preukazu príslušníkom Policajného Zboru SR

Proces pre overenie covid preukazu v aplikácii OverPass Special.

2.8.3 Frekvencia a objem komunikácie voči SCA

Popis komunikácie z hľadiska predpokladaného objemu a frekvencie volaní IS GreenPass ovplyvňujúcich komunikáciu s SCA podľa udalostí je zachytený v nasledujúcej tabuľke (predpoklad v špičke):

Udalosť	Predpokladaná početnosť
Získanie verejných kľúčov z SCA	Maximálne 1x za hodinu
Overenie na základe RČ (v závislosti od vybavenia oprávnených osôb)	10 000 – 30 000 za deň

Udalosti budú monitorované cez *Firebase Analytics* a počet použití veľmi závisí od penetrácie a správania sa používateľov, ktoré nie je možné presne predpovedať. V prípade kontroly počas hromadných podujatí alebo vydania veľkého počtu certifikátov za 1 deň môžu čísla a predpokladaná početnosť narásť 5 až 10 násobne.

Najväčšia početnosť volaní v rámci komunikácie najmä pri získaní záznamov o certifikátoch sa predpokladá medzi 06:00 – 20:00. S ohľadom na charakter a účel dokumentu je predpokladané použitie aj v dňoch pracovného pokoja a štátnych sviatkov.

2.9 Auditné logovanie

Logovania a zber udalostí z mobilnej aplikácie prebieha cez Firebase a podľa pravidiel Firebase. Nie sú logované žiadne osobné údaje a udalosti sú zbierané tak, aby bolo možné monitorovať používania krokov procesu, ktoré sa týkajú interakcie používateľa a aplikácie.

Doba archivovania logov je stanovená systémovým parametrom, default 6 mesiacov.

BE IS GreenPass používa štandardné aplikačné a systémové logy.

2.10 Testovacie scenáre

Testovacie scenáre budú zrealizované podľa dostupných dát-certifikátov v testovacom prostredí tak, aby boli preverené jednotlivé typy certifikátov a aj rôzne počty a typy certifikátov v rámci zoznamu certifikátov pre jedného užívateľa. Testovacie scenáre tvoria Prílohu č. 1 tejto Dohody.

2.11 Bezpečnosť IS GreenPass

Backend neukladá žiadne osobné údaje (data at rest). Komunikácia medzi BE IS GreenPass a SCA API je na báze mTLS.

2.12 Autentifikácia konečných užívateľov IS GreenPass

Používateľ – oprávnená osoba – aplikácie OverPassSpecial pristupuje k službám z aplikácie cez určený BE IS GreenPass na SCA API. Riadenie prístupov a distribúciu zariadení vykonáva MV SR prostredníctvom interných predpisov a pokynov.

Poskytovateľ zabezpečuje ochranu údajov v súlade s DIZ na úrovni API. Prevádzkovateľ zodpovedá za bezpečnosť spracovávaných údajov poskytnutých poskytovateľom, ktoré sú prenášané a spracovávané mimo API rozhranie. Konzument zodpovedá za oprávnenosť požiadaviek (requestov), ktoré sú na API Poskytovateľa zasielané z IS GreenPass.

Zodpovednosť za bezpečnosť údajov spracovávaných jednotlivými stranami (Poskytovateľom a Konzumentom) je definovaná rozhraním poskytovaného API Smarcert App.

2.13 Prístup na prostredia - certifikáty a kľúče

Pre komunikáciu s API SCA je potrebné využívať bezpečnostné certifikáty a kľúče, ktoré NCZI dodá MVSR vopred dohodnutým a zabezpečeným spôsobom, ktorý bude dohodnutý samostatne pre každé jedno prostredie..

3 Komunikačný plán

3.1 Popis rolí a zodpovednosti

Cieľom definovania komunikačného plánu je rozdelenie základných zodpovedností, komunikačných línií, eskalácií a údržby dokumentu. Role dodávateľa /konzument/ zahrnuté do rolí Konzumenta.

Rola	Konzument MVSR	Poskytovateľ NCZI
Prodct Owner		
Projektový manažér		
Hlavný biznis analytik		
Hlavný architekt alebo technický návrhár		
Integračný manažér		
Test manažér		
Prevádzka a infraštruktúra		
Bezpečnostný architekt		
Incident manažér		
Technický kontakt pre fyzickú výmenu kľúčov pre PROD		

prostredie (mTLS)		

3.2 Komunikačné procesy

Komunikačné procesy prebiehajú na úrovni projektového riadenia a zodpovedných garantov (rolí) na oboch stranách formou pravidelných stretnutí s intervalom 2 týždňov, resp. v závislosti od okolností a stavu úloh. Jednotlivé komunikačné procesy sú zhrnuté v nasledujúcej tabuľke.

Úroveň stretnutí	Komunikačný proces	Výstup
Projektoví manažéri	Návrh integračného zámeru a jeho úprav	Dohoda o integračnom zámere a jeho dodatok
Projektoví manažéri	Eskalácia problémov	Elektronický alebo papierový výstup k eskalácii problému
Projektoví manažéri	Integračné testovanie	Integračný protokol podpísaný projektovými manažérmi
Projektoví manažéri	Monitorovanie stavu integračných prác (odporúčaná periodicita raz mesačne)	Zápis zo stretnutia, elektronická alebo papierová statusová informácia
Prevádzka a infraštruktúra	Prepojenie infraštruktúry	Elektronická, alebo papierová statusová informácia o zriadení funkčného prepojenia infraštruktúry
Expertná komunikácia ohľadom biznis modelov	Zorchestrovanie služieb na úrovni biznis modelu	Integračný postup pri testovaní (prípadne úprava dokumentácie zúčastnených strán)
Test manažér	Integračné testovanie	Integračný protokol
Bezpečnosť	Definovanie požiadaviek, analýza, testy	Bezpečnostne požiadavky na výmenu informácií, na prístup a aplikáciu, bezpečnostné testovania, riziká,
Eskalácia na PM	1. stupeň	Zápis

4 Harmonogram

4.1 Popis harmonogramu

Aktivita	Vstup	Výstup	Dátum začiatku	Dátum Ukončenia	Závislosti aktivít	Zodpovedná osoba
Vypracovanie integračnej dokumentácie	Integračný manuál, Integračný zámer	Informácie v katalógu služieb, Integračný manuál poskytovanej služby, Model využívaných služieb, Návrh variantov pre naplnenie požiadaviek, Integračný technický návrh, Testovací plán, Protokol o pripravenosti technického návrhu	21.5.2021	3.6.2021	*Dokumentácia EÚ, Popis technických rozhraní vo finálnej verzii.*	Projektový manažér, Hlavný architekt alebo technický návrhár

Aktivita	Vstup	Výstup	Dátum začiatku	Dátum Ukončenia	Závislosti aktivít	Zodpovedná osoba
		integrácie				
Prepojenie testovacej infraštruktúry	Výstup predchádzajúcich aktivít	Špecifikácia prepojenia testovacej infraštruktúry, Protokol o pripravenosti testovacej infraštruktúry	21.5.2021	3.6.2021	Vypracovanie integračnej dokumentácie	Projektový manažér, Prevádzka a infraštruktúra
Príprava a vykonanie integračných testov	Výstupy predchádzajúcich aktivít Testovacie dáta	Testovacie scenáre a testovacie prípady integračného testovania, Protokol o ukončení integračných testov, Aktualizovaná relevantná dokumentácia integrácie (v prípade potreby)	31.5.2021	28.6.2021	Prepojenie testovacej infraštruktúry	Projektový manažér, Test manažér
Príprava a vykonanie používateľských akceptačných testov (UAT)	Výstupy predchádzajúcich aktivít	Testovacie scenáre a testovacie prípady používateľského akceptačného testovania (UAT), Protokol o ukončení používateľských akceptačných testov (UAT)	7.6.2021	28.6.2021	Príprava a vykonanie integračných testov	Projektový manažér, Test manažér
Zavedenie do prevádzky v produkčnej infraštruktúre, monitoring	Výstupy predchádzajúcich aktivít	Dohoda o úrovni poskytovaných služieb (SLA) a manažment post implementačných zmien, Akceptačný protokol o zavedení komponentov a integrácie do produkčného prostredia	28.6.2021	01.07.2021	Príprava a vykonanie používateľských akceptačných testov (UAT)	Projektový manažér

4.2 Nevyhnutné podmienky

Nevyhnutnými podmienkami integrácie subjektov pre naplnenie Dohody sú:

- dostupné API SCA na strane NCZI vo všetkých prostrediach (DEV, TEST, PROD),
- dostupná integračná platforma a back-office systémy na strane NCZI,
- dostupná technická špecifikácia poskytovaných služieb SCA (popis API, certifikáty a pod.),

- Platná legislatíva umožňujúca NCZI vydávanie a poskytovanie údajov o DCC pre MV SR
- Zmluva o spolupráci upravujúca niektoré práva a povinnosti NCZI a MV SR v súvislosti so sprístupňovaním certifikátov pre MV SR

4.3 Externé závislosti

Nie sú.

5 Mlčanlivosť a ochrana dôverných informácií

1. Subjekty tejto Dohody sa zaväzujú zachovávať mlčanlivosť o akýchkoľvek informáciách, materiáloch, dokumentácie poskytnutých resp. získaných v súvislosti s touto Dohodou ako aj s informáciami majúcimi charakter obchodného tajomstva (ďalej len súhrnne „dôverné informácie“) a sú povinné zabezpečiť ich ochranu pred ich vyzradením, únikom, poskytnutím a/alebo sprístupnením tretím osobám.
2. Subjekty tejto Dohody sú oprávnené poskytnúť tretej osobe dôverné informácie len s predchádzajúcim písomným súhlasom druhej strany - subjektu tejto Dohody, okrem prípadov, ak by povinnosť poskytnutia dôverných informácií tretej osobe vyplývala zo zákona alebo z právoplatného rozhodnutia príslušného štátneho orgánu, alebo je informácia poskytnutá odborným poradcom subjektov tejto Dohody, ktorí sú viazaní zákonnou povinnosťou mlčanlivosti (napr. advokáti, daňový poradcovia, audítori), a to v súvislosti s poskytovaním ich služieb dotknutému subjektu tejto dohody. Ostatné zákonné povinnosti mlčanlivosti ostávajú nedotknuté.
3. V prípade poskytnutia dôvernej informácie tretej osobe v súlade s ich zmluvným vzťahom, je subjekt tejto Dohody, ktorý poskytuje takúto informáciu, povinný zaviazať tretiu osobu povinnosťou zabezpečiť ochranu dôvernej informácie minimálne v rozsahu a podmienkami uvedenými v tejto Dohode.
4. Subjekty tejto Dohody sú povinné oboznámiť druhú stranu – subjekt tejto Dohody o porušení povinnosti mlčanlivosti bez zbytočného odkladu potom, čo sa o takomto porušení dozvie. Porušujúca strana – subjekt tejto Dohody je povinná bezodkladne vykonať opatrenia na zamedzenie porušovania povinnosti mlčanlivosti.

6 Záverečné ustanovenia

1. Táto Dohoda je vyhotovená v 3 vyhotoveniach, z ktorých jedno (1) vyhotovenia dostane MV SR, jedno (1) vyhotovenie dostane MIRRI a jedno (1) vyhotovenia NCZI. Táto Dohoda nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch strán - subjektov Dohody a účinnosť nasledujúci deň po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky, najskôr však dňom nadobudnutia účinnosti Zmluvy o spolupráci. Zverejnenie tejto Dohody v registri sa nepovažuje za porušenie mlčanlivosti.
2. Táto Dohoda sa uzatvára na dobu trvania Zmluvy o spolupráci.
3. Túto Dohodu je možné meniť a dopĺňať len písomnou dohodou oboch subjektov Dohody vo forme očíslovaných dodatkov.
4. Subjekty tejto Dohody sú povinné si písomne a bezodkladne navzájom oznamovať každú zmenu kontaktných údajov a/alebo kontaktnej osoby uvedených v tejto Dohode, najneskôr do 15 dní odo dňa kedy zmena nastala. Za týmto účelom nie je potrebné vyhotoviť dodatok k tejto Dohode.
5. Oprávnení zástupcovia oboch strán - subjektov tejto Dohody vyhlasujú, že túto dohodu uzavreli slobodne, vážne, určite a zrozumiteľne, nie v tiesni a za nápadne nevýhodných podmienok, rozumejú jej obsahu a na znak súhlasu s jej obsahom ju vlastnoručne podpísali.