

Dohoda o integračnom zámere spoločnosti Ministerstvo investícií, regionálneho rozvoja a informatizácie 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		Dátum	
Podpis		Podpis	

Projekt:	Integrácia aplikácie IS GreenPass na SmartCertApp
Dokument:	DIZ-MIRRI-NCZI-WalletApp-GreenPass-v1.0.docx
Verzia:	1.0
Dátum:	28.06.2021
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	24.06.2021	Upravené procesy	
0.4	25.6.2021	Pripomienkovanie a doplnenia dokumentu	
0.5	25.6.2021	Zpracovanie pripomienok	
0.6	27.06.2021	Pripomienkovanie a doplnenia dokumentu	
0.7	27.06.2021	Zpracovanie pripomienok	
1.0	28.6.2021	Finálny dokument	

Obsah

POUŽITÉ POJMY A SKRATKY	4
1 ÚVODNÉ USTANOVENIA.....	5
1.1 IDENTIFIKÁCIA SUBJEKTOV INTEGRAČNÉHO ZÁMERU.....	5
1.2 ZDÔVODNENIE A CIELE INTEGRAČNÉHO ZÁMERU	5
1.3 ROZPOČET	5
2 ROZSAH INTEGRÁCIE	6
2.1 ARCHITEKTÚRA RIEŠENIA SCA	6
2.2 BIZNIS ARCHITEKTÚRA DIGITÁLNEHO COVID PREUKAZU EÚ.....	7
2.3 APLIKAČNÁ ARCHITEKTÚRA DIGITÁLNEHO COVID PREUKAZU.....	8
2.4 TECHNOLOGICKÁ ARCHITEKTÚRA DIGITÁLNEHO COVID PREUKAZU EÚ	8
2.6 POPIS HLAVNÝCH SLUŽIEB VYUŽÍVANÝCH V PROCESOCH	10
2.7 POPIS PROCESOV	10
2.7.1 GreenPass - Import digitálneho COVID potvrdenia do aplikácie	10
2.9 KOMUNIKÁCIA MEDZI APLIKÁCIOU GREENPASS A SCA	12
2.9.1 Import digitálneho covid preukazu SK online	12
2.9.2 Stiahnutie PDF digitálneho covid preukazu SK online.....	13
2.9.3 Frekvencia a objem komunikácie voči SCA	13
2.10 AUDITNÉ LOGOVANIE	13
2.11 TESTOVACIE SCENÁRE	14
2.12 BEZPEČNOSŤ IS GREENPASS	14
2.13 AUTENTIFIKÁCIA KONEČNÝCH UŽÍVATEĽOV V APLIKÁCII GREENPASS.....	14
3 KOMUNIKAČNÝ PLÁN	14
3.1 POPIS ROLÍ A ZODPOVEDNOSTI.....	14
3.2 KOMUNIKAČNÉ PROCESY	16
4 HARMONOGRAM	16
4.1 POPIS HARMONOGRAMU	16
4.2 NEVYHNUTNÉ PODMIENKY.....	17
4.3 EXTERNÉ ZÁVISLOSTI	17
5 MLČANLIVOSŤ A OCHRANA DÔVERNÝCH INFORMÁCIÍ	18
6 ZÁVEREČNÉ USTANOVENIA	18

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.
DGC	Digital Green Certificate, digitálne zelené certifikáty.
MOA	Mobilná aplikácia.
BE	Backend, serverová časť informačného systému.
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.
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

1 Úvodné ustanovenia

1.1 Identifikácia subjektov integračného zámeru

Subjektmi Dohody o integračnom zámere sú Národné centrum zdravotníckych informácií (NCZI) a Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI) Konzumentom riešenia v rámci integrácie bude IS GreenPass, poskytovateľom riešenia bude IS Smart Cert App.

Subjekty Dohody	Rola	Správca (Gestor)	IS spadajúce pod Dohodu
	Konzument	MIRRI	<i>isvs_10804</i>
	Poskytovateľ	Národné centrum zdravotníckych informácií, so sídlom: Lazaretská 26, 811 09 Bratislava IČO: 00165387	<i>Smart Cert App</i>

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 testoch 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 a 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 GreenPass. Backend aplikácie GreenPass pre prístup bude umiestnený vo vládnom cloude.

Občan, ktorý chce využiť riešenie neprepojené a nevyužívajúce údaje použije natívnu mobilnú aplikáciu GreenPass (wallet app).

IS GreenPass podporuje dva najdôležitejšie prípady použitia digitálnych COVID preukazov EÚ:

- 1) **Medzinárodne akceptovaný dôkaz o vakcinácii, o negatívnom AG/PCR teste alebo o prekonaní choroby** – osoba potrebuje získať a v prípade potreby predložiť vakcinačný certifikát (osobe s alebo aj bez medicínskeho vzdelania). Tento dôkaz sa má dať využiť na národnej aj medzinárodnej úrovni.
- 2) **Digitálny preukaz, ktorý umožní kontinuálne poskytnutie zdravotnej starostlivosti** – osoba môže byť v situácii, že môže dostať vakcinačné dávky v rôznych krajinách a potrebuje sa preukázať informáciou o predošlej dávke poskytovateľov zdravotnej starostlivosti (ZS), ktorý ide podať druhú alebo ďalšiu dávku alebo ide poskytnúť ZS, kde je potrebná kontrola údajov o vakcinácii.

IS GreenPass má niekoľko aplikácií, ktoré sú vytvorené v súlade Projektovým zámerom a Projektový prístupom a príslušným katalógom požiadaviek, ktorý je prílohou Projektového zámeru:

- Mobilná aplikácia pre občana – držiteľa certifikátu alebo blízkych osôb (**GreenPass** / wallet app / iOS 13+ a Android 6+) v rozsahu:
 - import digitálnej verzie COVID preukaz EÚ naskenovaním QR kódu,
 - import digitálnej verzie COVID preukaz EÚ vložení kombinácie pre autentifikáciu osoby (identifikačné číslo a access code) (ak bude dostupné API a pripojenie na Internet),
 - uloženie digitálnej verzie COVID preukaz EÚ v mobilnom zariadení (wallet app),
 - certifikátu o vakcinácii (prvá dávka, druhá dávka),
 - certifikátu o vykonaní testu,
 - certifikátu o prekonaní ochorenia,
 - zobrazenie digitálnej verzie COVID preukaz EÚ na overenie pravosti certifikátu na mieste, kde dochádza k poskytovaniu služieb, ktoré si vyžadujú offline alebo aj online verifikovanie certifikátu (v rozsahu a v súlade s platnou metodikou):
 - QR kód a unikátny identifikátor COVID preukaz EÚ ,
 - QR kód a dáta COVID preukaz EÚ ,
 - Overenie používateľa cez 5-miestny PIN/TouchID/FaceID,

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 funkčnosť/služby.

Mobilná aplikácia GreenPass bude integrovaná:

Názov API rozhrania
Smart Cert App public 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 EÚ

Nasledujúci diagram znázorňuje architektúru biznis služieb DCC. Občan používa natívnu mobilnú aplikáciu (wallet), prostredníctvom ktorej bude môcť občan uložiť digitálnu verziu DCC vo svojom mobilnom zariadení a následne ju použiť na preukázanie sa oprávnenej osobe. Osoba oprávnené vykonávať overovanie platnosti a pravosti certifikátov používa aplikácie na overenie (verifier) platnosti a pravosti DCC predložených v papierovej alebo elektronickej podobe pre OVM, kde bude v rámci hygienických opatrení nutná kontrola.

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 **GreenPass**, ktorá je vytvorená tak, aby nebolo používanie dát a procesov DCC možné spojiť s inými procesmi, ktoré nesúvisia s riadením boja proti pandémiej spôsobenej koronavírusom,
- **Externé systémy eGOV** – ide o systém, ktoré cez API rozhranie poskytujú služby. Aplikácia **GreenPass** je integrovaná na:
 - Smart Cert App public api (Verejné API SCA)
- **Externé systémy** – systémy tretích strán, ktoré sú dôležité v procese publikovania aplikácií a ich sprístupneniu koncovým používateľom.

2.4 Technologická architektúra digitálneho COVID preukazu EÚ

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 DGC 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 DGC,
- nástroje pre pravidelné prevádzkové zálohovanie DGC.

Nasledujúci diagram zobrazuje Technologickú architektúru DGC:

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.

2.6 Popis hlavných služieb využívaných v procesoch

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.

Názov API rozhrania Smart Cert App	Popis
Smart Cert App public api	Autentifikácia používateľa a import COVID preukazov SK z SCA online.

Prostredia: DEV, TEST, PREPROD, PROD

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

2.7 Popis procesov

V tejto kapitole sú popísané procesy súvisiace s poskytnutím údajov zo SCA pre aplikáciu GreenPass prostredníctvom verejného API SCA.

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.

2.7.1 GreenPass - Import digitálneho COVID potvrdenia do aplikácie

Digitálne COVID potvrdenie môže existovať tak v listinnej, ako aj elektronickej podobe. Pre uchovávanie Digitálnych COVID potvrdení slúži Aplikácia GreenPass vytvorená v súlade s požiadavkami a Nariadením Európskeho parlamentu a rady (EÚ) 2021/953, ktorá umožňuje používateľovi pridať si svoje potvrdenia alebo aj potvrdenia svojich blízkych a to buď skenovaním alebo online.

Skenovanie vyžaduje, aby mal občan k dispozícii zobrazený QR kód buď na papieri alebo na obrazovke a zadal overovací prvok.

Predpokladom pre pridávanie COVID preukazu EÚ online je access code, ktorý generuje SCA; ak ho občan nedostal proaktívne, musí si oň požiadať na samoobslužnom portáli. Zadaním prvkov access code a rodné číslo je možné potvrdenie uložiť. Aplikácia zároveň v online režime umožňuje overenie platnosti potvrdenia, pričom používateľ sa sám rozhodne, či si neplatné potvrdenie ponechá, alebo zmaže.

Aktéri:

- Občan,
- GreenPass,
- SCA,
- GreenPass Service API (BackEnd)

Vstup procesu:

- Nainštalovaná aplikácia,
- Povolené používanie fotoaparátu v aplikácii,
- Vygenerovaný DCC v SCA,
- Vygenerovaný a prijatý access code,
- Napojenie na verejné API SCA,
- Zadaná požiadavka na samoobslužnom portáli

Výstup procesu:

- Pridané potvrdenie skenovaním,
- Online pridanie potvrdenia.

2.9 Komunikácia medzi aplikáciou GreenPass a SCA

2.9.1 Import digitálneho covid preukazu SK online

Proces importu covid preukazu do aplikácie GreenPass on-line volaním Smart Cert App public API.

2.9.2 Stiahnutie PDF digitálneho covid preukazu SK online

Proces stiahnutie PDF covid preukazu EÚ do aplikácie GreenPass on-line volaním Smart Cert App public API.

2.9.3 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 certifikátov osoby v online režime	10 000 – 20 000 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.

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.

2.10 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 pri importe, používaní a zrušení certifikátov.

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

2.11 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.

2.12 Bezpečnosť IS GreenPass

Mobilná aplikácie pre držiteľa certifikátu ukladá iba údaje so súhlasom osoby. Mobilná aplikácia je navrhnutá tak, aby splnila odporúčania a kritériá MASVS-L2. Komunikácia medzi aplikáciou a BE Greenpass service API je realizovaná cez HTTPS. Poskytovateľ zabezpečuje ochranu údajov v súlade s DIZ na úrovni API. Konzument zodpovedá za bezpečnosť spracovávaných údajov poskytnutých poskytovateľom, ktoré sú prenášané a spracovávané mimo API rozhranie. Súčasne konzument zodpovedá za bezpečnosť 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 SCA. Zodpovednosť za bezpečnosť a ochranu poskytnutých údajov na úrovni API SCA zabezpečuje Poskytovateľ. Údaje mimo informačný systém SCA, ktoré boli poskytnuté formou API SCA pre aplikáciu GreenPass ako aj do systému IS GreenPass sú v zodpovednosti Konzumenta.

V prípade identifikácie bezpečnostného incidentu súvisiaceho s kybernetickou bezpečnosťou je potrebné eskalovať informácie manažérovi kybernetickej bezpečnosti NCZI. V súvislosti s incidentami ohľadom narušenia bezpečnosti osobných údajov je potrebné kontaktovať DPO oboch strán.

2.13 Autentifikácia konečných užívateľov v aplikácii GreenPass

Používateľ – držiteľ certifikátu - sa pre prístup k online verzii autentifikuje dvojicou údajov identifikačné číslo osoby a access kód, ktorý získava v procese pri registrácii na očkovanie alebo dodatočne v súlade s procesmi Samoobslužného portálu.

Používateľ sa v aplikácii overuje zadaním 5-miestneho PIN kódu, ktorý môže byť doplnený o biometrické overenie vo forme TouchID, alebo FaceID. Vytvorenie PIN je podmienkou ďalšieho používania aplikácie, bez tohto kroku nie je možné skenovať, ani ukladať covid preukazy získané napojením na verejné API SCA.

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 /konzumenta/ zahrnuté do rolí Konzumenta.

Rola	Konzument MIRRI	Poskytovateľ NCZI
Projektový manažér		
Hlavný biznis analytik		
Hlavný architekt alebo technický návrhár		
Integračný manažér		
Test manažér		
Prevádzka a infraštruktúra		
Bezpečnostný architekt		
Incident manažér		

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 integrácie	21.5.2021	3.6.2021	<i>Dokumentácia EÚ, Popis technických rozhraní vo finálnej verzii.</i>	Projektový manažér, Hlavný architekt alebo technický návrhár
Prepojenie testovacej infraštruktúry	Výstup predchádzajúcich aktivít	Špecifikácia prepojenia testovacej infraštruktúry,	21.5.2021	3.6.2021	Vypracovanie integračnej dokumentácie	Projektový manažér, Prevádzka a

Aktivita	Vstup	Výstup	Dátum začiatku	Dátum Ukončenia	Závislosti aktivít	Zodpovedná osoba
		Protokol o pripravenosti testovacej infraštruktúry				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.),
- pravidlá pre používanie certifikátov platné v SR a EÚ
- Platná legislatíva umožňujúca NCZI vydávať DCC

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 zaviazat' 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 2 vyhotoveniach, z ktorých jedno (1) vyhotovenie dostane MIRR 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 (ďalej len „register“). Zverejnenie tejto Dohody v registri sa nepovažuje za porušenie mlčanlivosti.
2. Táto Dohoda sa uzatvára na dobu určitú do 30.6.2022.
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.