

Elektronické služby spracovania bezpečnostných spisov NBÚ - malé zlepšenie eGov služieb

dátum
Tento dokument obsahuje x strán

Obsah

- 1 Základné informácie
- 1.1 Prehľad
- 1.2 Dôvod
- 1.3 Rozsah
- 1.4 Použité skratky a značky
- 2 Manažérske zhrnutie
- 2.1 Motivácia
- 2.2 Popis aktuálneho stavu
- 2.2.1 Legislatíva
- 2.2.2 Architektúra
- 2.2.3 Prevádzka
- 2.3 Alternatívne riešenia
- 2.3.1 Alternatíva A – „Názov“
- 2.3.2 Alternatíva B – „Názov“
- 2.4 Popis budúceho stavu
- 2.4.1 Legislatíva
- 2.4.2 Architektúra
- 2.4.3 Prevádzka
- 2.4.4 Ekonomická analýza

Zoznam tabuliek

- Tabuľka 1 Základné informácie - zhrnutie
- Tabuľka 2 Skratky a značky
- Tabuľka 3 Motivácia – budúci stav
- Tabuľka 4 Legislatíva – aktuálny stav
- Tabuľka 5 Biznis architektúra - aktuálny stav
- Tabuľka 6 Architektúra informačných systémov - aktuálny stav
- Tabuľka 7 Technologická architektúra - aktuálny stav
- Tabuľka 8 Bezpečnostná architektúra - aktuálny stav
- Tabuľka 9 Prevádzka - aktuálny stav
- Tabuľka 10 Legislatíva - budúci stav
- Tabuľka 11 Biznis architektúra – budúci stav
- Tabuľka 12 Architektúra informačných systémov - budúci stav
- Tabuľka 13 Technologická architektúra - budúci stav
- Tabuľka 14 Implementácia a migrácia
- Tabuľka 15 Bezpečnostná architektúra - budúci stav
- Tabuľka 16 Prevádzka - budúci stav
- Tabuľka 17 Ekonomická analýza - budúci stav

1. Prehľad

Tabuľka 1 Základné informácie - zhrnutie

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy	
<p>Navrhovaný projekt „Elektronické služby spracovania bezpečnostných spisov Národného bezpečnostného úradu“ sa zameriava na vytvorenie IS pre elektronizáciu služieb NBÚ v oblasti ochrany utajovaných skutočností (OUS) a interných procesov NBÚ súvisiacich s bezpečnostnými previerkami fyzických osôb a právnických osôb (podnikateľov). Tento IS prispieva k plneniu cieľov NKIVS a vytvára predpoklady na lepšiu správu uvedenej agendy NBÚ minimálne nasledovnými spôsobmi:</p> <ul style="list-style-type: none">• vytvorením nových elektronických služieb pre podnikateľov, občanov a OVM v uvedenej oblasti,• elektronizáciou a automatizáciou súvisiacich interných procesov a teda ich zefektívnením a zrýchlením,• integráciou na registre VS. <p>Ide najmä o procesy súvisiace:</p> <ul style="list-style-type: none">• s autorizáciou osôb pozostávajúcej najmä z:<ul style="list-style-type: none">• bezpečnostnej previerky fyzických osôb v súvislosti s oprávnením oboznamovať sa s utajovanými skutočnosťami (US),• vydávania certifikátov o bezpečnostnej previerke fyzickej osoby pre oboznamovanie sa s utajovanými skutočnosťami EÚ a NATO,• bezpečnostnej previerky podnikateľov v súvislosti s priemyselnou bezpečnosťou,• vydávania certifikátov podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami EÚ a NATO,• skúšky bezpečnostného zamestnanca, školenia bezpečnostného zamestnanca a poučenia oprávnených osôb.• so získavaním údajov z referenčných registrov iných OVM,• s poskytovaním údajov z IS NBÚ pozostávajúce najmä z:<ul style="list-style-type: none">• vydávania metodických postupov a usmernení,• poskytovaním informácií podľa osobitných predpisov.	
Prijímateľ/partner národného projektu a dôvod jeho určenia	
<p>Národný bezpečnostný úrad je v zmysle zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov ústredným orgánom štátnej správy, ktorý spravuje úseky OUS, dôveryhodných služieb (DS) a kybernetickej bezpečnosti (KB).</p>	
Príslušnosť národného projektu k relevantnej časti PO7 OPII	<p>Špecifický cieľ 7.3: Zvýšenie kvality, štandardu a dostupnosti eGovernment služieb pre občanov.</p> <p>Špecifický cieľ 7.4: Zvýšenie kvality, štandardu a dostupnosti eGovernment služieb pre podnikateľov.</p>
Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu	<p>Na tento projekt 4 000 721 EUR (s DPH).</p>

2. Dôvod

Dôvodom vypracovania tejto ŠU je posúdenie uskutočniteľnosti, výhodnosti podmienok a vytvorenie predpokladov pre realizáciu projektu a jeho financovania z prostriedkov dopytovej výzvy č. OPII-2019/7/5-DOP „Malé zlepšenie eGov služieb“. Riešenie bude zapadať do celkovej stratégie budovania IS v gescii NBÚ.

Hlavným dôvodom vypracovania tejto ŠU a cieľom celého projektu je vybudovanie „IS spracovania bezpečnostných spisov NBÚ“ (IS SBS NBÚ), ktorý bude poskytovať fyzickým a právnickým osobám (podnikateľom) elektronické služby, ktoré dnes nie sú plne elektronizované. Uvedený cieľ bude dosiahnutý vytvorením a nasadením IS SBS NBÚ ako aj jeho prepojením so spoločnými modulmi, registrami a informačnými systémami iných inštitúcií verejnej správy. V aktuálnom stave totižto prebieha spracovanie agendy OUS a bezpečnostných spisov v manuálnom stave bez podpory elektronických služieb, ktoré by umožnili efektívne podávanie elektronických žiadostí zo strany občanov a podnikateľov a rovnako tak aj efektívne a rýchle elektronické spracovanie na strane pracovníkov NBÚ.

ŠU poskytuje vyhodnotenie uskutočniteľnosti zámeru vytvorenia IS SBS NBÚ.

ŠU realizuje nasledovný typ zlepšenia (aktivity OPII): "B. Zavedenie inovatívnych elektronických služieb VS pre občanov a podnikateľov."

Ďalšími cieľmi dlhodobej vízie NBÚ sú:

- zníženie administratívneho zaťaženia občanov a podnikateľov, ale aj úradníkov pri vybavovaní záležitostí v agende bezpečnostných previerok NBÚ a umožnenie elektronického podania kompletnej žiadosti, vrátane jej prílohy s mimoriadne citlivými údajmi, ktorú dnes nie je možné podať prostredníctvom portálu slovensko.sk,
- zabezpečenie jednotného výkonu procesov a skrátenie času vybavovania tejto agendy,
- zabezpečenie plnej elektronizácie procesov NBÚ v rámci agendy bezpečnostných previerok,
- prepojenie existujúcich registrov, vytvorenie nových potrebných registrov a zabezpečenie ich použiteľnosti na právne úkony,
- vybudovanie kľúčových nástrojov pre poskytovanie elektronických služieb NBÚ,
- vytvorenie spoločnej zabezpečenej infraštruktúry pre eGovernment a podporné činnosti,
- vybudovanie zdrojového registra NBÚ, ktorý bude obsahovať špecifické dáta, ktoré sú výhradne v kompetencii NBÚ,
- umožnenie elektronického spracovávania utajovaných skutočností stupňa utajenia „Dôverná“ vrátane.

Riešenie priamo nadväzuje na nasledujúce strategické dokumenty:

- národný program Koncepcia informatizácie verejnej správy,
- schválené strategické priority Národnej koncepcie informatizácie verejnej správy,
- pozičný dokument Európskej komisie k vypracovaniu Partnerskej dohody a programov na Slovensku na roky 2014-2020, kde jednou z piatich priorit je moderná a odborná verejná správa,
- „Návrh centralizácie a rozvoja dátových centier v štátnej správe“, ktorý bol schválený uznesením vlády SR č. 247/2014.

Dôvodom pre vypracovanie tejto štúdie uskutočniteľnosti a projektu je predovšetkým riešenie nižšie uvedených problémov a zároveň naplnenie uvedených príležitostí súčasnej doby:

- Problém: Aktuálny stav neumožňuje elektronické podávanie žiadostí o bezpečnostnú previerku fyzickej osoby a žiadostí o bezpečnostnú previerku podnikateľov v komplexnom tvare, t. j. vrátane jej prílohy s mimoriadne citlivými údajmi, ktorú dnes nie je možné podať prostredníctvom portálu slovensko.sk (cca 10 000 ks ročne).
 - Problém: Spracovanie na strane NBÚ prebieha manuálnym spôsobom bez podpory IS (spracováva sa cca 300 záznamov denne). Aktuálne každý záznam prechádza manuálnym prenosom cez 4 rôzne systémy, resp. skôr aplikácie (prenos do, resp. z podateľne, dožiadanie a spracovanie spisu, podpísanie, odoslanie), ktoré fungujú bez vzájomnej integrácie.
 - Problém: Získavanie informácií z iných registrov VS prebieha manuálnym spôsobom (napr. prostredníctvom portálu oversi.sk alebo manuálnym dožiadanim odpisu z registra trestov) bez akejkoľvek existujúcej integrácie typu systém-systém.
 - Problém: Aktuálny stav neumožňuje efektívnu realizáciu manažmentu práce a jej kontroly, strojové (fulltext) vyhľadávanie v existujúcich spisoch (ide o scany vo formáte .jpg), nasadenie analytických a report nástrojov.
 - Problém: Nie všetky postupy a bezpečnostné opatrenia v organizácii dosahujú potrebnú úroveň vyspelosti, ktorá je nevyhnutná pre znižovanie bezpečnostných rizík na prijateľnú úroveň.
 - Problém: Infraštruktúra v súčasnosti obsahuje izolované a zastarané prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne.
 - Problém: Aktuálny systém zabezpečenia a ochrany nespĺňa všetky požiadavky legislatívy (najmä zákona o kybernetickej bezpečnosti v oblasti riadenia prístupu, riadenia kontinuity prevádzky a bezpečnostného monitoringu kybernetických bezpečnostných incidentov).
 - Problém: Morálna, technická, technologická aj softvérová zastaranosť. Pôvodný Informačný systém Previerka bol vyvinutý v roku 2006 a nasadený do ostrej prevádzky v roku 2007. S minimálnymi aktualizáciami tak funguje nepretržite viac než 12 rokov. Pôvodný dodávateľ už neexistuje. Je mimoriadne komplikované, často až nemožné implementovať do systému zmeny a nové požiadavky vyplývajúce či už z legislatívnych zmien alebo zo zmien pracovných postupov. Sieťová infraštruktúra, na ktorej systém beží je ešte z rokov 2001 až 2002. Neposkytuje dostatočné kapacitné možnosti a zároveň nespĺňa nové bezpečnostné požiadavky.
 - Problém: NBÚ aktuálne dispobuje iba jediným príslušníkom, ktorý má historické skúsenosti a potrebné know-how ohľadom správy a údržby aktuálneho systému, čo extrémne zvyšuje mnohé riziká spojené s činnosťou IS Previerka a najmä s možnou nedostupnosťou aktuálneho systému v prípade výpadku alebo choroby tohto príslušníka.
 - Problém: Frontend systému bol vyvinutý ako nadstavba nad Microsoft Office 2003 a postavený na 32 bitovej platforme (MS SQL Server 2005, Windows Server 2003). Toto softwarové prostredie dnes už nevyhovuje po funkčnej, výkonnostnej ani bezpečnostnej stránke.
 - Problém: Súčasný systém iba generuje a uchováva registratúrne čísla písomností, nie je však systémom, ktorý by plne zabezpečoval manažment a workflow pracovných postupov a bol v súlade s platnou legislatívou (súlad s ňou sa zabezpečuje inými prostriedkami a zbytočne duplicitne v papierovej a elektronickej forme).
 - Problém: Obmedzená funkcionálna aktuálneho procesu spracovania bezpečnostných spisov sa vyvažuje ľudskými činnosťami, kopírovaním, prenášaním a systematizovaním záznamov, čo zvyšuje riziko chybovosti a vnáša riziko ľudského faktoru.
 - Problém: Súčasný systém nie je možné efektívne integrovať na registre iných OVM.
-
- Príležitosť: Umožnenie podávania elektronických žiadostí fyzickým a právnickým osobám ohľadom bezpečnostných previerok v komplexnom tvare, t. j. vrátane prílohy s mimoriadne citlivými údajmi.
 - Príležitosť: Možnosť plnej elektronizácie agendy bezpečnostných spisov NBÚ.
 - Príležitosť: Možnosť efektívneho a rýchleho získavania údajov z registrov iných OVM prostredníctvom integrácie na tieto registre.

- Príležitosť: Možnosť nasadenia vyhľadávacích (fulltext), analytických a report nástrojov, vzhľadom na skutočnosť, že nový systém bude pracovať so štruktúrovanou formou údajov.
- Príležitosť: Možnosť nasadenia nástrojov pre manažment úloh a kontrolu ich plnenia.
- Príležitosť: Možnosť nasadenia moderných, pokročilých bezpečnostných opatrení a sofistikovaných bezpečnostných mechanizmov, ktoré budú zaisťovať požadovanú úroveň ochrany všetkých bezpečnostne relevantných informačných aktív do stupňa utajenia „Dôverné“ vrátane. Zároveň možnosť zabezpečenia aj celej IKT infraštruktúry, vrátane nežiadúceho elektromagnetického vyžarovania. Tým bude možné reflektovať vývoj v oblasti kybernetických hrozieb a kybernetickej bezpečnosti.
- Príležitosť: Možnosť vyriešenia všetkých vyššie uvedených problémov týkajúcich sa morálnej zastaranosti, nedostatočnej funkcionality alebo kapacity, prípadne iných technických problémov.
- Príležitosť: Možnosť zabezpečiť súlad nového systému s legislatívnymi požiadavkami.

2.0.1. Negatívny stav v prípade, ak projekt nebude realizovaný:

V prípade, že tento projekt nebude zrealizovaný, nebude možné, vyššie uvedenú agendu bezpečnostných spisov a s ňou súvisiace služby NBÚ (uvedené v prílohe tejto ŠU), komplexne poskytovať elektronickou formou, vrátane podávania a spracovania mimoriadne citlivej prílohy. Zároveň nebude možné zabezpečiť plný súlad s požiadavkami legislatívy (najmä zákon o OUS, zákon o eGovernmente, zákon o ochrane OÚ a zákon o kybernetickej bezpečnosti).

3. Rozsah

Predložená ŠU vychádza z architektonického rámca verejnej správy a nadväzuje na Architektonickú víziu verejnej správy. Cieľom tejto ŠU je poskytnúť strategický rámec, plánovaný rozsah, očakávaný časový harmonogram, závislosti na iné projekty a odporúčania ďalších aktivít, z ktorých treba pri realizácii implementácie elektronických služieb NBÚ vychádzať.

ŠU sa vo svojom rozsahu zameriava najmä na tieto základné služby a procesy:

- bezpečnostná previerka fyzickej osoby,
- bezpečnostná previerka právnickej osoby (podnikateľa),
- metodické riadenie v oblasti OUS (vydávanie metodických postupov a usmernení),
- poskytovanie informácií z bezpečnostných spisov podľa osobitných predpisov.

ŠU je súčasťou predprojektov prípravy na vybudovanie IS SBS NBÚ. Predkladá víziu cieľového riešenia informatizácie jednotlivých agend NBÚ a identifikuje konkrétne elektronické služby, ktoré je potrebné prostredníctvom IS SBS NBÚ implementovať, aby príslušné eGovernment služby mohli byť poskytované všetkým stranám – teda občanom, podnikateľom, odbornej verejnosti a celej verejnej správe.

ŠU sa zameriava najmä na implementáciu agendového IS SBS NBÚ pre spracovávanie bezpečnostných spisov NBÚ a jeho integráciu na registre iných OVM. IS SBS NBÚ umožní elektronické spracovávanie utajovaných skutočností stupňa utajenia „Dôverné“ vrátane a zároveň zabezpečí ochranu voči pokročilým bezpečnostným hrozbám a nežiadúcemu elektromagnetickému vyžarovaniu.

Z hľadiska NBÚ uvedené služby spadajú pod nasledovný úsek verejnej správy:

- U00207 – Ochrana utajovaných skutočností, šifrová služba a elektronický podpis.

Vymedzenie subjektov, ktorých sa dotýka navrhované riešenie projektu:

- Problém podávania elektronických žiadostí o bezpečnostnú previerku sa týka najmä fyzických osôb a právnických osôb (podnikateľov).
- Problém umožnenia efektívneho elektronického spracovávanie bezpečnostných spisov NBÚ, vrátane efektívneho manažmentu a kontroly úloh, nasadenia analytických a report nástrojov a elektronickej integrácie na registre iných OVM, sa priamo dotýka NBÚ a jeho zamestnancov.
- Problém výmeny a zdieľania informácií z bezpečnostných spisov NBÚ sa dotýka všetkých ostatných OVM, ktoré potrebujú tieto informácie pre ich vlastnú činnosť a rozhodovanie.

Aktér	Rola	ISVS
fyzická osoba	žiadateľ o službu (žiadosť o bezpečnostnú previerku)	IS SBS NBÚ
právnická osoba (podnikateľ)	žiadateľ o službu (žiadosť o bezpečnostnú previerku)	IS SBS NBÚ
pracovník NBÚ	spracovateľ žiadosti	IS SBS NBÚ
vedúci pracovník NBÚ	manažment a kontrola úloh, spracovanie analýz a reportov	IS SBS NBÚ
iné OVM	výmena a zdieľanie informácií	IS SBS NBÚ

4. Použité skratky a značky

Tabuľka 2 Skratky a značky

Skratka / Značka	Vysvetlenie
CA	Certifikačná autorita
CMS	Redakčný systém (Content management system)
CSRÚ	Centrálne správa referenčných údajov
DFŠ	Detailná funkčná špecifikácia
DLP	Ochrana proti strate dát (Data loss prevention)
DS	Digitálna služba
ES	Elektronické služby
EÚ	Európska únia
GDPR	General data protection regulation
HSM	Hardvérový bezpečnostný modul (Hardware security module)
HW	Hardvér
IAM	Manažment identít a prístupov (Identity and access management)
IB	Informačná bezpečnosť
IKT	Informačno-komunikačné technológie
IS	Informačný systém
IS PEP	Informačný systém pre platby a evidenciu správnych a súdnych poplatkov
IS SBS	Informačný systém spracovávania bezpečnostných spisov
ISVS	Informačný systém verejnej správy
KB	Kybernetická bezpečnosť
KPI	Kľúčový ukazovateľ výkonnosti (Key Performance Indicator)
MCA	Multikriteriálna analýza
NASES	Národná agentúra pre sieťové a elektronické služby
NBÚ	Národný bezpečnostný úrad
NEV	Nežiadúce elektromagnetické vyžarovanie
NKIVS	Národná koncepcia informatizácie verejnej správy
OPII	Operačný program integrovaná infraštruktúra
OUS	Ochrana utajovaných skutočností
OVM	Orgány verejnej moci
PKI	Infraštruktúra správy verejných kľúčov (Public key infrastructure)
RPO	Recovery point objective
RTO	Recovery time objective

SR	Slovenská republika
SW	Softvér
ŠU	Štúdia uskutočniteľnosti
ÚPVS	Ústredný portál verejnej správy
US	Utajované skutočnosti
UX	Používateľská skúsenosť (User experience)
VS	Verejná správa

Predložená ŠU sa zameriava na vytvorenie IS spracovávanie bezpečnostných spisov NBÚ v oblasti ochrany utajovaných skutočností a súvisiacich interných procesov. Ide najmä o procesy súvisiace s autorizáciou fyzických a právnických osôb (podnikateľov), budovaním bezpečnostného povedomia, vydávaním metodických postupov a usmernení, efektívnym získavaním informácií od iných OVM (integráciou na registre týchto OVM) a efektívnou výmenou a zdieľaním informácií s inými OVM, ktoré ich potrebujú pre realizáciu svojich úloh a činností.

Súčasný stav na úseku agendy spracovávanie bezpečnostných spisov NBÚ nie je z pohľadu občana a podnikateľa veľmi priaznivý. V súčasnosti nie je možné, zo strany fyzických a právnických osôb (podnikateľov), elektronicky podávať úplné žiadosti v štruktúrovanej forme týkajúce sa agendy bezpečnostných previerok, t.j. vrátane prílohy s mimoriadne citlivými údajmi. Rovnako dnes neexistuje proces plne elektronického spracovania na strane NBÚ, ktorý by následne umožňoval efektívny manažment úloh a ich kontrolu, nasadenie vyhľadávacích, analytických a report nástrojov a zároveň integráciu na registre iných OVM. Proces spracovania trvá neúmerne dlho a výstupom nie je právne relevantná elektronická forma, ale prevažne neštruktúrovaný papierový dokument. Cieľové riešenie bude umožňovať plne elektronickú formu komunikácie a výmenu dokumentov, vrátane priebežného zisťovania stavu podania.

Výsledkom projektu by teda malo byť zjednodušenie administratívy občanov, podnikateľov a OVM, ako aj skrátenie konania pri vybavovaní záležitostí vo vzťahu k NBÚ. Zároveň bude umožnené pracovníkom NBÚ pracovať s plne elektronickými dátami, nad ktorými bude možné realizovať požadované vyhľadávania, analýzy a poskytovať reporty a štatistické údaje.

Projekt v čo najväčšej možnej miere využíva už existujúce komponenty eGovernmentu ako aj princípy NKIVS a jednotlivých schválených strategických priorít NKIVS. Zároveň zohľadňuje aj požiadavky zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, nakoľko budovaný IS bude certifikovaným technickým prostriedkom (systémom určeným na vytváranie, spracúvanie, prenos, ukladanie a ochranu utajovaných skutočností), ktorý umožní spracovávať utajované skutočnosti až do stupňa utajenia „Dôverné“ vrátane.

Hlavnými cieľmi projektu je:

- zavedenie plne elektronických služieb NBÚ v oblasti bezpečnostných previerok, ktoré zabezpečia občanom, podnikateľom a OVM komplexné vybavovanie záležitostí vo vzťahu k NBÚ a sprístupnenie služieb, ktoré umožnia podávanie žiadostí a následných dokumentov pri vybavovaní záležitostí vo vzťahu k NBÚ,
- zaistenie používania elektronických služieb NBÚ v podmienkach eGovernmentu, a to:
 - vytvorením podmienok pre občanov a podnikateľov, kedy nebude nutné pre potreby procesov eGovernment služieb dokladať informácie, ktoré už sú evidované v IS SBS NBÚ, prípadne v referenčných registroch,
 - komplexným riešením elektronického obehu dokumentov pre služby NBÚ zabezpečujúce zjednodušenie administratívnych činností a odstránenie neefektívnej práce s manuálnym obehom dokumentov, zefektívnenie komunikácie a pod.,
- vybudovanie integrovaného IS SBS NBÚ, a to:
 - vytvorenie portálu a rozhrania, ktoré umožní podávanie požiadaviek pri vybavovaní záležitostí vo vzťahu k NBÚ,
 - implementácia systému pre registratúru a manažment dokumentov z dôvodu zabezpečenia efektívnej práce s dokumentmi,
 - implementácia manažmentu a kontroly procesov týkajúcich sa vybavovania agendy bezpečnostných spisov NBÚ a súvisiacich interných procesov,
 - implementácia vyhľadávacích, analytických a report nástrojov,
 - umožnenie spracovania bezpečnostných spisov v režime utajenia do stupňa utajenia „Dôverné“ vrátane, t.j. nasadenie príslušných bezpečnostných opatrení a prostriedkov,
 - zabezpečenie sieťovej infraštruktúry systému voči pokročilým bezpečnostným hrozbám a nežiadúcemu elektromagnetickému vyžarovaniu.

Projekt je plne v súlade s princípmi a požiadavkami dopytovej výzvy č. OPII-2019/7/5-DOP „Malé zlepšenie eGov služieb“, nakoľko elektronizuje služby pre fyzické a právnické osoby (podnikateľov) v oblasti bezpečnostných previerok.

V súlade s prílohou č. 14 ŽoNFP v rámci dopytovej výzvy ide o podporu nasledovnej e-služby v rámci e-Government benchmarku: Začatie podnikania - 1.5 Konkrétne aktivity: "Konkrétne znalosti týkajúce sa konkrétnej profesie. Táto služba sa týka preukazovania (napríklad prostredníctvom diplomu), že podnikateľ je schopný a vyškolený na vykonávanie konkrétnej profesie."

Zároveň ide o riešenie ŽS, ktorá je súčasťou 25-tich prioritných životných situácií, konkrétne o: „Začatie podnikateľskej činnosti, priebeh podnikateľskej činnosti a ukončenie podnikateľskej činnosti“.

V tomto prípade ide o možnosť podnikateľa realizovať zákazky, pri ktorých dochádza k oboznamovaniu sa s utajovanými skutočnosťami, alebo k vytváraniu utajovaných skutočností. Za týmto účelom je potrebné preukázať, že podnikateľ má vydané osvedčenie o bezpečnostnej previerke.

ŠU realizuje nasledovný typ zlepšenia (aktivity OPII): "B. Zavedenie inovatívnych elektronických služieb VS pre občanov a podnikateľov."

Náklady na riešenie predstavujú výšku 4.000.721,- eur.

5. Motivácia

Tabuľka 3 Motivácia – budúci stav

Súhrnný popis
<p>V súčasnosti nie je možné, zo strany fyzických a právnických osôb (podnikateľov), elektronicky podávať úplné žiadosti v štruktúrovanej forme týkajúce sa agendy bezpečnostných previerok, t.j. vrátane prílohy s mimoriadne citlivými údajmi.. Rovnako dnes neexistuje proces plne elektronického spracovania na strane NBÚ, ktorý by následne umožňoval efektívny manažment úloh a ich kontroly, nasadenie vyhľadávacích, analytických a report nástrojov a zároveň integráciu na registre iných OVM.</p> <p>Realizáciou projektu „Elektronické služby spracovania bezpečnostných spisov NBÚ“, teda vytvorením a nasadením IS SBS NBÚ ako aj jeho prepojením so spoločnými modulmi ÚPVS a informačnými systémami iných inštitúcií verejnej správy, sa dosiahne súlad s požiadavkami pre elektronický výkon štátnej správy. Úspešnou realizáciou nastane:</p> <ul style="list-style-type: none"> • zníženie administratívneho zaťaženia občanov a podnikateľov (už nebude nutné prílohu žiadosti zasielať separátnym spôsobom osobne alebo poštou), ale aj úradníkov pri vybavovaní záležitostí v agende bezpečnostných previerok NBÚ a umožnenie elektronického podania kompletnej žiadosti, vrátane jej prílohy, ktorú dnes nie je možné podať prostredníctvom portálu slovensko.sk, • zabezpečenie jednotného a opakovateľného postupu v rámci procesov riešenia bezpečnostných previerok a skrátenie času vybavovania agendy bezpečnostných spisov, • zabezpečenie elektronizácie procesov bezpečnostných previerok NBÚ a umožnenie elektronického spracovania utajovaných skutočností do stupňa utajenia „Dôverné“ vrátane, • vytvorenie spoločnej zabezpečenej sieťovej infraštruktúry pre uvedené eGovernment služby v rámci NBÚ, • vybudovanie zdrojových registrov NBÚ (zoznam autorizovaných osôb), ktorý bude obsahovať špecifické referenčné dáta. <p>Služba bude dostupná cez ÚPVS len formou odkazu na IS SBS NBÚ, ktorý ju reálne poskytne z dôvodu ochrany citlivých informácií nachádzajúcich sa v prílohe žiadosti.</p> <p>Všetky KS v rámci IS SBS NBÚ budú budované v súlade s jednotným dizajnom manuálom e-služieb eGovernmentu a na základe analýzy budú aplikované príslušné behaviorálne inovácie. Zároveň bude zabezpečené, že všetky služby budú volané cez web API gateway - podrobnosti sú uvedené v tab. 12.</p>
<p>The diagram illustrates the relationship between stakeholders, security goals, and service outcomes. At the top, five stakeholder groups are listed: NBÚ, Iné OVM, Podnikateľ, Občan, and Conformity assesment body. These groups are connected to three central security goals: Bezpečnosť údajov a transakcií, Ochrana kybernetického priestoru, and Kompetentnosť. These goals then lead to four service outcomes: Súlad s EIDAS, Bezpečnosť kybernetického priestoru, Posun k službám zameraným na nárast konkurencieschopnosti, and Umožnenie modernizácie a racionalizácie verejnej správy IKT prostriedkami.</p>

Základné požiadavky, ktoré projekt naplní, sú nasledovné:

- Požiadavky fyzických a právnických osôb (podnikateľov):
 - umožnenie podania komplexnej elektronickej žiadosti a elektronickej komunikácie s NBÚ v oblasti bezpečnostných previerok, vrátane elektronickej prílohy s mimoriadne citlivými údajmi.
- Požiadavky NBÚ:
 - zabezpečenie elektronického výkonu agendy spracovávanía bezpečnostných spisov NBÚ, vrátane utajovaných skutočností definovaného stupňa utajenia,
 - zabezpečenie efektívneho výkonu správy a riadenia úloh a ich kontroly,
 - umožnenie realizácie fulltextového vyhľadávania, analýz a reportov a spracovanie štatistických údajov,
 - efektívne elektronické získavanie údajov z iných registrov iných OVM prostredníctvom integrácie systém-systém,
 - zabezpečenie informačnej a kybernetickej bezpečnosti vo svojej pôsobnosti a zabezpečenie efektívnej detekcie a riešenia bezpečnostných incidentov v rámci budovaného systému a sieťovej infraštruktúry a ochrana sieťovej infraštruktúry voči nežiadúcemu elektromagnetickému vyžarovaniu,
 - zabezpečenie efektívnej, spoľahlivej a bezpečnej prevádzky IS SBS NBÚ.
- Požiadavky sektorových OVM:
 - zabezpečenie efektívnej, spoľahlivej a bezpečnej komunikácie a výmeny informácií s NBÚ.

ŠU realizuje nasledovný typ zlepšenia (aktivity OPII): "B. Zavedenie inovatívnych elektronickej služieb VS pre občanov a podnikateľov."

Z pohľadu hodnotiaceho kritéria 2.11, v súlade s prílohou č. 14 ŽoNFP v rámci dopytovej výzvy, ide o podporu nasledovnej e-služby v rámci e-Government benchmarku: Začatie podnikania - 1.5 Konkrétne aktivity: "Konkrétne znalosti týkajúce sa konkrétnej profesie. Táto služba sa týka preukazovania (napríklad prostredníctvom diplomu), že podnikateľ je schopný a vyškolený na vykonávanie konkrétnej profesie." Zároveň ide o riešenie ŽS, ktorá je súčasťou 25-tich prioritných životných situácií, konkrétne o: „Začatie podnikateľskej činnosti, priebeh podnikateľskej činnosti a ukončenie podnikateľskej činnosti“. V tomto prípade ide o možnosť podnikateľa realizovať zákazky, pri ktorých dochádza k oboznamovaniu sa s utajovanými skutočnosťami, alebo k vytváraniu utajovaných skutočností. Za týmto účelom je potrebné preukázať, že podnikateľ má vydané osvedčenie o bezpečnostnej previerke.

Pri realizácii je možné sledovať nasledovné projektové merateľné ukazovatele:

- Počet zavedených elektronickej služieb pre fyzické osoby.
- Počet zavedených elektronickej služieb pre právnické osoby (podnikateľov).
- Skrátenie konania.
- Počet integrácií na registre VS.

Aktér	Cieľ	Požiadavky	KPI	Hodnota KPI	Časový horizont	Obmedzenie
fyzická osoba	Komplexná elektronickej komunikácia občana s NBÚ elektronickej služieb	Realizácia služieb tohto projektu	Počet zavedených elektronickej služieb, ktoré prispievajú k riešeniu životných situácií pre občanov (P0739)	as-is: 0 to-be: 4	2022	Schválenie prostriedkov z dopytovej výzvy
právnická osoba (podnikateľ)	Komplexná elektronickej komunikácia podnikateľa s NBÚ elektronickej služieb	Realizácia služieb tohto projektu	Počet zavedených elektronickej služieb, ktoré prispievajú k riešeniu životných situácií pre podnikateľov (P0738)	as-is: 0 to-be: 4	2022	Schválenie prostriedkov z dopytovej výzvy
pracovník NBÚ	Zredukovaný čas potrebný pri vybavovaní agendy bezpečnostných previerok NBÚ	Realizácia služieb a funkcionalít IS SBS NBÚ	skrátene konania previerky FO	as-is: 19,5 hod. to-be: 14,5 hod.	2022	Schválenie prostriedkov z dopytovej výzvy
pracovník NBÚ	Zredukovaný čas potrebný pri vybavovaní agendy bezpečnostných previerok NBÚ	Realizácia služieb a funkcionalít IS SBS NBÚ	skrátene konania previerky PO	as-is: 17,5 hod. to-be: 11,5 hod.	2022	Schválenie prostriedkov z dopytovej výzvy
iné OVM	Efektívnejšie a rýchlejšie získavanie informácií	dostupnosť integračných rozhraní na strane iných OVM	integrácie na registre VS	as-is: 0 to-be: 5	2022	Schválenie prostriedkov z dopytovej výzvy

Riziká **Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.**

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

Prílohy **Diagramy, modely, obrázky v plnom rozlíšení**

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

6. Popis aktuálneho stavu

6.1. Legislatíva

Tabuľka 4 Legislatíva – aktuálny stav

Súhrnný popis	
<p>Európska úroveň:</p> <ul style="list-style-type: none">• Stratégia Európskej komisie „Európa 2020“,• Digitálna agenda pre Európu, COM(2010) 245 z 26.8.2010,• Smerom k interoperabilite európskych verejných služieb – Towards interoperability for European public services, COM(2010) 744 final zo 16.12.2010, príloha 1 Európska stratégia interoperability pre európske verejné služby – European Interoperability Strategy (EIS) a príloha 2 Európsky rámec interoperability pre európske verejné služby – European Interoperability Framework (EIF),• 2013/488/EÚ: Rozhodnutie Rady z 23. septembra 2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ,• Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) <p>NATO Direktívy:</p> <ul style="list-style-type: none">• C-M (2002)49 Security within North Atlantic Treaty Organisation (NATO),• AC/35-D/2001 REV 2 Directive on Physical Security,• AC/35-D/1030 Guidelines on Physical Security,• AC/35-D/1032 Guidelines on the Security of Information,• AC/35-D/1035 NATO Security Risk Management Process (NSRMP). <p>Národná legislatíva – informatizácia:</p> <ul style="list-style-type: none">• Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o eGovernmente) v znení neskorších predpisov,• Zákon č. 95/2019 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov• Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov,• Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,• Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),• Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,• Zákon č. 71/1967 Z. z. o správnom konaní (správny poriadok) v znení neskorších predpisov,• Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,• Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.	
Riziká	Spresnenie identifikovaných rizík: <i>Odkazy na relevantné identifikátory rizík v prílohe Riziká.</i>
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

6.2. Architektúra

6.2.1. Biznis architektúra

Tabuľka 5 Biznis architektúra - aktuálny stav

Súhrnný popis	
<p>V súčasnosti neexistuje žiadny jednotný IS, ktorý by dokázal plne pokryť potreby NBÚ v oblasti spracovania bezpečnostných spisov NBÚ. Najmä v oblasti OUS (bezpečnostné preverky) sú činnosti zabezpečované nejednotným spôsobom s prevládajúcou papierovou komunikáciou a architektúrou systémov a sieťovej infraštruktúry budovaných v rokoch 2001-2007.</p> <p>NBÚ má vybudované informačné systémy izolovane a obsahujú najmä jednoúčelovo prepojené samostatné aplikácie, pričom sú často použité rôznorodé technológie založené na platforme Windows, Solaris a free klonov LINUX. Informačné systémy nie sú ako celok vzájomne prepojené a z tohto dôvodu obsahujú duplicitné funkcionality, ktoré sú riešené pre každý IS iným spôsobom. Nie sú pripravené na rýchle a efektívne zmeny a nevedia dynamicky reagovať na zmeny požiadaviek používateľov – teda majú nízku flexibilitu a škálovateľnosť.</p> <p>NBÚ súčasnými systémami nedokáže udržateľne zabezpečiť požiadavky vyplývajúce z legislatívy (napr. poskytovanie plne elektronických služieb a výkon elektronickej moci v súlade so zákonom o eGovernmente), pričom úprava existujúcich systémov nie je systémovým riešením, najmä vzhľadom na ich vek.</p> <p>Pre obeh písomností v rámci úradu samotného slúži registratúrny systém Fabasoft.</p> <p>Scenár pri podaní podania je v súčasnosti nasledovný:</p> <ul style="list-style-type: none">• občan alebo podnikateľ si sám zistí, aké dokumenty sú potrebné pre výkon požadovanej služby (najmä zákon o OUS), zvyčajne vyhľadáva informácie na webovom sídle NBÚ, prípadne problém rieši osobnou návštevou,• po zhromaždení a vypracovaní potrebných dokumentov ich občan alebo podnikateľ doručí na NBÚ,• na základe poskytnutých dokumentov je vykonaná služba,• na základe doterajších skúseností je tento systém časovo náročný a ako problémom sa javí nie vždy kompletne odovzdanie požadovanej dokumentácie. <p>Z pohľadu hodnotiaceho kritéria 2.11, v súlade s prílohou č. 14 ŽoNFP v rámci dopytovej výzvy, ide o podporu nasledovnej e-služby v rámci e-Government benchmarku: 1.5 Konkrétne aktivity: "Konkrétne znalosti týkajúce sa konkrétnej profesie. Táto služba sa týka preukazovania (napríklad prostredníctvom diplomu), že podnikateľ je schopný a vyškolený na vykonávanie konkrétnej profesie."</p> <p>Zároveň ide o riešenie ŽS 016 "Rozširovanie podnikania", ktorá je v zmysle prílohy č. 19 súčasťou 25-tich prioritných životných situácií, konkrétne v zmysle prílohy č. 19 ide o: „Začatie podnikateľskej činnosti, priebeh podnikateľskej činnosti a ukončenie podnikateľskej činnosti“. V tomto prípade ide o možnosť podnikateľa realizovať zákazky, pri ktorých dochádza k oboznamovaniu sa s utajovanými skutočnosťami, alebo k vytváraniu utajovaných skutočností. Za týmto účelom je potrebné preukázať, že podnikateľ má vydané osvedčenie o bezpečnostnej preverke.</p>	
Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Product viewpoint“, „Business Process Viewpoint“	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

6.2.2. Architektúra informačných systémov

Tabuľka 6 Architektúra informačných systémov - aktuálny stav

Súhrnný popis	
<p>Východiskovú architektúru informačných systémov NBÚ je možné rozdeliť do nasledovných logických vrstiev:</p> <ul style="list-style-type: none"> • Prezentačná vrstva: <ul style="list-style-type: none"> • agendový portál. • Aplikačná vrstva: <ul style="list-style-type: none"> • podateľňa úradu (skenovanie dokumentov) • e-mailová pošta úradu, • IS Previerka, • Fabasoft, • podporná infraštruktúra. • Databázová vrstva. • Infraštruktúrna vrstva. <p>Dáta NBÚ sú udržiavané najmä prostredníctvom registratúrnych záznamov, ktoré sú vytvárané elektronicky v rámci Fabasoftu. Fabasoft predstavuje komplexnú automatizovanú správu registratúry.</p> <p>Od 1. mája 2017 bol spustený systém tenkých klientov s centrálnym serverom s tým, že lokálne priečinky sa presunuli do vzdialeného sieťového úložiska. V podmienkach NBÚ však stále neexistuje centrálné úložisko štruktúrovaných dát a dáta (s výnimkou lokálnych používateľských priečinkov) sú obsiahnuté v rôznych izolovaných systémoch. Ďalším rovnako závažným problémom zostáva nutnosť migrácie dát, ktoré sa už síce ukladajú na sieťové úložisko, ale neexistuje jednotný manažment týchto dát.</p>	
<p>Architektúra jednotlivých IS dotknutých navrhovaným riešením je rôznorodá a nie je možné sa k nej postaviť ako k jednému celku. Nosná časť infraštruktúry bola vybudovaná v rokoch 2001 až 2002 a prakticky bez zásadných zmien pracuje do dnešných dní. Zmeny v architektúre boli realizované len v priebehu rokov 2006 až 2007, kedy sa modernizoval fragment sieťovej infraštruktúry, prostredníctvom ktorej pristupuje NBÚ na Internet. Poslednou významnejšou zmenou realizovanou v roku 2017 bolo spustenie systému tenkých klientov s centrálnym serverom a presunom lokálnych používateľských priečinkov do vzdialeného sieťového úložiska.</p>	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
<p>Stručná charakteristika identifikovaných rizík (Max. 400 znakov)</p>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

6.2.3. Technologická architektúra

Tabuľka 7 Technologická architektúra - aktuálny stav

Súhrnný popis	
<p>Vzhľadom na osobitnú povahu činností, ktoré NBÚ plní, nebude existujúca technologická architektúra podrobne popisujúca existujúci stav systémov súčasťou tejto ŠU. Relevantným dotknutým osobám bude samostatne sprístupnená na základe dohody medzi NBÚ a partnerom.</p> <p>Základný prehľad v súčasnosti prevádzkovaných sietí je nasledovný:</p> <ul style="list-style-type: none">• sieťová infraštruktúra Intranetu NBÚ,• sieťová infraštruktúra pripojenia NBÚ na Internet (Govnet),• virtuálna privátna sieť pre spojenie so stálou delegáciou v Bruseli,• optické prepojenie NBÚ do peeringového centra,• sieťová infraštruktúra PKI NBÚ a ich pripojenia na Internet,• sieťová infraštruktúra záložnej lokality (Govnet),• sieťová infraštruktúra pre prenos US. <p>Uvedená sieťová infraštruktúra je prevádzkovaná na zastaranej metallickej kabeláži (z roku 2001-2002), ktorá je aktuálne na hranici svojich kapacitných možností a navyše neposkytuje dostatočnú ochranu pre prácu s utajovanými skutočnosťami stupňa utajenia „Dôverné“ a neposkytuje ochranu voči nežiadúcemu elektromagnetickému vyžarovaniu (NEV).</p> <p>V priebehu rokov 2006 až 2007 sa modernizovala len sieťová infraštruktúra prostredníctvom, ktorej prístupuje úrad na Internet.</p>	
Riziká	Spresnenie identifikovaných rizík: <i>Odkazy na relevantné identifikátory rizík v prílohe Riziká.</i>
<i>Stručná charakteristika identifikovaných rizík (Max. 400 znakov)</i>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

6.2.4. Bezpečnostná architektúra

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis	
<p>Aktuálna bezpečnostná architektúra je založená primárne na bezpečnom rozdelení systémov a pracovných staníc zamestnancov do vhodných segmentov siete. Na výstupnom perimetri je vybudovaný monitorovací systém chrániaci pred prístupom k škodlivým stránkam a kódom smerom do internetu. Systém rovnako kontroluje, prípadne blokuje prenos paketov prichádzajúci smerom do NBÚ. V rámci internej infraštruktúry sú prevádzkované viaceré monitorovacie systémy a lokálne aktualizčné servery. Niektoré kritické systémy sú prevádzkované bez fyzického pripojenia do siete Internet.</p> <p>Pripojenie do peeringového centra je realizované formou optickej linky a NBÚ má prenajaté virtuálne privátne linky na spojenie so stálou misiou v Bruseli pre výmenu evidencie o US od NASES.</p> <p>Samostatnú časť bezpečnostnej architektúry tvoria vnútorné systémy súvisiace s oblasťou OUS. Tieto sú vybudované a prevádzkované s ohľadom na citlivú povahu informácií plne v súlade s požiadavkami zákona o OUS a nemôžu byť zverejňované.</p>	
Riziká	Spresnenie identifikovaných rizík: <i>Odkazy na relevantné identifikátory rizík v prílohe Riziká.</i>
<i>Stručná charakteristika identifikovaných rizík (Max. 400 znakov)</i>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

6.3. Prevádzka

Tabuľka 9 Prevádzka - aktuálny stav

Súhrnný popis	
<p>Prevádzka systémov je plne v gescii NBÚ a systémy sú prevádzkované v rámci interných kapacít úradu. Systémy sú umiestnené v serverovni v priestoroch úradu a sú spravované zamestnancami úradu. Okrem hlavného pracoviska je prevádzkované aj záložné pracovisko v geograficky vzdialenej lokalite, ktoré v prípade významnej havárie dokáže zastúpiť iba poskytovanie základných služieb (len služieb PKI, ktoré sú mimo rámca tohto projektu).</p> <p><i>Nakoľko systémy sú budované decentralizovane a bez centrálného úložiska dát, je prevádzka mierne komplikovaná a náročnejšia vzhľadom na správu väčšieho množstva decentralizovaných IS a tým pádom aj väčšie pracovné zaťaženie zodpovedných správcov.</i></p> <p>NBÚ deklaruje, že disponuje dostatočnými kapacitami s potrebnou odbornou spôsobilosťou (projektovým manažérom pre projektové riadenie), know-how a potrebným materiálno-technickým zázemím pre realizáciu projektu v danej oblasti. Zároveň deklaruje, že disponuje kvalifikovanými prevádzkovými kapacitami (s potrebnou odbornou spôsobilosťou a know-how a potrebným materiálno-technickým zázemím), ktoré budú schopné prevádzkovať implementované riešenie.</p>	
Riziká	Spresnenie identifikovaných rizík: <i>Odkazy na relevantné identifikátory rizík v prílohe Riziká.</i>
<i>Stručná charakteristika identifikovaných rizík (Max. 400 znakov)</i>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

7. Alternatívne riešenia

7.1. Alternatíva A – „Názov“

Súhrnný popis
Úvodné informácie (Max. 800 znakov)
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.
Ďalšie informácie (Max. 800 znakov)
Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)

7.2. Alternatíva B – „Názov“

Súhrnný popis
Úvodné informácie (Max. 800 znakov)
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.
Ďalšie informácie (Max. 800 znakov)
Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)

8. Popis budúceho stavu

8.1. Legislatíva

Tabuľka 10 Legislatíva - budúci stav

Súhrnný popis	
Pre oblasť OUS sa predpokladajú nasledovné legislatívne úpravy: <ul style="list-style-type: none">• novelizácia vyhlášok NBÚ,• novelizácia štandardov NBÚ.	
Kritéria kvality	Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Stručná charakteristika požadovanej kvality (Max. 400 znakov)	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

8.2. Architektúra

8.2.1. Biznis architektúra

Tabuľka 11 Biznis architektúra – budúci stav

Súhrnný popis

Základom nového riešenia systému ES SBS NBÚ je agendový modul, v ktorom sú implementované interné procesy NBÚ v oblasti bezpečnostných previerok a spracovania bezpečnostných spisov NBÚ. Tento systém svoje výstupy, prostredníctvom komponentu API gateway (aplikačné služby) alebo portálu (koncové služby), bude poskytovať používateľom z radu občanov, podnikateľov a iných OVM.

Systém predstavuje architektúru založenú na mixe už komerčne dostupných (ale na potreby NBÚ customizovaných) komponentov integrovaných do jedného spolupracujúceho riešenia, ktoré bude podľa možnosti čo najviac pre-používať už existujúce komponenty eGovernmentu (vládný cloud, ÚPVS, referenčné registre).

V rámci riešenia budú podporované koncové služby pre oblasť bezpečnostných previerok, pre fyzické osoby a právnické osoby (podnikateľov), konkrétne:

- Podávanie žiadosti o bezpečnostnú previerku právnickej osoby (ks_338835).
- Podávanie žiadosti o vydanie certifikátu podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami EÚ (ks_338847).
- Podávanie žiadosti o vydanie certifikátu podnikateľa o priemyselnej bezpečnosti pre oboznamovanie sa s utajovanými skutočnosťami NATO (ks_338848).
- Podávanie žiadosti o uznanie, zmenu alebo ochranu zahraničných informácií v rámci bezpečnostnej previerky právnickej osoby (ks_338849).
- Podávanie žiadosti o bezpečnostnú previerku fyzickej osoby (ks_338834).
- Podávanie žiadosti o vydanie certifikátu o bezpečnostnej previerke fyzickej osoby pre oboznamovanie sa s utajovanými skutočnosťami EÚ (ks_338850).
- Podávanie žiadosti o vydanie certifikátu o bezpečnostnej previerke fyzickej osoby pre oboznamovanie sa s utajovanými skutočnosťami NATO (ks_338851).
- Podávanie žiadosti o zmenu v rámci bezpečnostnej previerky fyzickej osoby (ks_338852).

ŠU realizuje nasledovný typ zlepšenia (aktivity OPII): "B. Zavedenie inovatívnych elektronických služieb VS pre občanov a podnikateľov."

Pre všetky vyššie uvedené KS platia nasledovné zlepšenia:

- úroveň služby sa z as-is stavu 2 zvýši na úroveň služby 4 pre to-be stav,
- početnosť za skupinu služieb ks_338850, ks_338851, ks_338852 a ks_338834 je **8526**, nakoľko tieto služby sú na seba úzko naviazané a sú priamo závislé na výsledku služby ks_338834, resp. bez tejto služby a jej výsledku nie je možné samostatne realizovať zvyšné služby,
- početnosť za skupinu služieb ks_338847, ks_338848, ks_338852 a ks_338835 je 127, nakoľko tieto služby sú na seba úzko naviazané a sú priamo závislé na výsledku služby ks_338835, resp. bez tejto služby a jej výsledku nie je možné samostatne realizovať zvyšné služby,
- z pohľadu zlepšenia atribútov uvedených v prílohe č. 12 ide o zlepšenie všetkých atribútov okrem 6, 26 a 27 z nasledovných dôvodov:
 - 6 - služba nie je viackanálová z dôvodu špecifickej prílohy s mimoriadne citlivými údajmi,
 - 26 - irelevantné pre cudzincov - služba vzhľadom na jej špecifický charakter je určená len pre SR,
 - 27 - irelevantné pre cudzincov - služba vzhľadom na jej špecifický charakter je určená len pre SR,
- všetky uvedené služby budú v súlade s nasledovnými požiadavkami na zlepšenie:
 - responzívny dizajn,
 - UX analýza,
 - info o stave vybavovania,
 - implementácia bežne dostupného štandardného analytického nástroja
 - automatizovaná informácia o úspešne zrealizovanom podaní pre ÚPVS - informáciu o úspešnom zrealizovaní bude sprostredkovať priamo systém, aj z dôvodu, že podanie, kvôli špecifickej citlivej prílohe, nebude môcť byť realizované cez ÚPVS,
 - nastavenie aktívnych „listerov“ a zabezpečenie integrácií na iné systémy VS (registre a centrálné moduly),
 - umožnenie online platenia,
 - prihlasovanie/podpisovanie pomocou smartfónu - systém bude predpripravený aj pre takúto možnosť, keď bude táto funkcionálna oficiálne zavedená zo strany NASES,
- pre všetky uvedené služby nebudú dosiahnuté nasledovné parametre zlepšení z nasledovných dôvodov:
 - dosiahnutie multikanálového prístupu - služba nie je viackanálová z dôvodu špecifickej prílohy s mimoriadne citlivými údajmi,
 - zriadenie proaktívnej služby (úroveň 5) - služba bude zasielať notifikáciu o blížiacom sa konci platnosti certifikátu, avšak rozhodnutie o podaní opätovnej žiadosti je na používateľovi.

Ďalšie podrobnosti k jednotlivým zlepšeniam a parametrom služieb sú uvedené v samostatnom xls súbore "NBU_Parametre_a_zlepsenia_sluzieb.xlsx".

Z pohľadu hodnotiaceho kritéria 2.11, v súlade s prílohou č. 14 ŽoNFP v rámci dopytovej výzvy, ide o podporu nasledovnej e-služby v rámci e-Government benchmarku: 1.5 Konkrétne aktivity: "Konkrétne znalosti týkajúce sa konkrétnej profesie. Táto služba sa týka preukazovania (napríklad prostredníctvom diplomu), že podnikateľ je schopný a vyškolený na vykonávanie konkrétnej profesie."

Zároveň ide o riešenie ŽS 016 "Rozširovanie podnikania", ktorá je v zmysle prílohy č. 19 súčasťou 25-tich prioritných životných situácií, konkrétne v zmysle prílohy č. 19 ide o: „Začatie podnikateľskej činnosti, priebeh podnikateľskej činnosti a ukončenie podnikateľskej činnosti“. V tomto prípade ide o možnosť podnikateľa realizovať zákazky, pri ktorých dochádza k oboznamovaniu sa s utajovanými skutočnosťami, alebo k vytváraniu utajovaných skutočností. Za týmto účelom je potrebné preukázať, že podnikateľ má vydané osvedčenie o bezpečnostnej previerke.

Biznis architektúra navrhovaného riešenia musí byť v súlade s procesmi v rámci agendy NBÚ ako aj procesmi platnými pre prostredie eGovernmentu.

Architektúra bude z pohľadu používateľov nasledovná:

- občan, podnikateľ, alebo OVM pristupuje k informačným službám prostredníctvom verejne dostupného portálu, kde sa nachádzajú všeobecné informácie, predpisy a stanoviská NBÚ. Ostatné služby sú dostupné prostredníctvom formulárov, či už cez modul formulárov, ÚPVS eForm, alebo jeden z multikanálových prístupov. Niektoré formuláre budú dostupné iba cez formulárový modul, nakoľko informácie v nich uvedené by mali byť podľa GDPR šifrované.
- pracovník NBÚ pristupuje k systému najmä prostredníctvom registratúrneho systému Fabasoft, kde rieši došlú agendu.

Cieľové riešenie bude umožňovať elektronickú formu komunikácie a výmenu dokumentov a bude poskytovať podporu pre úlohy a činnosti v kompetencii NBÚ. Pre používateľov systému bude k dispozícii plná používateľská podpora vo forme navigácie a usmerňovania používateľa v závislosti od typu žiadosti, oblasti, systému, produktu a iných aspektov a parametrov.

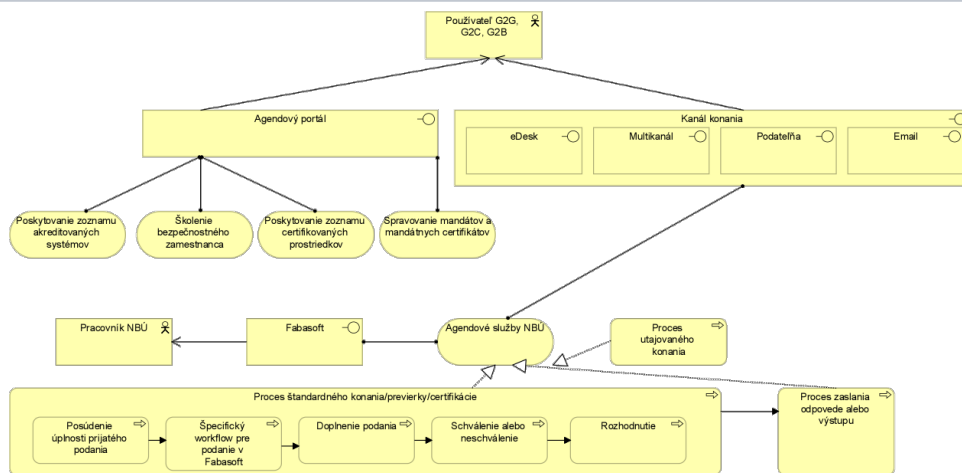
Systém umožní realizáciu plne elektronického procesu, ktorý pozostáva z nasledovných krokov:

- elektronické podanie a podpísanie žiadateľom,
- prijatie, spracovanie a zaevidovanie podania v elektronickej registratúre,
- presun podania do modulu spracovávajúceho utajované skutočnosti,
- spracovanie podania, vrátane získania informácií z iných registrov iných OVM - prostredníctvom integrácie,
- dožiadanie, schválenie a podpísanie nadriadeným,
- odoslanie a doručenie výsledku spracovania žiadateľovi do elektronickej schránky na ÚPVS.

Okrem toho systém umožní realizáciu funkcionalít súvisiacich s:

- manažmentom a kontrolou úloh a manažmentom vyťaženia pracovníkov NBÚ,
- vyhľadávaním informácií vo fulltex formáte a realizáciou analýz,
- generovaním reportov a štatistických údajov.

Celé riešenie bude implementované tak, aby bolo možné v rámci systému spracovávať údaje, ktoré budú klasifikované z pohľadu utajovaných skutočností ako „Dôverné“.



Kritéria kvality	Spresnenie kritérií kvality: <i>Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.</i>
Stručná charakteristika požadovanej kvality (Max. 400 znakov)	
Riziká	Spresnenie identifikovaných rizík: <i>Odkazy na relevantné identifikátory rizík v prílohe Riziká.</i>
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

8.2.2. Architektúra informačných systémov

Tabuľka 12 Architektúra informačných systémov - budúci stav

Súhrnný popis
<p>IS ES NBÚ bude obsahovať štandardnú aplikačnú a dátovú architektúru. Aplikačná vrstva IS ES NBÚ, ktorá má zhmotniť načrtnutú biznis architektúru a podporiť jednotný výkon činností a elektronizáciu procesov NBÚ je nasledovná.</p> <p>Základom systému budú nasledovné základné moduly:</p> <ul style="list-style-type: none">• modul portál - spracovania a realizácie elektronických podaní,• modul registrácie elektronických podaní,• work-flow modul pre spracovávanie bezpečnostných spisov NBÚ (utajovaných skutočností stupňa utajenia „Dôverné“), zabezpečujúci všetky potrebné úkony v rámci spracovania podania,• modul odoslania a doručenia výsledku spracovania žiadateľovi. <p>Modul spracovania a realizácie elektronických podaní umožní žiadateľovi bezpečným a dôveryhodným spôsob vyplniť žiadosť o bezpečnostnú previerku (v prípade opakovanej žiadosti aj pred-vyplniť požadované údaje, ktoré už NBÚ bude mať), následne túto žiadosť autorizovať elektronickým podpisom a odoslať zabezpečeným kanálom do systému NBÚ na jej spracovanie. Portál predstavuje prezentačnú vrstvu vystavenú do internetu pre externých používateľov. Táto vrstva je doplnená o Web API gateway, čo je komponent, ktorý analogicky vystavuje aplikačné služby. Portál obsahuje nasledovné moduly:</p> <ul style="list-style-type: none">• CMS predstavuje obsahovú časť portálu, ktorá poskytuje CMS a Wiki služby - statický používateľsky editovateľný obsah, podporujúci aj automatické publikovanie obsahu z interných systémov pomocou webových služieb,• Modul osobný účet umožňuje zisťovať stav podania príslušného používateľa, <p>Celá žiadosť bude spracovaná v štruktúrovanej forme vo formáte elektronického formulára, takže ju bude možné na strane NBÚ spracovávať aj strojovo priamo systémom a navrhnutými algoritmami. Funkcionalita formulárov umožní:</p> <ul style="list-style-type: none">• vizualizáciu a možnosť uloženia na disk,• šifrovanie podania,• spracovanie PDF a HTML formulárov,• integráciu na podpisovú aplikáciu ÚPVS a odoslanie autorizovaného podania (formuláru) do podateľne NBÚ / elektronickej schránky NBÚ. <p>Modul registrácie elektronických podaní zabezpečí registráciu prijatého elektronického úradného záznamu v súlade s požiadavkami zákona o archívoch a registratúre a priradenie záznamu do príslušného spisu, prípadne založenie nového spisu.</p> <p>Kľúčovým a najdôležitejším modulom bude work-flow modul pre spracovávanie bezpečnostných spisov NBÚ. Tento modul pre spracovávanie utajovaných skutočností stupňa utajenia „Dôverné“ umožní, vytvorí alebo poskytne:</p> <ul style="list-style-type: none">• virtuálne prostredie pre centrálnu správu a prácu tenkých klientov,• pripájanie certifikovaných hrubých klientov a ich centrálnu správu,• nástroje pre autentifikáciu zariadení v sieti NBÚ (protokol 802.1x),• nástroje a technológie pre ochranu dát (DLP a označovanie dokumentov – labeling),• nástroje pre ochranu a správu koncových zariadení (End Point Protection),• nástroje pre dvoj-faktorovú autentifikáciu používateľov prostredníctvom PKI certifikátov (identifikácia a autentifikácia kryptografickou čipovou kartou zamestnanca a implementácia internej CA pre vydávanie certifikátov),• nástroje pre autorizáciu (podpísanie) elektronických úradných dokumentov mandátnym certifikátom alebo elektronickej pečaťou NBÚ,• nástroje pre realizáciu automatického zálohovania,• nástroje pre centrálny manažment konfigurácií, riadenia bezpečnostných záplat a licenčný manažment, vrátane aktivácie licencií. <p>Modul odoslania a doručenia výsledku spracovania zabezpečí prenos elektronického úradného dokumentu (aj certifikátu) z modulu spracovania utajovaných skutočností do „neutajovaného“ sveta a jeho finálne doručenie žiadateľovi do jeho elektronickej schránky v rámci spoločných modulov ÚPVS.</p> <p>Spôsob integrácie na externé ISVS a poskytovanie aplikačných služieb na externú integráciu je cez integračný komponent, ktorý predstavuje Web API gateway, ktorý predstavuje jeden centrálny bod, cez ktorý budú poskytované aplikačné služby predovšetkým na báze protokolu REST. Tento modul bude mať vystavené služby nielen na počúvanie, ale zabezpečí aj volania aplikačných služieb iných ISVS. Riešenie bude integrované s centrálnymi komponentami e-Governmentu, najmä CSRÚ pre dátovú a procesnú integráciu. Relevantné údaje budú dostupné vo forme otvorených údajov na platforme data.gov.sk. Web API gateway bude poskytovať nasledovné služby:</p>

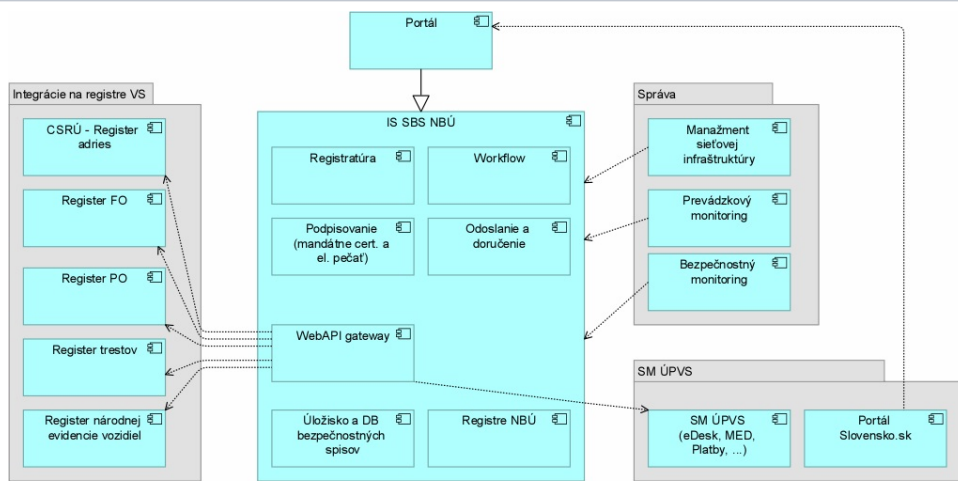
- proxy a transformácie API,
- analytika nad API,
- IAM nad aplikačnými službami,
- messaging

Systém bude integrovaný najmä na nasledovné registre iných OVM:

- register adries (prostredníctvom CSRÚ),
- register fyzických osôb,
- register právnických osôb (prostredníctvom CSRÚ),
- register trestov,
- register národnej evidencie vozidiel.

Integrácie na uvedené registre (okrem registra adries a registra právnických osôb) budú riešené priamou integráciou, t.j. mimo CSRÚ, z dôvodu požiadavky na prístup k informáciám, ktoré nie sú súčasťou CSRÚ datasetu a z dôvodu riešenia bezpečnosti prístupu k týmto špecifickým a citlivým údajom a jeho logovania a auditovania.

Platby budú realizované elektronicky platobnou kartou alebo bezhotovostne pomocou mechanizmov uvedených v aktuálnom návrhu novely zákona č. 305 /2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o eGovernmente) v znení neskorších predpisov, resp. pomocou IS PEP, ktorý už platby kartou umožňuje.



Dátová vrstva:

Táto bude relatívne nezávislá na aplikačnej vrstve. Ide primárne o úložisko (DB) bezpečnostných spisov a s tým súvisiace registre NBÚ. V registroch sú vedené a aktualizované evidencie ohľadne dát, ktorých vlastníkom je NBÚ ako povinná osoba, t. j. nezáškávajú sa z iných zdrojov ISVS, a s ktorými sa narába v rámci procesov, prípadne ktorých vznik v rámci týchto procesov povoľuje. Tieto registre je možné považovať za potenciálne zdrojové registre. Ide najmä o nasledovné registre, resp. údaje:

- Osvedčenie o bezpečnostnej previerke fyzickej osoby.
- Potvrdenie o priemyselnej bezpečnosti podnikateľa.
- Evidencia oprávnených osôb pre stupeň utajenia Prísne tajné, Tajné a Dôverné.
- Evidencia osôb, so zaniknutým oprávnením pre stupeň utajenia Prísne tajné, Tajné a Dôverné.
- Evidencie osôb s vydaným potvrdením o vykonaní skúšky bezpečnostného zamestnanca.

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

8.2.3. Technologická architektúra

Tabuľka 13 Technologická architektúra - budúci stav

Súhrnný popis

Základom technologickej architektúry bude kompletne vynovená sieťová infraštruktúra na báze optických vlákien a optických sietí, ktorá umožní komplexný manažment siete a prevádzkový monitoring, vrátane bezpečnostného monitoringu.

Kľúčovou vlastnosťou takejto siete je jej ochrana, resp. odolnosť voči nežiadúcemu elektromagnetickému vyžarovaniu čo umožní zachovať ochranu utajovaných skutočností požadovaného stupňa utajenia. Vzhľadom na skutočnosť, že agenda sekcie previerok disponuje informáciami stupňa utajenia Dôverné, je potrebné zohľadnenie požiadaviek NEV ako napr. tienenie, nízko úrovňový prenos signálov, oddelenie kabeláže a filtrácia napájacích a signálových vedení už v počiatočnej fáze projektu.

Informácie prenášané optickým spojením sú prenášané ako svetelné signály. Pre takéto káble je charakteristická ich schopnosť prenášať vysoké množstvo informácií za časovú jednotku, nízky útlm, odolnosť voči elektromagnetickej interferencii, nevedú elektrický prúd (nulová možnosť skratov, požiaru) a bezpečnosť prenosu (signál sa nedá jednoducho zachytiť).

Kľúčové sieťové prvky budú zdvojené z pohľadu zachovania požadovanej dostupnosti (redundancia vybraných aktívnych a pasívnych sieťových prvkov). Pre optické spojenie je problematické využitie súčasných zariadení a z tohto dôvodu je potrebná kompletná (zatiaľ mimo zariadení určených pre zabezpečenie siete Internet) obnova zariadení.

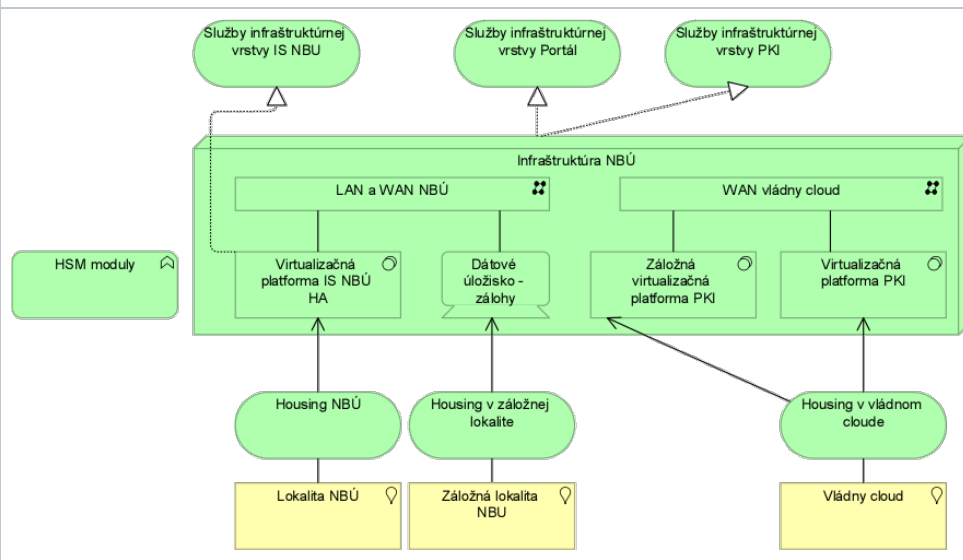
Detailný návrh technologickej architektúry bude predmetom samotného projektu, t. j. bude výstupom analytickej fázy a fázy návrhu projektu. Základné, rámcové požiadavky NBÚ na technologickú architektúru sú nasledovné:

- pre časť infraštruktúry (portál) prevádzkovej v štátnom cloudu, ako i pre zálohu a rozdelenie záťaže budú využívané možnosti štátneho cloudu,
- časť infraštruktúry prevádzkovaná v priestoroch a na prostriedkoch NBÚ (modul spracovávania bezpečnostných spisov a utajovaných skutočností stupňa utajenia „Dôverné“), dátová záloha v záložnom pracovisku NBÚ,
 - modul nie je prepojený s inými systémami (galvanicky oddelený), prenos informácií je jednosmerný a pod dohľadom operátora,
 - systém bude obsahovať HSM pre uloženie kľúčov elektronickej pečate,
 - modul je prevádzkovaný v high-availability konfigurácii na prostriedkoch NBÚ.

Pre tento „Dôverný“ segment sa počíta s dedikovaným Rack-om, hardvérom a vyššie uvedenou prenosovou infraštruktúrou.

Predpokladané prevádzkové parametre sú nasledovné:

- RPO 2 dni
- RTO 1 deň
- prevádzka 24x7
- dostupnosť 98 %



Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

8.2.4. Implementácia a migrácia

Tabuľka 14 Implementácia a migrácia

Súhrnný popis

Implementácia je predpokladaná v štyroch fázach:

Fáza I. – Analýza a príprava:

- konzultačno-analytické práce spojené s identifikáciou potrebných zdrojov,
- detailná analýza a návrh procesov v rámci NBÚ a návrh ich optimalizácie,
- nákup potrebných licencií a nákup HW.

Fáza II. – Vybudovanie IS SBS NBÚ:

- tvorba DFŠ zároveň s wireframe modelom zákazníckych obrazoviek,
- agilná implementácia a nasadenie v súlade s bežným SDLC (pre neštandardné komponenty) IS SBS NBÚ,
- vybudovanie novej sieťovej infraštruktúry na báze optických sietí,
- vytvorenie potrebných konektorov a integrácie,
- obvyklé testovania vrátane UX testovania komponentov pre externých aj interných používateľov.

Fáza III. – Pilotná prevádzka:

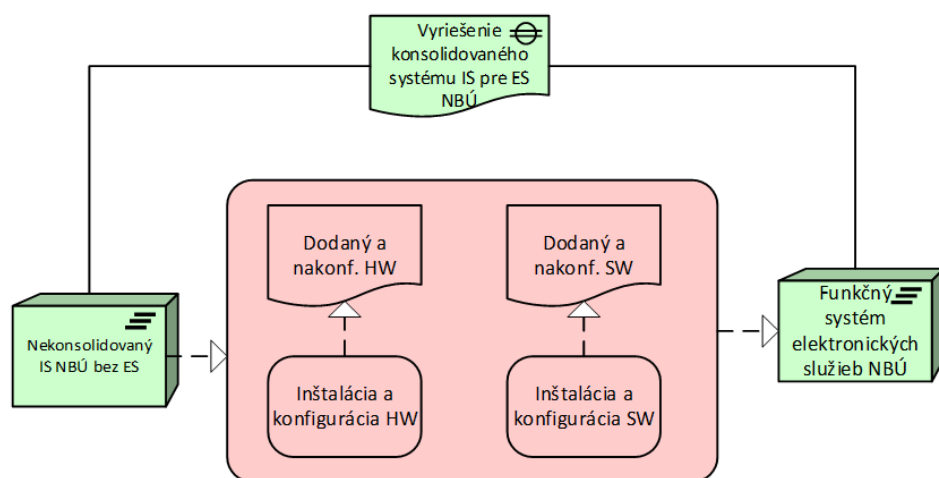
- iniciálna fáza projektu v rámci NBÚ a ladenie.

Fáza IV. – Prevádzka systému

Po dokončení a vyladení systému prechod na plnú prevádzku systému už plne v gescii NBÚ.

Vzhľadom na výšku nákladov sa jedná o pomerne veľký projekt, pričom cieľom je, aby jeho riadenie zahŕňalo poučenia z projektov realizovaných v rámci programu OPIS. Týmito poučeniami sú:

- podľa možnosti agilný prístup k vývoju s častým dodávaním prototypov a testovaním (a tvorba DFŠ súčasne s vývojom prototypu),
- zabezpečenie dostatočného projektového tímu na strane zákazníka minimálne na úrovni garantov, ktorý sa vie projektu venovať na dennej báze,
- dodržiavanie princípov projektového riadenia PRINCE2 (definované produkty s akceptačnými kritériami, zmenový rozpočet, tolerancie jednotlivých míľnikov, etáp a aj samotných produktov),
- dôraz na včasné prijatie potrebných legislatívnych zmien.



Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

8.2.5. Bezpečnostná architektúra

Tabuľka 15 Bezpečnostná architektúra - budúci stav

Súhrnný popis	
<p>Význam systému a jeho dopady na bezpečnosť jednotlivých kooperujúcich ISVS je z pohľadu bezpečnosti nezastupiteľný a vyžaduje preto osobitnú ochranu.</p> <p>Bezpečnostná architektúra predpokladá vybudovanie komplexného systému ochrany, ktorý bude implementovaný technickými prostriedkami, ktoré zahŕňajú dedikované bezpečnostné prostriedky tvoriace súčasť aplikačných komponentov a infraštruktúry ako aj netechnické prostriedky pre manažment informačnej bezpečnosti.</p> <p>Bezpečnostná architektúra bude zahŕňať nasledovné oblasti:</p> <ul style="list-style-type: none">• dodržiavanie pravidiel riadenia informačnej bezpečnosti (podľa zákona č. 69/2018 o kybernetickej bezpečnosti, medzinárodnej normy ISO/IEC 27001: 2013 a podľa zákona č. 95/2019 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov,• systém riadenia aplikačnej bezpečnosti,• monitorovanie bezpečnosti a incident management,• segmentácia siete, monitoring a ochrana sieťového spojenia,• hardening staníc a whitelisting aplikácií. <p>Pri návrhu sa požaduje zohľadniť nasledovné kritériá bezpečnosti:</p> <ul style="list-style-type: none">• architektúra technických prvkov musí byť navrhnutá tak, aby v kooperácii s ostatnými oblasťami riešenia, ako napr. sieťová a aplikačná architektúra, umožnila stálu dostupnosť a škálovateľnosť,• pre pripájanie externých IS musí byť vytvorený bezpečný a autentizovaný komunikačný kanál,• autentizácia používateľov prístupujúcich k IS musí byť adekvátna spôsobu ich pripojenia a oprávnení používateľov na činnosti v IS,• pri návrhu komunikácie medzi ISVS sa musí používať štandardný spôsob komunikácie medzi systémami, predovšetkým webové služby schválené dátové prvky a identifikátory,• príslušné dátové typy pre údaje prenášané webovými službami sa požaduje navrhnuť tak, aby bola umožnená účinná kontrola špecializovanými bezpečnostnými mechanizmami,• artefakty vytvorené počas fázy návrhu musia byť vytvárané podľa jednotných pravidiel tak, aby umožňovali jednoznačné bezpečnostné overenie najmä s dôrazom na typy a formu údajov, spôsob ich spracovávania, zabezpečenia integrity a riadenie prístupu k nim. <p>Realizácia systému si vyžiada zabezpečenie prevádzky, správy a údržby IS v súlade s požiadavkami riadenia IB. Systém musí zohľadňovať všetky požiadavky kladené zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti, zákonom č. 95/2019 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov a súvisiacich právnych predpisov.</p> <p>Pre prístup k administratívnejmu rozhraniu budú prevádzkované služby zápisu administrátora s mapovaním na riadenie prístupov, s osobitným ohľadom na zvýšenú bezpečnosť (samostatné školenie každého zamestnanca, viacfaktorové prihlasovanie, vyhradené lokality prístupu).</p>	
<p>V rámci realizácie projektu bude potrebné z pohľadu bezpečnosti zabezpečiť najmä:</p> <ul style="list-style-type: none">• samostatné testovanie,• anonymizáciu osobných dát a identít osôb pre účely testovania,• logický a fyzický prístup k testovaciemu a vývojovému prostrediu,• používateľské akceptačné testy,• bezpečnú implementáciu kryptografických algoritmov, vrátane hash algoritmov použitých na autentifikačné účely,• logovanie všetkých dôležitých aktivít,• u vybraných záznamov z logovania zabezpečiť osobitné ukladanie a vyhľadávanie,• nad vybranými citlivými úkonmi administrátorov a operátorov v systéme zabezpečiť autorizáciu týchto úkonov min. elektronickým podpisom. <p>Technologická a bezpečnostná architektúra bude popísaná a zhrnutá v bezpečnostnom projekte, ktorý bude okrem iného obsahovať špecifikáciu použitých bezpečnostných štandardov na zabezpečenie pred stratou dôvernosti, integrity a dostupnosti údajov, vymedzenie kľúčových problémových miest v navrhovanom IS SBS NBÚ s popisom hrozieb zabezpečených a nezabezpečených protiopatreniami.</p>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

8.3. Prevádzka

Tabuľka 16 Prevádzka - budúci stav

Súhrnný popis	
<p>NBÚ deklaruje, že disponuje dostatočnými kapacitami s potrebnou odbornou spôsobilosťou (projektovým manažérom pre projektové riadenie), know-how a potrebným materiálno-technickým zázemím pre realizáciu projektu v danej oblasti. Zároveň deklaruje, že disponuje kvalifikovanými prevádzkovými kapacitami (s potrebnou odbornou spôsobilosťou a know-how a potrebným materiálno-technickým zázemím), ktoré budú schopné prevádzkovať implementované riešenie.</p> <p>Prevádzka bude zabezpečená pracovníkmi NBÚ, ktorí aktuálne spravujú informačné systémy prevádzkované v rámci NBÚ. V tejto súvislosti bude kľúčové, aby súčasťou projektu bolo aj dodanie kvalitnej bezpečnostnej, projektovej a prevádzkovej dokumentácie. Nepredpokladá sa zvýšený nárok na personálne obsadenie v súvislosti s prevádzkou, nakoľko systém bude centralizovaný a nastavený na rovnakú úroveň bezpečnosti aj použitých technológií. Dodávateľským spôsobom (na základe SLA) bude zabezpečovaná L3 úroveň podpory a change requesty.</p> <p>Dostupnosť prevádzky sa predpokladá v móde 24x7 s parametrom dostupnosti 99 percent.</p> <p>NBÚ bude schopný prevádzku nového informačného systému plne pokryť zo svojho rozpočtu. Jedná sa o nasledovné náklady:</p> <ul style="list-style-type: none">• náklady úrovne podpory L3 a change requesty,• náklady na licencie a údržbu (maintenance). <p>V prípade, ak sa výška rozpočtu na prevádzku zníži, môže to predstavovať potenciálne riziko poskytovania garantovaných služieb.</p>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<i>Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.</i>	<i>Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.</i>

8.4. Ekonomická analýza

Tabuľka 17 Ekonomická analýza - budúci stav

Súhrnný popis

Zavedenie IS SBS NBÚ bude mať veľký dopad na príslušný úsek verejnej správy, a to tak horizontálne ako aj vertikálne. Centrálny systém s jednotnými dátami a procesmi podporí plne elektronický výkon agendy NBÚ v oblasti bezpečnostných previerok. Svojim širokým dopadom, potrebou spolupráce s inými ISVS a ambíciou optimalizovať procesy jednotlivých konaní a činností NBÚ môže mať zásadný prínos pre budovanie eGovernmentu v SR, kedy občan, podnikateľ i verejná správa pocítia priamo benefity elektronickej verejnej správy.

Prínosy projektu sa skladajú z dvoch hlavných oblastí - časové úspory z optimalizácie a automatizácie procesov a časové úspory z menej častých a kratších výpadkov systému.

1. Časové úspory pri spracovaní podania na strane úradníka vyplývajú z detailnej analýzy procesov spracovania previerky a meraní trvania jednotlivých aktivít. Na základe návrhu systému boli určené aktivity, ktoré budú v novom systéme plne automatizované (úspora 99% súčasného času), čiastočne automatizované aktivity (zrýchlenie aktivity bude mať za následok časovú úsporu 60 percent z súčasného trvania) a aktivity, ktoré budú aj v budúcom stave prebiehať manuálne (bez úspory). Takto je možné ušetriť ekvivalent 14,22 FTE, resp. 30 percentné zrýchlenie času spracovania.
2. Súčasný systém je morálne zastaralý, jeho pôvodný dodávateľ neexistuje a nie je už naň možné na trhu obstaráť náhradné komponenty. O systém sa stará výhradne jeden pracovník NBÚ. Z týchto dôvodov je každý výpadok systému spojený s pomerne veľkými nákladmi, pričom do budúcnosti je predpoklad zvyšovania frekvencie výpadkov. Priemerné trvanie incidentu je na základe historických údajov NBÚ približne 3 dni, pričom za rok 2019 boli 3 takéto incidenty. V prípade výpadku systému je nutné pracovať offline, čo na základe meraní zvyšuje pracovnosť spracovania podania trojnásobne. Uvažujeme, že nový systém bude prakticky bez incidentov tohto typu (úplný výpadok počas pracovnej doby), nakoľko cluster riešenie zabezpečí prakticky neustálu dostupnosť. Incidenty potom môžu byť riešené na cluster nóde, ktorý vypadol pri zachovaní prevádzky, alebo mimo pracovnej doby. Aj na základe tohto aspektu je vypočítaný prínos nového systému na 138 142 EUR ročne.

Čistá súčasná ekonomická hodnota (ENPV) = 419 068 EUR

Pomer prínosov a nákladov (BCR) = 1.10

Ekonomická vnútorná miera návratnosti (IRR) = 7.6%

Rok návratu investície (PBP) = 9

Náklady na riešenie = 4 000 721

Celkové náklady za 10 rokov = 4 981 179