digitální ; ČESKO

Vládní program digitalizace
České republiky 2018+

INFORMAČNÍ KONCEPCE ČR

Implementační plán hlavního cíle č. 3 - IKČR
Rozvoj celkového prostředí podporujícího digitální technologie a budování/provoz klíčových systémů eGovernmentu

Verze dokumentu: **1.1**

Datum poslední změny dokumentu: **29. 5. 2020**

Poznámka k verzi:

_____

Úřad vlády České republiky, Nábřeží Edvarda Beneše 4, 118 01 Malá Strana
info@digitalnicesko.cz digitalnicesko.cz

Obsah

1 Základní informace

1.1 Rekapitulace cílů

Název a popis cíle
IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie
IKČR 3.01 Aktivně prosazovat alokaci prostředků z ESIF na podporu prostředí digitálních technologií
Při tvorbě nového programovacího období bude ČR aktivně prosazovat alokaci prostředků z ESIF na podporu prostředí digitálních technologií, v rámci IKČR pro rozvoj rozsahu a dostupnosti služeb elektronické veřejné správy.
IKČR 3.02 Digitalizace dosud nedigitalizovaného obsahu
Digitalizace dosud nedigitalizovaného obsahu důležitého pro podporu konkurence-schopnosti a rozvoj eGovernment služeb pro veřejnost. Jedná se například o fondy duševního vlastnictví, knihovní fondy a fond kulturního dědictví, dokončení digitalizace katastru nemovitostí, digitalizace výstupů územního plánování zejména územních plánů, projektových dokumentací, digitalizace historických úředních dokumentů, agend pro podporu stavebnictví atd.
IKČR 3.03 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu
Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu, jako předpokladu pro plně digitální, bezpapírové procesy veřejné správy.
IKČR 3.04 Rozvoj a provoz základních registrů
Zkvalitnění, aktualizace a validace obsahu Registru práv a povinností. Jedná se zejména o zlepšení popisu dekompozice činností agend, agendových rolí a správné registrace agendových, provozních i dalších systémů (ISVS) do příslušných agend, ve vazbě na informace o řízení přístupu k datovým položkám, včetně prostorových. Dále o správu číselníků všech údajů důležitých pro řízení služeb eGovernmentu (životní události a situace, komponenty IS a jejich služby, datové sady apod.). Obecně jde o řídící (meta) informace eGovernmentu a tzv. META-informační systém (Meta-IS). V této souvislosti je nutné pro stále častější užívání těchto nástrojů při vývoji a správě služeb zjednodušit jejich obsluhu a provázat ji přirozeně s životním cyklem agend a informačních systémů veřejné správy.
IKČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy
Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy. Komunikační infrastruktura veřejné správy včetně Centrálního místa služeb (CMS) se musí stát sdíleným, bezpečným a řízeným komunikačním prostředím zejména pro všechny správce agendových systémů v přenesené působnosti. Musí umožnit bezpečné propojování poskytovaných online služeb s jejich uživateli, a to jak uvnitř veřejné správy, tak i pro klienty na internetu. Celá komunikační infrastruktura musí být nákladově efektivní, bez zbytečných duplicit v komunikačních kanálech, robustní a bezpečná s definovanými a měřitelnými parametry jednotlivých služeb formou SLA. Budována bude i nadále vícezdrojově, s využitím vlastní infrastruktury veřejné správy i s využitím komerčních služeb. Komunikační prostředí veřejné správy je nástrojem umožňujícím dostupnou, spolehlivou a bezpečnou komunikaci mezi jednotlivými IT systémy a uživateli těchto systémů. Komunikačního prostředí veřejné správy je mimo jiné nutné pro využití při zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a řešení krizových situací. Bezpečná a dostatečně odolná cesta přenosu informací mezi dotčenými složkami veřejné správy, jejichž informační a rozhodovací potenciál je klíčový pro případ rychlé reakce, je nezbytným technickým předpokladem odolnosti státu vůči všem hrozbám bez rozdílu. Existence funkční infrastruktury parametricky odpovídající poskytovaným službám, s případnou rezervou pro další rozvoj těchto služeb, je také podmínkou dalšího rozvoje eGovernmentu a naplňování mnoha vládních strategií (např. Strategie digitálního vzdělávání do roku 2020, Strategie digitální gramotnosti). Aby se předešlo spontánním zásahům do tohoto prostředí, je potřeba rozvoj komunikačního prostředí veřejné správy korigovat. Koncepce rozvoje komunikačního prostředí veřejné správy bude sledovat dlouhodobé cíle a zajistí efektivní vynakládání prostředků v této oblasti.
IKČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe
Zavedení systému důvěryhodné elektronické identifikace do praxe. Do cíle spadá jak elektronická identifikace občanů a zástupců právnických osob (NIA, nové občanské průkazy, komerční poskytovatelé identifikace, …) a cizinců, tak společná centrální fyzická i elektronická identifikace úředníků prostřednictvím jednotného autentizačního systému (SSO). Součástí cíle jsou i prostředky pro elektronický podpis a pečeť pro úředníky a úřady, a jejich poskytování jako sdílené služby státu. Součástí cíle je i zajištění elektronizace oprávnění k úkonům na základě zákonných zmocnění, plných mocí, profesních způsobilostí (lékaři apod.) a dalších oprávnění (řidičská, zbrojní apod.).

IKČR 3.07 Rozvoj a provoz základních služeb
Implementace strategie sdílení dat mezi veřejnou správou a privátním sektorem formou Digitální mapy veřejné správy, zejména Digitální technické mapy ČR a dalších autoritativních široce využitelných datových zdrojů (vzniklých např. na základě použití metod jako je BIM – Informační modelování staveb apod.) jako nedílných součástí Národní infrastruktury pro prostorové informace.
IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu
Podpora opatření kybernetické bezpečnosti pro veřejnou správu. Obsahem cíle je zajišťování důvěry a bezpečnosti interních i externích digitálních služeb veřejné správy plněním „Akčního plánu k Národní strategii kybernetické bezpečnosti ČR“, a to pro příslušné období, a dalšími opatřeními, nezahrnutými do jiných cílů IK ČR. Opatření tohoto cíle pro veřejnou správu souvisí s opatřeními cílů DES HC5 pro celou společnost, zejména pak s dílčími cíli 5.4 a 5.5. Cíl byl přesunut z DES 5.1, protože je zaměřen výhradně na veřejnou správu a patří tak do IKČR.

1.2 Klasifikace záměrů A, B a C

A. Záměr je dlouhodobě připravený, schválený v gesčním úřadu, je „v běhu“, má zajištěné financování (např. projekty již schválené OHA). V rámci metodiky to odpovídá stavu „závazku“, popř. dalších stavů. Záměry „A“ jsou uvedeny v příloze implementačních plánů.

B. Záměr je definovaný gesčním úřadem, tj. má prioritu a podporu v gesčním úřadu, ale nemá finanční nebo personální krytí. Tyto záměry tvoří těžiště implementačního plánu.

C. Potřebný záměr, existuje koncept záměru (tj. prakticky všechna políčka jsou vyplněná), ale není dojednána podpora gestora, gesční úřad, ani zdroje (typicky průřezové záměry, multirezortní a sdílené).

V katalogu záměrů se nachází ještě další záměry ve stavu „**D**“, tj. náměty na záměr. Tyto náměty vznikly z různých inspirací, například z potřeby pomoci úřadů dostát požadavkům architektonickým principů a zásad řízení ICT ze schválené Informační koncepce. Mnohé náměty mohou být ještě nedostatečně popsané, duplicitní nebo příliš detailní, proto je pro jejich převod do stavu „C“ při příštím implementačním plánování nutná jejich konsolidace.

1.3 Shrnutí problematiky, celkové přínosy

Cílem opatření v rámci hlavního cíle 3 je ve spolupráci se sociálními partnery a s dalšími subjekty vytvořit prostředí, podporující českou společnost v digitální transformaci. Plnění tohoto cíle je spolu s legislativními úpravami klíčovým předpokladem významného posunu v celé oblasti vzdělávání, výzkumu a vývoje, ICT infrastruktury, legislativy, trhu práce, standardizace a kybernetické bezpečnosti. Je třeba se zaměřit na vytvoření příznivých podmínek pro oblast eGovernmentu, například cestou rozvoje Národního identitního prostoru České republiky, v rámci něhož by každý občan, potenciálně schopný digitální komunikace, měl disponovat alespoň jedním elektronickým identitním prostředkem na vzdálené prokázání své totožnosti. Podporovat firmy a občany v přijímání digitálních technologií. Vytvořit prostředí příznivé pro vznik, vývoj a testování digitálních a mobilních služeb a s tím související nastavení očekávání občanů. Součástí tohoto cíle jsou i digitální služby v oblasti elektronických podpisů, například realizace sdílené služby pro vytváření úředně ověřeného elektronického podpisu, podle zákona o právu na digitální služby.

Za „digitalizaci“ se přirozeně považuje transformace dosud nedigitalizovaného obsahu na plně digitální, nicméně spadá sem i posun ve významné a komplikované oblasti zavedení průkazné elektronické identity všech subjektů a rovněž i zkvalitnění dosud nekvalitního, již existujícího digitálního obsahu (např. obsah Registru práv a povinností).

Z hlediska předpokladů efektivního využití eGovernmentu a zlepšení mezinárodní konkurenceschopnosti ČR tvoří zásadní oblast rovněž rozvoj vysokorychlostních sítí, zejména dostupnosti vysokorychlostního internetu. Do tohoto cíle rovněž spadá rozvoj komunikační infrastruktury veřejné správy.

K tomu, aby digitalizovaná veřejná správa dobře fungovala a aby v ni organizace i občané měli důvěru, je klíčové zajistit bezpečnost digitálních služeb. Jedná se, jak o obranu proti kybernetickým útokům a zajištění efektivní a kvalitní kybernetické infrastruktury, tak o ochranu soukromí a osobních i obchodních údajů uživatelů.

Jedním ze základních předpokladů pro efektivní fungování jednotlivých centrálních i lokálních agendových i neagendových informačních systémů je jejich napojení na robustní základní registry jako centrální autoritativní zdroje základních informací. Stávající systémy základních registrů mj. i z důvodu implementace Zákona č.12/2020 o právu na digitální služby musí projít výraznými úpravami. Na tuto aktuální situaci reaguje **dílčí cíl – 3.04 Rozvoj a provoz základních registrů.** Tento cíl vychází z původního dílčího cíl 3.04 – Zkvalitnění, aktualizace a validace obsahu Registru práv a povinností a dále jej rozšiřuje v návaznosti na aktuální požadavky.

V současnosti řešená problematika GIS si vyžádala úpravu dílčího cíle 3.7, kdy jeho původní zaměření spočívalo v úzké specializaci na Digitální technické mapy ČR a Informační systém technické infrastruktury veřejné správy. Toto zaměření je stále validní a je i dále akcelerováno především v souvislosti s novým stavebním zákonem a digitalizací stavebního řízení. Nově formulovaný **dílčí cíl 3.07 Rozvoj a provoz základních služeb** v sobě nově zahrnuje i veškeré záměry z oblasti Národní infrastruktury pro prostorové informace.

1.4 Počty záměrů a odhad finanční alokace dle gesce

Klasifikace (stav) - Gestor	Počet	Výdaje 2021 [mil. Kč]	Výdaje 2022 [mil. Kč]	Výdaje v dalších letech [mil. Kč]
A	**24**	**237,00**	**110,00**	**665,74**
Česká správa sociálního zabezpečení	1			54,45
FN u sv. Anny v Brně	1			81,00
Národní úřad pro kybernetickou a informační bezpečnost	7			0,00
Správa základních registrů	3	105,00	86,00	377,50
Ministerstvo vnitra	6			54,40
Ministerstvo spravedlnosti	1	0,00	15,00	0,00
Ministerstvo práce a sociálních věcí	1	5,00	5,00	0,00
Ministerstvo zemědělství	1	4,00	4,00	0,00
Ministerstvo kultury	2	123,00		97,53
Ministerstvo dopravy	1			0,86
B	**9**	**209,00**	**238,00**	**115,95**
Institut postgraduálního vzdělávání ve zdravotnictví	1	10,00	9,00	0,00
Národní úřad pro kybernetickou a informační bezpečnost	1	15,00	15,00	0,00
Správa základních registrů	1	154,00	144,00	88,00
ÚV – úřad vlády	1	0,00	0,00	0,00
Ministerstvo vnitra	3	30,00	70,00	20,00
Ministerstvo kultury	2			7,95
C	**7**	**931,00**	**953,50**	**1 012,00**
Český statistický úřad	3	31,00	28,50	0,00
Ministerstvo vnitra	3	900,00	925,00	902,00
Ministerstvo spravedlnosti	1	0,00	0,00	110,00
Celkový součet	**40**	**1 377,00**	**1 301,50**	**1 793,69**

1.5 Počty záměrů a odhad finanční alokace dle cílů

Klasifikace (stav) - Dílčí cíl	Počet	Výdaje 2021 [mil. Kč]	Výdaje 2022 [mil. Kč]	Výdaje v dalších letech [mil. Kč]
A	**24**	**237,00**	**110,00**	**665,74**
IKČR 3.02 Digitalizace dosud nedigitalizovaného obsahu.	6	123,00	15,00	184,99
IKČR 3.04 Rozvoj a provoz základních registrů	5			10,00
IKČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.	1			38,80
IKČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.	5	114,00	95,00	431,95
IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	7			0,00
B	**9**	**209,00**	**238,00**	**115,95**
IKČR 3.02 Digitalizace dosud nedigitalizovaného obsahu.	1			3,72
IKČR 3.04 Rozvoj a provoz základních registrů	4	184,00	214,00	108,00
IKČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.	1			4,23
IKČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.	2	10,00	9,00	0,00
IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	1	15,00	15,00	0,00
C	**7**	**931,00**	**953,50**	**1 012,00**
IKČR 3.04 Rozvoj a provoz základních registrů	3	27,00	53,50	0,00
IKČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.	1	900,00	900,00	900,00
IKČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.	1	4,00		0,00
IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	1	0,00	0,00	110,00
IKČR 3.07 Rozvoj a provoz základních služeb	1			2,00
Celkový součet	**40**	**1 377,00**	**1 301,50**	**1 793,69**

1.6 Výsledky za rok 2019 - stav záměrů v realizaci

Gestor – Název záměru	Počet	Hotovo %	Výdaje 2021 [mil. Kč]	Výdaje 2022 [mil. Kč]	Výdaje v dalších letech [mil. Kč]
Česká správa sociálního zabezpečení	**1**				**54,45**
Implementace nařízení eIDAS, ČSSZ	1	100			54,45
Ministerstvo dopravy	**1**				**0,86**
Zpřístupnění informací o řidiči prostřednictvím Portálu občana	1	100			0,86
Ministerstvo kultury	**1**				**69,34**
Národní eKnihovna	1	10			69,34
Ministerstvo práce a sociálních věcí	**1**		**5,00**	**5,00**	**0,00**
Poskytování služeb při vydávání kvalifikovaných a komerčních certifikátů v resortu MPSV	1	100	5,00	5,00	0,00
Ministerstvo vnitra	**5**		**30,00**	**70,00**	**30,00**
Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů	1	5	30,00	70,00	20,00
Právní úprava rozšíření funkcionalit RPP o údaje vedené doposud v IS o ISVS a IS DP	1	90			0,00
RPP, rozvoj registru a jeho agendového informačního systému	1	80			0,00
RPP, rozvoj, analýza datového modelu, analýza procesu plnění a užívání údajů	1	10			0,00
RPP, začlenění ISoISVS do RPP a další rozvoj	1	20			10,00
Ministerstvo zemědělství	**1**		**4,00**	**4,00**	**0,00**
Vybudování přístupového bodu ke službám elektronické identifikace, MZe	1	10	4,00	4,00	0,00
Správa základních registrů	**3**		**259,00**	**230,00**	**465,50**
Implementace ZoPDS v prostředí SZR – ISZR, ISSS / eGSB	1	5	154,00	144,00	88,00
Národní certifikační autorita (NCA)	1	65	85,00	66,00	214,50
Rozvoj NIA – Národního bodu el. identifikace a autentizace	1	80	20,00	20,00	163,00
ÚV – úřad vlády	**1**		**0,00**	**0,00**	**0,00**
Revize agend dle RPP	1	25	0,00	0,00	0,00
Celkový součet	**14**		**298,00**	**309,00**	**620,15**

1.7 Prioritní záměry pro období 2020-2021

- Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů
- Implementace digitální ústavy v prostředí SZR – ZoPDS, ISZR, eGSB/ISSS

2 Sestava plánovaných záměrů dle data ukončení realizace (klasifikace B, C)

Rok konce realizace – měsíc – název záměru	Počet	Hotovo %	Výdaje 2021 [mil. Kč]	Výdaje 2022 [mil. Kč]	Výdaje v dalších letech [mil. Kč]
2020	**1**		**0,00**	**0,00**	**0,00**
12	**1**		**0,00**	**0,00**	**0,00**
Revize agend dle RPP	1	25	0,00	0,00	0,00
2021	**2**		**14,00**	**9,00**	**0,00**
1	**1**		**10,00**	**9,00**	**0,00**
Opatření pro kybernetickou bezpečnost v IPVZ	1	0	10,00	9,00	0,00
12	**1**		**4,00**		**0,00**
SIS_I_Centrální autentizační bod	1		4,00		0,00
2022	**6**		**72,00**	**138,50**	**20,00**
1	**1**				**0,00**
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu	1				0,00
12	**5**		**72,00**	**138,50**	**20,00**
Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů	1	5	30,00	70,00	20,00
ROS - 2020+	1		19,00	26,00	0,00
ROS – IAIS - 2020+	1		8,00	2,50	0,00
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí	1			25,00	0,00
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence	1		15,00	15,00	0,00
2023	**2**		**1 054,00**	**1 044,00**	**988,00**
12	**2**		**1 054,00**	**1 044,00**	**988,00**
Implementace ZoPDS v prostředí SZR – ISZR, ISSS / eGSB	1	5	154,00	144,00	88,00
Vysokorychlostní datová síť krajů a technologická centra krajů	1		900,00	900,00	900,00
2025	**1**				**0,00**
7	**1**				**0,00**
Rozšiřování počtu Service Providerů (SeP), připojených do NIA	1				0,00
2027	**1**		**0,00**	**0,00**	**110,00**
12	**1**		**0,00**	**0,00**	**110,00**
Kybernetická bezpečnost rezortu justice	1		0,00	0,00	110,00
Celkový součet	**13**		**1 140,00**	**1 191,50**	**1 118,00**

3 Plánované náklady a pracnosti záměrů (klasifikace B, C)

Název záměru	Celk. výdaje na realizaci [mil. Kč]	Výdaje na realizaci 2021 [mil. Kč]	Odhad pracnosti realizace (dny)	Externí výdaje na udržitelnost [mil. Kč]	Pracnost udržitelnosti (dny)
Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů	120,00	30,00		20,00	
Kybernetická bezpečnost rezortu justice	110,00	0,00			
Metodická podpora zavedení DTM ČR	2,00				
Opatření pro kybernetickou bezpečnost v IPVZ	19,00	10,00		4,00	
Revize agend dle RPP		0,00	10,00		
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK	4,23		200,00	0,00	0,00
Rozšiřování počtu Service Providerů (SeP), připojených do NIA					
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí					
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu					
Vysokorychlostní datová síť krajů a technologická centra krajů	2 750,00	900,00	5 000,00	60,00	9 000,00
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK	3,72		200,00	43 832,00	1 600,00
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence	30,00	15,00			
Implementace ZoPDS v prostředí SZR – ISZR, ISSS / eGSB	386,00	154,00	2 510,00	160,00	753,00
ROS - 2020+	45,00	19,00	100,00	3,00	
ROS – IAIS - 2020+	10,50	8,00	100,00		
SIS_I_Centrální autentizační bod	4,00	4,00	150,00	0,20	290,00
Celkový součet	**3 484,45**	**1 140,00**	**8 270,00**	**44 079,20**	**11 643,00**

4 Přehled pokrytí cílů – plánované záměry (klasifikace B, C)

Cíl – název záměru
IKČR 3.02 Digitalizace dosud nedigitalizovaného obsahu.
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK
IKČR 3.04 Rozvoj a provoz základních registrů
Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů
Revize agend dle RPP
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu
Implementace ZoPDS v prostředí SZR – ISZR, ISSS / eGSB
ROS - 2020+
ROS – IAIS - 2020+
IKČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK
Vysokorychlostní datová síť krajů a technologická centra krajů
IKČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.
Opatření pro kybernetickou bezpečnost v IPVZ
Rozšiřování počtu Service Providerů (SeP), připojených do NIA
SIS_I_Centrální autentizační bod
IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.
Kybernetická bezpečnost rezortu justice
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence
IKČR 3.07 Rozvoj a provoz základních služeb
Metodická podpora zavedení DTM ČR

5 Kontaktní osoby – plánované záměry (klasifikace B, C)

Gestor – kontaktní osoba – název záměru
Český statistický úřad
Pavel Charvát
SIS_I_Centrální autentizační bod
Michal Čigáš
ROS - 2020+
ROS – IAIS - 2020+
Institut postgraduálního vzdělávání ve zdravotnictví
Antonín Malina
Opatření pro kybernetickou bezpečnost v IPVZ
Národní úřad pro kybernetickou a informační bezpečnost
Viktor Paggio
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence
Správa základních registrů
František Knotek
Implementace ZoPDS v prostředí SZR – ISZR, ISSS / eGSB
ÚV – úřad vlády
Jan Braunstein
Revize agend dle RPP
Ministerstvo vnitra
Alois Slovák
Vysokorychlostní datová síť krajů a technologická centra krajů
Eva Kubátová
Metodická podpora zavedení DTM ČR
František Knotek
Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů
Jan Tretera
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu
Pavel Hrabě
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí
Petr Kuchař
Rozšiřování počtu Service Providerů (SeP), připojených do NIA
Ministerstvo spravedlnosti
Daniel Štorek
Kybernetická bezpečnost rezortu justice

Ministerstvo kultury
Josef Praks
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK

6 Popisy záměrů (klasifikace A, B, C)

Gestor – stav – název záměru – popis záměru
Česká správa sociálního zabezpečení
A
Implementace nařízení eIDAS, ČSSZ
Český statistický úřad
C
ROS - 2020+
Cílem projektu bude implementovat vybrané požadavky cílového konceptu ZR 2.0, zákona č. 12/2020 o právu na digitální služby a novely zákona o základních registrech. Konkrétně půjde o tyto aktivity: a) implementace souhlasu subjektu údajů se zpřístupněním jeho dat pro konkrétní orgán veřejné moci – realizace požadavku vyplývajícího z §8 zákona o právu na digitální služby. Pokud bude aplikováno stejné řešení jako v případě ROB, tak se předpokládá vytvoření nových služeb pro FAIS, zavedení evidence sdílených údajů a realizace úprav dle požadavků bezpečnostních složek. Odhadované náklady na tuto akci jsou 1000 MDs tj. 13 800 000 Kč (vč. DPH). b) zařazení nových referenčních údajů do ROS – realizace požadavku vyplývajícího z §10 zákona o právu na digitální služby (zařazení kontaktních údajů do ROS). V této souvislosti se předpokládá vytvoření nové editační služby ROS a úprava dosavadních publikačních služeb ROS. Předpokládané náklady na tuto akci jsou 103 MDs tj. 1 500 000 Kč (vč. DPH). c) aplikace analytického modulu – aplikace analytického modulu umožní kontrolu integritních vazeb v rámci editorů registrů, kontrolu integritních vazeb mezi základními registry, vytváření vlastních a předpřipravených reportů na základě provozních a infrastrukturních dat (reporty budou využity k optimalizaci služeb ROS) a poskytování údajů ve formě open dat (buď ve formě statistik o počtech osob dle vybraných charakteristik (region, právní forma apod.) nebo ve formě poskytování informací o jednotlivých osobách). Předpokládané náklady na tuto akci jsou 1000 MDs tj. 13 800 000 Kč (vč. DPH). d) implementace APP cache – APP cache bude sloužit na podporu analytického modulu, bezodstávkového provozu ROS a k převzetí určité části publikačních služeb při velkém zatížení vlastní databáze ROS. Předpokládané náklady na tuto akci jsou 860 MDs tj. 12 500 000 Kč (vč. DPH). e) zlepšování kvality dat vedených v ROS – realizace širokého spektra aktivit vedoucích ke zvýšení kvality dat v ROS, větší kontrole správce nad údaji vedenými v ROS a rozšíření možností poskytování exportů z ROS. Konkrétně se bude jednat o doplnění možnosti zápisu speciálního PSČ k adresnímu kódu, filtrování změn na registrované IČO pro poskytování notifikací uživatelům ZR, zobrazování historických změn k IČO ve správcovské aplikaci, rozšíření exportů správcovské aplikace, výmaz a oprava záznamu v externím číselníku ROS, zpřístupnění výdeje údajů správci nebo úpravu testovacích dat na platné agendy a OVM. Předpokládané náklady na tuto akci jsou 200 MDs tj. 3 000 000 Kč (vč. DPH).
ROS – IAIS - 2020+
ROS-IAIS je ISVS, definovaný zákonem č. 111/2009 Sb. o základních registrech. Jde o centrální webové řešení, které poskytuje nástroj pro přidělení IČO, zápis osob i změn referenčních údajů do ROS u těch editorů ROS, kteří nemají vlastní informační systém pro vedení a zápis osob do ROS. Kromě toho přináší možnost získávat aktuální údaje ze základních registrů a další výhody, jako je například vytištění výstupů referenčních údajů osoby. Správcem ROS-IAIS je Český statistický úřad. Okruh uživatelů ROS-IAIS je poměrně rozsáhlý. Používají jej pracovníci profesních komor, vybraných ministerstev, ústředních, krajských a obecních úřadů a dalších orgánů veřejné moci. ROS-IAIS tak v současnosti využívá více než 2.000 orgánů veřejné moci. Technické řešení ROS-IAIS bylo připravováno v letech 2010–2012. V této době nebylo dostatek praktických informací o

potřebách jednotlivých orgánů veřejné moci. Využívání ROS-IAIS je tak zejména u méně zdatných uživatelů vnímáno jako zbytečně komplikované a těžkopádné. V některých případech také uživatelé využívají funkcionalitu nesprávně nebo proces zápisu nedokončí, což může vést k problémům s aktuálností osob v ROS a vyšší kapacitní nároky na zajištění podpory ze strany správce. Také chybí větší kontrola kvality údajů zasílaných do ROS. Výše uvedené skutečnosti mají za následek, že uživatelé ROS-IAIS využívají pro svoji činnost data ze základních registrů jen velmi omezeně a spíše je získávají tradičními způsoby tedy přímo od subjektu údajů.
Cílem projektu bude změna uživatelského rozhraní a rozšíření funkcionalit pro administraci a podporu aplikace tak, aby se zjednodušily a sjednotily postupy vedoucí k zápisu, opravě, odstranění nebo aktualizaci vedených osob, omezila se variabilita stávající funkcionality, zajistilo se automatické provedení aktualizací RUIAN na základě plánované úlohy a vytvořil se průvodce na podporu práce méně zkušených uživatelů. Dále se předpokládá doplnění údajů ROS-IAIS o nově vedené referenční údaje ROS, úprava uživatelských manuálů ROS-IAIS a větší kontrola textových zápisů do ROS (mělo by se jednat výlučně o zahraniční adresy).
Očekáváme, že výše uvedené úpravy zvýší motivaci uživatelů aktualizovat a využívat referenční údaje základních registrů a zároveň zvýší kvalitu dat vedených v ROS. Společně s tím budou uvolněny nemalé kapacity správce ROS-IAIS, které se v současnosti věnují podpoře uživatelů ROS-IAIS. Realizované změny budou zároveň představovat první krok pro zajištění budoucího využití ROS-IAIS při získávání nezbytných údajů ze základních registrů a z propojeného datového fondu pro činnost decentralizovaných agend veřejné správy zaměřených na evidenci vybraných fyzických a právnických osob.

SIS_I_Centrální autentizační bod

Vybudování centrálního autentizačního bodu pro externí uživatele aplikací ČSÚ zjednoduší situaci především respondentům se statistickou povinností. Tito uživatelé aplikací ČSÚ si budou moci zvolit způsob autentizace k aplikaci, který jim nejlépe vyhovuje. Odpadne nutnost lokální registrace do dané aplikace.
Vedle zachování možnosti autentizace lokálním účtem aplikace (registr externích uživatelů ČSÚ) bude možné zvolit autentizaci prostřednictvím systému Datových schránek. Toto bude vhodná a pravděpodobně preferovaná metoda autentizace právnických osob, které byly obeslány zprávou o své statistické povinnosti prostřednictvím zprávy do Datové schránky. Výhodou tohoto způsobu autentizace je především odpadnutí procesu registrace uživatele.
Další možností autentizace k aplikacím ČSÚ bude autentizace prostřednictvím Národní identitní autoritou (NIA). Toto může být vhodná alternativa pro přihlášení fyzické osoby, která vystupuje vůči právnické osobě se statistickou povinností jako zpracovatel zajišťující plnění této povinnosti. Nemusí se nutně jednat o pracovníka dané právnické osoby, může jít o smluvního dodavatele služeb. V případě tohoto druhu autentizace je nutné zajistit propojení takové fyzické osoby s příslušnou právnickou osobou.
Pro autentizaci osob z jiných OVM pak lze použít služby JIP/KAAS.

FN u sv. Anny v Brně

A

Elektronizace zdr. dokumentace, FN u svaté Anny v Brně

Projekt schválený OHA v rámci výzev z ESIF.

Institut postgraduálního vzdělávání ve zdravotnictví

B

Opatření pro kybernetickou bezpečnost v IPVZ

Projekt si klade za cíl vyřešení problémů v oblasti informační a kybernetické bezpečnosti, zejména posílení chybějících nebo nedostatečných součástí ochrany informačního systému IPVZ v oblasti fyzické, aplikační a systémové bezpečnosti.
Mezi hlavní aktivity projektu patří činnosti spadající do kategorií: fyzická bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí a aplikační bezpečnost.
Mezi hlavní očekávané multiplikační efekty předkládaného projektu jsou především: zvýšení bezpečnosti dat a informačních systémů, zvýšení spolehlivosti a dostupností dat a informačních systémů, automatizace a digitalizace vybraných procesů a zrychlení procesu řízení.
Projekt bude zahrnovat následující aktivity a oblasti:
• Bezpečnost dat: řešení pro zajištění bezpečnosti a důvěrnosti dat.
• Architektura a integrace: řešení, které zajišťuje spolupráci jednotlivých prvků v rámci IPVZ, ale i vazby na informační systémy partnerských organizací v rámci ekosystému IPVZ.
• Log management: pořízení centralizovaného úložiště logů. Cílem je identifikace kybernetických bezpečnostních incidentů, včetně včasného varování všech bezpečnostních rolí.
• Nástroj pro ověřování identity uživatelů a řízení přístupových oprávnění.
• Monitoring připojení a omezení využívání výměnných zařízení. Cílem je zajistit hlavně bezpečnost při přenášení dat z USB médií lektory vzdělávacích akcí na VT v učebnách.

Ministerstvo dopravy

A

Zpřístupnění informací o řidiči prostřednictvím Portálu občana

Zajištění dostupnosti dat z registru řidičů veřejnosti on-line formou. V první fázi publikace základního kontextu údajů o řidiči prostřednictvím portálu veřejné správy (Portál občana) v rozsahu identifikace osoby, řidičského průkazu a skupin řidičského oprávnění, stavu konta bodového hodnocení řidiče a informace o platnosti dokladů agendy řidičů. Ve druhé fázi publikace rozšířeného kontextu údajů, doplnění o výpis přestupků, podrobnosti bodového hodnocení či omezení řidičského oprávnění.

Ministerstvo kultury

A

Národní eKnihovna

Národní eKnihovna je v souladu s trendy v kulturně rozvinutých zemích světa, kde dochází k přeměně klasických knihoven na moderní kulturně vzdělávací a kreativní centra. Národní knihovna ČR je vlastníkem největšího souboru papírové i digitalizované literatury, monografií, hudebnin, map a grafik v České republice, které po digitalizaci budou nabídnuty ke komfortnímu využití nejširší laické i odborné veřejnosti, což bude zcela nová kvalitativní úroveň služby.

Národní platforma pro el. správu a evidenci muzejních sbírek a agend (ELVIS), MK

Vytvoření nového IS ELVIS – Národní platforma pro elektronickou správu a evidenci muzejních sbírek a agend, společně s Národním muzeem, Moravským zemským muzeem (CITEM) a dalšími významnými a krajskými muzei. Nahradí morálně a technologicky zastaralý stávající produkt DEMUS, na nějž budou moci efektivně přejít i další uživatelé/správci sbírek muzejní povahy, kteří dosud využívali komerční nebo jiné alternativní programy, nebo s digitalizací evidence sbírky dosud nezapočali.

B

Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK

Projekt "Rozšíření bezpečnostních systémů checkpoint" je plánován v souvislosti se zvýšením bezpečnosti Ministerstva kultury, čímž reaguje na zjištění a doporučení ze strany NBÚ a metodických pokynů NÚKIB.

Zabezpečení digitalizace sbírek Technického Muzea Brno, MK

Pořízení skeneru pro digitalizaci výkresů, map a pozůstalostí a zpřístupnění tohoto kulturního dědictví badatelům a veřejnosti. Ochrana a zachování sbírkových předmětů.

Ministerstvo práce a sociálních věcí

A
Poskytování služeb při vydávání kvalifikovaných a komerčních certifikátů v resortu MPSV
Jednotlivým úředníkům vydávající správní rozhodnutí je zajišťován výdej a generování kvalifikovaných certifikátů dle nařízení eIDAS. Pro vzájemné budování důvěry na elektronickém trhu jsou a budou vydávány kvalifikované serverové certifikáty dle nařízení eIDAS (tzv. elektronické pečetě).
Ministerstvo spravedlnosti
A
Hardware složek justice (skenery)
Nákup OCR zařízení pro převádění podání do digitální podoby se strojově čitelnou vrstvou. Součást projektu eISIR.
C
Kybernetická bezpečnost rezortu justice
Rozšíření technické infrastruktury zajišťující kybernetickou bezpečnost soudů, státních zastupitelství, ministerstva spravedlnosti a dalších organizačních složek resortu justice. Jedná se o projektový záměr připravený v rámci výzvy č. 10 Kybernetická bezpečnost programu IROP, na který (po jeho schválení OHA a odsouhlasení IROP) však v tomto programu již nezbyly potřebné finanční prostředky, a proto nemohl být realizován. Záměr byl v mezidobí rozšířen o další technické prvky dle definice zákona o kybernetické bezpečnosti. Zdroj financování IROP, částečně státní rozpočet.
Ministerstvo vnitra
A
Evidence Národního archivního dědictví na Portálu Národního archivu ČR
Evidence NAD bude prostřednictvím IS PEvA II navázána na evidenci původců, evidenci archivů a dalších subjektů, které vedou základní evidenci NAD podle § 16 archivního zákona. Rovněž bude vytvořena vazba NAD na další funkce Národního portálu, a to zvláště v oblasti elektronického výběru archiválií a zveřejňovaných archivních pomůcek.
Kontinuální rozvoj DCeGOV, OKB MV
Tento projekt navazuje na předchozí projektové aktivity jednotlivých projektů „Dohledového centra eGovernmentu“. Vybudováním „DCeGOV“ bylo v oblasti centralizace bezpečnostního a provozního dohledu k implementaci převážné části zásad a požadavků vyplývajících ze zákona č. 181/2014 Sb. a pokrytí první části resortu MV službami centralizovaného monitoringu vybraných provozovaných informačních systémů. Realizací projektu dojde k vytvoření „IS DCeGOV“ a napojení dalšího portfolia informačních systémů v souladu s implementačním plánem projektu na Dohledové centrum se souběžnou implementací nových částí ICT infrastruktury provozovaného DCeGOV. Vytvoření „IS DCeGOV“ pro zajištění provozně-bezpečnostního dohledu a řízení bezpečnosti systémů v aktivním i pasivním módu s ohledem na požadavky zákona o kybernetické bezpečnosti. Napojení dalších IS rezortu MV na aktivní dohled. Nová verze systému Ambiente HoneyNet – nová verze systému reagující na nové kybernetické hrozby.
Právní úprava rozšíření funkcionalit RPP o údaje vedené doposud v IS o ISVS a IS DP
Jak informační systém o informačních systémech veřejné správy (IS o ISVS), tak informační systém o datových prvcích (IS DP) byly až doposud vedeny jako samostatné informační systémy veřejné správy. Z důvodů duplicity s architekturou základních registrů je dlouhodobým záměrem NAP převedení jejich funkcionalit pod univerzální referenční rozhraní, které je nyní reprezentováno Informačním systémem základních registrů ISZR a obecným referenčním rozhraním pro komunikaci tzv. eGSB/ISSS v rámci Centrálního místa služeb. Z výše uvedených důvodů je v obou případech třeba provést úpravu technické povahy a tyto samostatné ISVS převést do RPP.
RPP, rozvoj registru a jeho agendového informačního systému
Nové funkcionality: katalog životních událostí, úkonů na žádost, evidence adres výkonu agend, evidence veřejnoprávních smluv, Realizace Opendat RPP.
RPP, rozvoj, analýza datového modelu, analýza procesu plnění a užívání údajů

Je potřeba naplnit údaji nový ISoISVS, pokrývající ale všechny IS úřadů v jejich celém životním cyklu a v integraci nejenom na agendy a služby, ale i na všechny klíčové ekonomické a projektové centrální služby veřejné správy a jejich IS. Je nutné přizpůsobit stávající údaje v RPP dle zákona 12/2020 Sb. tak aby byly datovou základnou k poskytovaným službám OVM
RPP, začlenění ISoISVS do RPP a další rozvoj
Je potřeba vybudovat nový ISoISVS, pokrývající ale všechny IS úřadů v jejich celém životním cyklu a v integraci nejenom na agendy a služby, ale i na všechny klíčové ekonomické a centrální služby veřejné správy a jejich IS.
B
Digitální Česko – rozvoj ROB a souvisejících AIS v důsledku přijetí ZoPDS a dalších zákonů
Předmětem tohoto záměru je realizace úprav: 1. V Registru obyvatel (ROB) zejména v důsledku přijetí zákona č. 12/2020 Sb. o právu na digitální služby, mezi které patří např. rozšíření okruhu evidovaných údajů, úprava lhůty pro výmaz záznamů údajů z tohoto registru, editace osob zemřelých od 1. 7. 2010 do 30. 6. 2016, realizace úprav navazujících IS apod. 2. Souvisejících s provozem agendových informačních systémů správních evidencí (AIS EOP a AIS ECD) a výrobního systému CDBP v důsledku přijatého zákona o právu na digitální služby a souvisejících zákonů, Nařízení EU 2019/1157 a zákona o občanských průkazech. 3. Související s provozem agendového informačního systému evidence obyvatel: a) Dopady legislativy do procesů zápisu údajů a využívání údajů prostřednictvím formulářů CzechPOINT, b) Digitalizace přihlašovacích lístků k trvalému pobytu.
Rozšiřování počtu Service Providerů (SeP), připojených do NIA
Rozšiřování SeP v Národním identitním prostoru. Navazuje na podobný bod kontrolní pořadí=2306008 s textem: Plně implementovat služby kvalifikovaného systému dle zákona 250/2017 Sb. A to jak vnějších systémů, tak do vnitřních systémů
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu
C
Metodická podpora zavedení DTM ČR
Výzkumný projekt na podporu zavedení DTM ČR, který bude financován z BETA2 (bude těsně navazovat na záměr Jednotný výměnný formát Digitální technické mapy (JVF DTM).
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí
Tento záměr by měl sloužit k centrální správě číselníků, které jsou použity v RPP, např. pro katalog služeb událostí, situací, rolí apod., potřebných pro řízení běhu eGovernmentu a k implementaci legislativních změn v roce 2020 (změna zákona o bankách; DEPO II), přístupy SPUU k ZR, agendám, JIP/KAAS
Vysokorychlostní datová síť krajů a technologická centra krajů
Záměr byl navržen Asociací krajů ČR a týká se výstavby a rozvoje Vysokorychlostní datové sítě krajů a technologických center krajů. Je (údajně) v souladu s Memorandem o podpoře výstavby, rozvoje a využívání telekomunikačních datových sítí veřejné správy mezi Ministerstvem vnitra, Svazem měst a obcí ČR a Asociací krajů ČR.
Ministerstvo zemědělství
A
Vybudování přístupového bodu ke službám elektronické identifikace, MZe
Předmětem záměru je vybudování jednoho centrálního autentizačního prvku resortu Ministerstva zemědělství, poskytujícího interní autentizační služby a zprostředkovávajícího přístup k externím autentizačním službám, zejména NIA a JIP/KAAS. Centrální autentizační prvek zcela odstíní agendové informační systémy a aplikace resortu MZe od detailů autentizace. Cílový agendový systém či aplikace obdrží od centrálního prvku elektronické identifikace informace o identitě, bez ohledu na to, jaký poskytovatel identitních služeb byl pro autentizaci využit. Zda byl využit interní poskytovatel identitních služeb (LDAP/AD) či externí poskytovatelé, jako jsou NIA a JIP/KAAS. Díky vybudování jednotného centrálního přístupového bodu ke službám elektronické identifikace bude v jednotlivých agendových systémech a aplikacích resortu MZe velmi jednoduché implementovat podporu autentizace prostřednictvím NIA a JIP/KASS. Agendové systémy a aplikace budou napojeny na centrální autentizační

prvek resortu a tím budou automaticky akceptovat identity pocházejících z prostoru všech integrovaných identitních služeb. Napojení všech agendových systémů a aplikací rezortu MZe na centrální autentizační prvek umožní okamžitě akceptovat identity JIP/KAAS pro přihlášení ke všem těmto systémům a aplikacím pro fyzické osoby v roli úředníka. Budoucí integrace jakékoli identitní služby již nebude mít na cílové agendové systémy a aplikace žádný dopad. Veškeré změny se v takovém případě odehrají čistě na straně centrálního autentizačního prvku a pro cílové systémy a aplikace budou zcela transparentní.
Národní úřad pro kybernetickou a informační bezpečnost
A
Navyšování integrity sítí kritické informační infrastruktury
NÚKIB poskytuje metodickou i technickou podporu všem subjektům kritické informační infrastruktury. Je určeno více než 100 prvků kritické informační infrastruktury.
Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR
Vytvoření mechanismu spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Popsáno v Akčním plánu a Národní strategii kybernetické bezpečnosti České republiky na období let 2015–2020.
Poskytování služeb GovCERT veřejným institucím a provozovatelům strategicky významných sítí
Vládní CERT České republiky (GovCERT.CZ) kontinuálně poskytuje široké spektrum služeb veřejným institucím, subjektům kritické informační infrastruktury (KII), významných informačních systémů (VIS) a provozovatelům základní služby (PZS).
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020
Splnění všech úkolů vyjmenovaných v Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 schválila Vláda České republiky 25. května 2015, Akční plán je dlouhodobě realizován a pro vládu pravidelně jednou ročně vyhodnocován.
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti
E-learningové kurzy kybernetické bezpečnosti pro vybrané cílové skupiny – úředníky a manažery kybernetické bezpečnosti.
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány.
Spolupráce kontinuálně prováděná a zlepšována. Zároveň je průběžně vyhodnocována v každoroční Zprávě o stavu kybernetické bezpečnosti ČR.
Zřízení nezávislého znaleckého a standardizačního centra (KII)
Centrum by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků strategické informační infrastruktury.
B
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence
Kybernetickou bezpečnost považuje za jednu z priorit jak rámcový program EU pro výzkum a inovace Horizont Evropa, tak paralelní program Digitální Evropa zřizující síť center digitální inovace s cílem aplikovat nové technologie v praxi a uvést úspěšně na trh nové postupy nebo výrobky s důrazem na malé a střední podniky. Tyto a další programy zaměřené na kybernetickou bezpečnost by mělo podle návrhu nařízení EP a Rady [COM (2018) 630 final – 2018/0328 (COD)] nově provádět Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost („kompetenční centrum“) a jím řízená síť národních koordinačních center v jednotlivých členských státech („národní koordinační centra“). Národní koordinační centrum kybernetické bezpečnosti bude podle tohoto nařízení vykonávat NÚKIB, a mezi jeho hlavní úkoly bude patřit zejména podpora centrálního celoevropského kompetenčního centra při dosahování jeho cílů, posuzování žádostí potenciálních nových členů komunity kompetencí pro kybernetickou bezpečnost na národní úrovni, usnadňování účasti místního průmyslu a dalších hráčů na přeshraničních projektech, provádění osvěty a další. Zlepší se tak dostupnost a možnost čerpání EU prostředků především pro subjekty působící v oblasti výzkumu, vývoje a inovací kybernetické bezpečnosti.
Správa základních registrů
A
[P] Program – Základní registry 2.0

Program Základní registry 2.0 (ZR 2.0) vznikl na základě projednaného a schváleného Cílového konceptu ZR 2.0 a s tím související Operační strategie ZR 2.0 vládou ČR dne 10. 10. 2018 (č. usnesení 650).
Program ZR 2.0 obsahuje projekty jednotlivých správců systémů ZR (tedy ROB, RPP, RÚIAN, ROS, ISZR a ORG) a dalších prioritních systémů (např. eGSB/ISSS), které reagují na 12 níže uvedených prioritních oblastí rozvoje ZR definovaných v Cílovém konceptu ZR 2.0.
Jedná se o:
1) Zajištění bezodstávkového provozu ZR.
2) Rozšíření množiny referenčních údajů vedených v ZR.
3) Podporu interoperability v rámci EU (zohlednění role ZR ČR v rámci interoperabilní veřejné správy EU).
4) Zpřístupnění data a služeb prostřednictvím otevřených dat a služeb.
5) Vedení historie údajů v ZR.
6) Zavedení autoritativních údajů a rozvoj propojeného datového fondu.
7) Obnovu infrastruktury ZR/sdílené platformy.
8) Optimalizaci komunikační infrastruktury a datových center.
9) Činnosti ke zlepšení spolupráce jednotlivých ZR
10) Dořešení evidence cizinců (EJFO) v ROB.
11) Posílení kontroly ze strany správců registrů a vytvoření administrativních nástrojů pro správce ZR.
12) Vybudování „interního testovacího“ a „vývojového“ prostředí ZR.
Význam a využití ZR bude v následujících letech dále růst, zejména s ohledem na:
1. Rozvoj propojeného datového fondu poskytující další zdroje údajů z klíčových oblastí výkonu VS (doprava, zdravotnictví, sociální služby apod.).
2. Rozvoj elektronické identifikace občanů, cizinců a zástupců právnických osob a dokončení portálu občana.
3. Využívání služeb ZR i ze strany soukromoprávních subjektů. Pro rozvoj digitálních služeb a růst produktivity hospodářství ČR je důležité, aby sdílené služby eGovernmentu (ZR, e-identifikace, datové schránky a další) mohly být využívány nejprve silně regulovanými podnikatelskými odvětvími (bankovnictví a pojišťovnictví, energetika, telekomunikace a vodárenství atd.) a postupně i dalšími soukromoprávními subjekty.

Národní certifikační autorita (NCA)

Předmětem projektu je vybudování Národní certifikační autority (dále taká „NCA“), zabezpečení jejího provozu a zajištění dalšího rozvoje. Vybudováním NCA vznikl systém podřízených certifikačních autorit pro vydávání:
• kvalifikovaných certifikátů pro elektronický podpis,
• kvalifikovaných elektronických časových razítek,
• kvalifikovaných certifikátů pro elektronické pečetě.
SZR splnila veškeré zákonné požadavky, které jsou na poskytovatele kvalifikovaných služeb kladeny a na základě správního rozhodnutí odboru eGovernmentu MVČR ze dne 30. 4. 2019 byla zapsána jako pátý subjekt v ČR na „Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru“. Vybudováním NCA se SZR stala kvalifikovaným poskytovatelem a správcem všech částí NCA a s tím související infrastruktury.
Projekt je členěn na tyto fáze:
Fáze 1 a fáze 2: 08/2018–03/2020
Předmětem této fáze je zejména:
• Vytvoření primárně požadovaných služeb NCA a implementace s tím souvisejícího HW a SW v izolovaných sítích jednotlivých bezp. složek.
• Zavedení specializovaných funkcionalit pro správu NCA.
• Vytvoření dokumentace systému, certifikačních politik apod.
• Zajištění školení uživatelů NCA a operátorů RA
• Vytvoření analýz rozvoje NCA
Fáze 3: 03/2020-12/2020
• Vytvoření funkcionality pro vzdálené on-line poskytování služeb kvalifikovaných elektronických časových razítek (fyzicky umístěné v prostředí SZR). Řešení je určené primárně pro MV a nezabezpečené sítě BS.
• Implementace opatření dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
• Pořízení dodatečného HW pro potřeby BS.
Fáze 4: 1/2021 - dále
• Vydávání komerčních certifikátů
• Vytvoření funkcionality pro vzdálené on-line poskytování služeb elektronických pečetí
• Vybudování CA pro vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek VS

• Ověřování platnosti kvalifikovaných el. podpisů a pečetí • Vytvoření druhého stromu CA pro vydávání certifikátů s ECC technologií S ohledem na další požadavky BS a požadované provozní parametry poskytovaných služeb, budou původně předpokládané náklady na zajištění provozu a rozvoje NCA vyčerpány v roce 2020 a pro roky 2021+ bude nezbytné zajistit další financování, doporučené je cestou veřejné pokladní správy.
Rozvoj NIA – Národního bodu el. identifikace a autentizace
Systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci. IS se skládá ze základního federačního modulu – národního bodu – a přidružených komponent poskytujících vlastní proces elektronické identifikace a komunikaci s jednotlivými poskytovateli identit a poskytovateli služeb.V roce 2020 pokračuje implementací modulu CUL a realizací nového mobilního IdP.
B
Implementace ZoPDS v prostředí SZR – ISZR, ISSS / eGSB
V souvislosti s realizací změn dopadajících na systém ISZR a ISSS/eGSB po přijetí ZoPDS a s tím provedených novel příslušných zákonů je nezbytné zabezpečit požadavky vyvolané legislativou.
ÚV – úřad vlády
B
Revize agend dle RPP
Revize stávajících agend v RPP (A48, A611, A866,868)