

Příloha č. 1

Zápisu o podmínkách DISOSS

Detailní technická specifikace ISOSS

Obsah

1.	Seznam zkratek a pojmů	3
2.	Úvod	4
3.	Popis realizace Technického týmu (TECH)	5
3.1	Popis stávajícího stavu.....	5
3.2	Budoucí stav.....	11

1. Seznam zkratk a pojmů

Pojem	Výklad
AIS	Agendový informační systém
APL	Tým Aplikační
CAAIS	Centrální autentizační a autorizační informační systém
DISOSS	Projekt Delimitace ISOSS na ÚV ČR
EKIS MV	Ekonomický informační systém MV
EOSM	Evidence obsazovaných služebních míst
EUÚZ	Evidence uskutečněných úřednických zkoušek
HTP	Hlavní tým projektu
HW	Hardware
ISDS	Informační systém datové schránky
ISOSS	Informační systém o státní službě
ISZR	Informační systém základní registry
JIP/KAAS	Jednotný identitní prostor, Katalog autentizačních a autorizačních služeb
MN	Manažer nastavení OIT
MV	Ministerstvo vnitra České republiky
NAKIT	Národní agentura pro komunikační a informační technologie, s. p.
NMV	Náměstek ministra vnitra
OČ	Obecná část úřednické zkoušky
OIT	Odbor informačních technologií
OPRE	Dřívější název (Odbor provozu a rozvoje EKIS), nyní OIT
OSYS	Organizační struktura a systemizace
PPÚZ	Portál pro přihlašování a úřednickou zkoušku
PS	Pracovní skupina
ROB	Registr obyvatel
RPP	Registr práv a povinností
RZ	Rejstřík státních zaměstnanců a zaměstnanců ve služebních úřadech
ŘT	Řešitelský tým
ŘV	Řídící výbor
SAP	Název firmy, název produktu
SAP BTP	SAP Business Technology Platform
SAP ETD	SAP Enterprise Thread Detection
SAP NW	SAP NetWeaver
SAP NW PI	SAP NetWeaver Process Integration
SAP SM	SAP Solution Manager
SP	Tým Smluvně právní
SSS	Sekce pro státní službu
SW	Software
SZ	Státní zaměstnanec
S4ISOSS	Technický název projektu „Upgrade ISOSS“
TECH	Technický tým
ÚV ČR	Úřad vlády České republiky
ÚZ	Úřednická zkouška
VP	Vedení projektu
ZČ	Zvláštní část úřednické zkoušky
ZP	Změnový požadavek
ZPP	Zaměstnanec v pracovním poměru

2. Úvod

Tento dokument shromažďuje a popisuje technické části a procesy, které jsou součástí nebo jinak spojené se systémem ISoSS a na které má proces delimitace dopad v podobě změny nebo reimplementace.

Na obsah kapitoly „3.2 - Budoucí stav“ je odkazováno z dokumentu „Zápis o delimitaci“, resp. dílčí kapitoly tohoto dokumentu.

3. Popis realizace Technického týmu (TECH)

3.1 Popis stávajícího stavu.

3.1.1 Souhrn informací a předpokladů

Současný stav systému ISoSS je ovlivněn následujícími skutečnostmi a plány na jeho rozvoj:

- ISoSS je v rozsahu HW infrastruktury v současné době hostován společností NAKIT v SP CSS a následně je poskytován včetně podpory MV ČR na základě smlouvy o Hostingu s platností do 03/2028,
- Aplikačně je ISoSS v současné době podporován ze strany společnosti NAKIT pro MV ČR na základě Rámcové smlouvy o podpoře s platností do 03/2027,
- ISoSS je jako SAP systém evidován v rámci skupiny SAP systémů Ministerstva vnitra a sdílí některé komponenty společně se systémem EKIS MV,
- Před předáním ISoSS Úřadu vlády proběhne v rámci projektu S4ISOSS povýšení aplikačních komponent ISoSS na nové verze SW, případně na nové generace produktů SAP. Při upgrade dojde i ke změně HW infrastruktury, finální stav po upgrade je zachycen v kapitole 3.2.3.

3.1.2 Přehled HW

Obsah a struktura kapitoly popisuje stávající stav HW, budoucí stav je popsán v kapitole 3.2.2.

3.1.2.1 Přehled HW infrastruktury

HW infrastruktura je v současném hostingu společná pro systémy MV EKIS a ISoSS a svým nastavením a provázaností je neoddělitelná.

PN	Popis	Množství v 1 nodu
	Compute cluster	
7Y94CTO5WW	Server ThinkAgile VX 2U Node	10
5641PX5	XClarity Pro, Per Endpoint w/5 Yr SW S&S	10
5PS7A23877	Essential ThinkAgile CN - 5Yr 24x7 4Hr Resp + YDYD VX 2U	10
7S06CTOEWW	VMware vSAN	10
	Management cluster	
7Y93CTO4WW	Server Lenovo ThinkAgile VX 1U Certified Node	4
5641PX5	XClarity Pro, Per Endpoint w/5 Yr SW S&S	4
5PS7A23777	Essential ThinkAgile CN - 5Yr 24x7 4Hr Resp + YDYD VX 1U	4
7S06CTOEWW	VMware vSAN	4
	DB Cluster	
7Y94CTO6WW	VX 2U VSAN 768GB Node for SAP HANA 2x 6238R 28c : Lenovo ThinkAgile VX 2U Certified Node for SAP HANA	9
5641PX5	XClarity Pro, Per Endpoint w/5 Yr SW S&S	9
5PS7A87388	Premier Essential ThinkAgile CN - 5Yr 24x7 4Hr Resp + YDYD VX 2U	9
7S06CTOEWW	VMware vSAN	9

7Y94CTO6WW	VX 2U VSAN 3TB Node for SAP HANA 2x 8276L 28c : Lenovo ThinkAgile VX 2U Certified Node for SAP HANA	14
5641PX5	XClarity Pro, Per Endpoint w/5 Yr SW S&S	14
5PS7A87388	Premier Essential ThinkAgile CN - 5Yr 24x7 4Hr Resp + YDYD VX 2U	14
7S06CTOEWW	VMware vSAN	14
	VMware vCenter	
7S06070YWW	VMware vCenter Server 7 Standard for vSphere 7 (Per Instance) w/Lenovo 5Yr S&S	1
	VMware vRealize Operations	
7S060933WW	VMware vRealize Operations 8 Advanced (25 OSI Pack) w/Lenovo 5Yr S&S	3
7S060930WW	VMware vRealize Operations 8 Advanced (Per CPU) w/Lenovo 5Yr S&S	8
7S060933WW	VMware vRealize Operations 8 Advanced (25 OSI Pack) w/Lenovo 5Yr S&S	2

3.1.2.2 Přehled virtuálních serverů ISOSS – databázový cluster

Systém	Hostname	IP adresa	Prostředí	Popis
SH3	sh3d1v	-	PROD	HR backend – primární DB instance
SH3	sh3d2v	-	PROD	HR backend – záložní DB instance
SB3	sb3d1v	-	PROD	BW – primární DB instance
SB3	sb3d2v	-	PROD	BW – záložní DB instance
SX3	sx3d1v	-	PROD	PO middleware – primární DB instance
SX3	sx3d2v	-	PROD	PO middleware – záložní DB instance
SP3	sp3d1v	-	PROD	Portál – primární DB instance
SP3	sp3d2v	-	PROD	Portál – záložní DB instance
SH2	sh2d1v	-	TEST	HR backend – primární DB instance
SH2	sh2d2v	-	TEST	HR backend – záložní DB instance
SX2	sx2d1v	-	TEST	PO middleware – DB instance
SP2	sp2d1v	-	TEST	Portál – DB instance
SH1	sh1d1v	-	DEV	HR backend – DB instance
SB1	sb1d1v	-	DEV	BW – DB instance
SX1	sx1d1v	-	DEV	PO middleware – DB instance
SP1	sp1d1v	-	DEV	Portál – DB instance
SH4	sh4d1v	-	T3S	HR backend – DB instance
SX4	sx4d1v	-	T3S	PO middleware – DB instance
SP4	sp4d1v	-	T3S	Portál – DB instance

3.1.2.3 Přehled virtuálních serverů ISSS – výpočetní cluster

Systém	Hostname	IP adresa	Prostředí	Popis
SH3	sh3c1v	-	PROD	HR backend CI
SH3	sh3a1p	-	PROD	HR backend AS
SH3	sh3a2p	-	PROD	HR backend AS
SB3	sb3c1v	-	PROD	BW CI
SP3	sp3c1v	-	PROD	Portál CI
SP3	sp3a1p	-	PROD	Portál AS

SP3	sp3a2p	-	PROD	Portál AS
SQ3	sq3c1v	-	PROD	Portál proxy
SX3	sx3c1v	-	PROD	PO middleware CI
SY3	sy3c1v	-	PROD	PO proxy
SR3	sr3c1v	-	PROD	saprouter PROD
SH2	sh2c1v	-	TEST	HR backend CI
SH2	sh2a1p	-	TEST	HR backend AS
SH2	sh2a2p	-	TEST	HR backend AS
SP2	sp2c1v	-	TEST	Portál CI
SP2	sp2a1p	-	TEST	Portál AS
SP2	sp2a2p	-	TEST	Portál AS
SQ2	sq2c1v	-	TEST	Portál proxy
SX2	sx2c1v	-	TEST	PO middleware CI
SY2	sy2c1v	-	TEST	PO proxy
SR2	sr2c1v	-	TEST	saprouter PROD
SH1	sh1c1v	-	DEV	HR backend CI
SB1	sb1c1v	-	DEV	BW CI
SP1	sp1c1v	-	DEV	Portál CI
SX1	sx1c1v	-	DEV	PO middleware CI
SH4	sh4c1v	-	T3S	HR backend CI
SP4	sp4c1v	-	T3S	Portál CI
SQ4	sq4c1v	-	T3S	Portál proxy
SX4	sx4c1v	-	T3S	PO middleware CI
SY4	sy4c1v	-	T3S	PO proxy

3.1.3 Systémy ISoSS

3.1.3.1 Přehled systémů ISoSS

Funkční celek ISoSS se skládá z několika systémů, které využívají produkty SAP.

Značka	Produkt SAP	Význam
SH	SAP ECC R/3	Hlavní komponenta, backend systém
SX	SAP NetWeaver 7.5 PI/PO	Integrační server, zajištění veškerých rozhraní na externí systémy
SP	SAP NetWeaver 7.5 Enterprise Portal	Portál ISoSS, prezentační vrstva pro externí uživatele
SB	SAP NetWeaver 7.5 Business Warehouse	Manažerský informační systém, slouží pouze pro potřeby sekce pro státní službu.

3.1.3.2 Sdílené komponenty

Pro provoz a monitoring ISoSS jsou využívány komponenty, které náleží do landscape EKIS MV a jsou z tohoto landscape neoddělitelné.

Jsou využívány jak produktivní instance k vykonávání reálných procesů a funkcí, tak vývojové instance, na kterých se připravují a testují nové nebo upravené funkce.

Systém	Hostname	IP adresa	Prostředí	Popis
SM3	ssmsap3	-	PROD	Solution Manager
ET3	etddb1	-	PROD	Enterprise Threat Detection
SM1	ssmsap1	-	DEV	Solution Manager
ET1	etddb1	-	DEV	Enterprise Threat Detection

Popis procesů a funkcí, které jsou ve sdílených systémech řešeny pro ISOSS:

- Solution Manager
 - Generování a údržba kmenových dat systémů ISOSS, generování licenčních klíčů, plánování aktualizací systémů ISOSS, stahování servisních balíčků – pouze SM3,
 - Evidence HelpDesk požadavků – vytváření kmenových dat business partnerů z prostředí Portál ISOSS pomocí integrace přes SAP NW PI; vytváření incidentů z prostředí Portál ISOSS pomocí integrace přes SAP NW PI, incidenty navázané na kmenová data business partnerů,
- Enterprise Threat Detection
 - Sběr logů a monitoring činností uživatelů v systémech ISOSS,
 - Systémy SH a SP odesílají data průběžně pomocí SAP RAL (Read Access Logging)
 - Je implementováno doplňkové rozhraní pro export logů přihlášení a specifických aktivit portálových uživatelů ISOSS,
 - Na vyžádání pracovníků sekce pro státní službu provádí pověření uživatelé z OIT MV analýzu a vyhodnocení zaznamenaných událostí,

3.1.3.3 Správa uživatelů systémů ISOSS

Správa uživatelů jednotlivých systémů ISOSS je prováděna v každém systému zvlášť pracovníky MV OIT.

Značka	Produkt SAP	Popis
SH	SAP ECC R/3	Zakládají se uživatelé backend systémů tj. pracovníci sekce pro státní službu, manažeři nastavení, konzultanti podpory NAKIT. Pro PROD systém SH3 je zavedena jmenná konvence: - EKXXXXXXXXXXXX - externí konzultant - MNXXXXXXXXXXXX - manažer nastavení (OIT) - SSXXXXXXXXXXXX - uživatel Sekce pro Státní službu - TSXXXXXXXXXXXX - testovací uživatel - SUXXXXXXXXXXXX - uživatel správního úřadu
SX	SAP NetWeaver 7.5 PI/PO	Zakládají se techničtí uživatelé ve formátu TUXXXXXXXXXX pro potřebu přihlašování externích personálních informačních systémů služebních úřadů; přidělují se jim komerční certifikáty, <u>které se průběžně aktualizují</u> . Proces žádání o vytvoření tech. uživatele je popsán v dokumentu Technický manuál ISOSS.
SP	SAP NetWeaver 7.5 Enterprise Portal	Dva typy uživatelů: • servisní uživatelé MV OIT a NAKIT - vytvoření, setrvalý stav, • personalisté služebních úřadů - jsou vytvářeni automaticky přebíráním ověřených informací z JIP/KAAS.

SB	SAP NetWeaver 7.5 Business Warehouse	Zakládají se uživatelé backend systémů tj. pracovníci sekce pro státní službu, manažeři nastavení, konzultanti podpory NAKIT.
----	---	---

Pro generování unikátní číselné části uživatelských ID se používá zákaznická transakce v systému SH3.

3.1.4 Ostatní systémy a služby s dopadem na provoz ISoSS

Kromě vlastních systémů SAP je pro komplexní funkčnost nutné zajistit řadu dalších servisních úkonů a aktivit. Některé jsou vykonávány průběžně, jiné jsou dlouhodobě neměnné, nicméně převod systému ISoSS pod ÚV ČR znamená minimálně jednorázový proces změny.

3.1.4.1 Domény

Seznam externích rozhraní:

Rozhraní	IP adresa	DNS	Popis
Portál ISoSS			
Webové služby ISoSS			
T3S Portál ISoSS			
T3S WS ISoSS - internet			
T3S WS ISoSS - CMS			
Saprouter PROD			Nutno vypublikovat do CMS pro ÚV. Bude instalován nový SAPROUTER.
Saprouter TEST			Nutno vypublikovat do CMS pro ÚV. Bude instalován nový SAPROUTER.
TEST Portál ISoSS			Nutno vypublikovat do CMS pro ÚV

3.1.4.2 Certifikáty

Seznam certifikátů použitých v systémech ISoSS:

CN	Platnost do	Vydavatel	Použití
	29.9.2026	Thawte TLS RSA CA G1	SSL rozhraní produkčního portálu
	6.10.2026	PostSignum Public CA 5	SSL rozhraní produkčních WS
	13.10.2026	PostSignum Public CA 5	SSL rozhraní T3S portálu
	13.10.2026	PostSignum Public CA 5	SSL rozhraní T3S WS v internetu
	31.10.2026	PostSignum Public CA 5	SSL rozhraní T3S WS v CMS
	24.9.2025	PostSignum Public CA 5	SSL rozhraní testovacího portálu

devportal.isoss.gov.cz	31.10.2026	HST Issuing CA G1	SSL rozhraní vývojového portálu
Informační systém o státní službě	26.8.2026	PostSignum Qualified CA 4	El. podpis odpovědí ISoSS
ISoSS	5.7.2026	PostSignum Public CA 4	Autentizace do JIP / ISDS
ISoSS.cz	3.12.2026	ISZR CA	Autentizace do ISZR
ISoSS-TEST	5.6.2026	PostSignum Public CA 4	Autentizace do JIP / ISDS TEST
ISoSS.cz	3.12.2026	ISZR CA TEST	Autentizace do ISZR TEST

Kromě těchto certifikátů jsou na systémech instalovány SSL certifikáty od interní CA služby Hosting, které slouží výhradně pro mezi-systémovou komunikaci v rámci perimetru ISoSS. Obnovu těchto certifikátů zajišťuje bázev podpora prostřednictvím CA Hosting.

3.1.4.3 Záznamy RPP

ISoSS jako AIS státní správy je registrován v RPP pod ID A1761. Tento AIS je napárován na organizaci MV.

V RPP jsou dále definovány činnostní role pro práci v systému ISoSS.

Aktuální přehled záznamů agendy: https://rpp-ais.egon.gov.cz/gen/agendy-detail/A1761_01012025.xlsx

3.1.4.4 Integrace na externí autentizační službu

Pro běžné portálové uživatele, tj. uživatele-personalisty služebních úřadů, je v současné době využívána externí autentizační služba JIP/KAAS.

Uživatelé na Portálu ISOSS jsou automaticky zakládáni po úspěšném přihlášení v prostředí JIP/KAAS a za předpokladu, že má externí uživatel přiděleno alespoň jednu činnostní roli AIS A1761.

3.1.4.5 Aditivní datová schránka v ISDS

Systém ISoSS využívá k některým procesům tzv. aditivní datovou schránku ISoSS, id. t88358j. Datová schránka je zřízena pro MV.

3.1.4.6 Přístup do ISZR

Ze zákona může systém ISoSS přistupovat do ISZR ROB (dříve uvedeno v zák.234/2014, §183; nyní zák.111/2009, §5). Přístup do ISZR ROB je realizován formou volání webových služeb ISZR pomocí integračního serveru SAP PI/PO. Pro přístup k webovým službám je vlastníkem systému zajišťováno:

- seznam IP adres, ze kterých jsou webové služby ISZR volány.
- generování přihlašovacího certifikátu – zajišťuje automat ISZR. V současné době zajišťuje  z MV OIT 1x za 3 roky. Vydání, resp. obnova certifikátu za Úřad vlády bude dohodnuto s DIA CZ, viz. text níže.

3.1.4.7 SMTP a emailová adresa ServiceDesk ISoSS

Systém ISoSS využívá k některým procesům odesílání emailových notifikací. K tomu je na integračním serveru SX a backend systému SH nastaveno spojení na SMTP server ministerstva vnitra (smtp://10.254.11.5) a je vytvořen účet přihlášení.

3.2 Budoucí stav

3.2.1 Definice a předpoklady pro provedení delimitace ISoSS

Hlavní parametry:

- ÚV ČR v souladu s § 2 odst. 1 písm. d) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, pověří provozováním ISoSS MV ČR a současně s ním dojedná komplexní provozní podporu.
- O tomto ÚV ČR uzavře s MV ČR samostatný Zápis.
- HW infrastruktura a nastavení zůstane nezměněno, resp. ve stavu po upgrade projektu S4ISOSS.
- Stav potrvá do konce životnosti HW hosting, které je stanoveno na 03/2028. Po tomto datu bude ÚV řešit nový HW hosting a provoz ISoSS samostatně.

Technické předpoklady pro provedení delimitace systému:

- Pracovníkům sekce pro státní službu, která je převáděna pod ÚV ČR, budou ponechány přístupy do systémů ISoSS ve stejném stavu a rozsahu. Přístup k systémům ISoSS bude zprostředkován skrze síť ÚV ČR.
- Pracovníci sekce pro státní službu budou nadále využívat MOTP aplikaci k generování tokenů pro autentizaci JIP/KAAS.
- Pracovníci IT odboru ÚV budou mít zpřístupněné systémy ISoSS. Bude definován seznam uživatelů a k nim specifikované role, na základě kterých bude zřízen přístup do relevantních systémů.
- Manažeři nastavení z MV OIT budou využívat stávající přístup do ServiceDesk systému SM3, který bude i nadále využit jako centrální evidence požadavků na podporu a rozvoj ISoSS.

3.2.2 HW, infrastruktura a provoz

3.2.2.1 HW infrastruktura

Proces delimitace ISoSS na HW infrastrukturu nebude mít žádný dopad.

3.2.2.2 Přehled virtuálních serverů ISOSS – databázový cluster

Popis virtuálních serverů finálního stavu po dokončení projektu S4ISOSS, resp. v momentu finální verze CK projektu S4ISOSS, část TNŘ („technický návrh řešení“ - interní dokument poskytovatele hosting).

Systém	Hostname	IP adresa	Prostředí	Popis
SH3	sh3d1v	-	PROD	HR backend – primární DB instance
SH3	sh3d2v	-	PROD	HR backend – záložní DB instance
EC3	???	-	PROD	SIS middleware – primární DB instance
EC3	???	-	PROD	SIS middleware – záložní DB instance
SP3	???	-	PROD	Portál – primární DB instance
SP3	???	-	PROD	Portál – záložní DB instance
SH2	sh2d1v	-	TEST	HR backend – primární DB instance
SH2	sh2d2v	-	TEST	HR backend – záložní DB instance
SP2	???	-	TEST	Portál – DB instance
SH1	sh1d1v	-	DEV	HR backend – DB instance
EC1	eic-npr.isoss.local	-	DEV	SIS middleware – DB instance
SP1	???	-	DEV	Portál – DB instance
SH4	sh4d1v	-	T3S	HR backend – DB instance
SP4	???	-	T3S	Portál – DB instance

3.2.2.3 Přehled virtuálních serverů ISSS – výpočetní cluster

Popis virtuálních serverů finálního stavu po dokončení projektu S4ISOSS, resp. v momentu finální verze CK projektu S4ISOSS, část TNŘ („technický návrh řešení“ - interní dokument poskytovatele hosting).

Systém	Hostname	IP adresa	Prostředí	Popis
SH3	sh3c1v	-	PROD	HR backend CI
SH3	sh3a1p	-	PROD	HR backend AS
SH3	sh3a2p	-	PROD	HR backend AS
SH2	sh2c1v	-	TEST	HR backend CI
SH2	sh2a1p	-	TEST	HR backend AS
SH2	sh2a2p	-	TEST	HR backend AS
SH1	sh1c1v	-	DEV	HR backend CI
SH4	sh4c1v	-	T3S	HR backend CI

3.2.2.4 Síťová infrastruktura

Systém ISOSS je umístěn v prostředí CMS a je publikován veřejnými službami pro přístup personalistů služebních úřadů do Portálu ISOSS, případně pro volání webových služeb ISOSS z personálních systémů služebních úřadů. Portál ISOSS je navíc publikován do internetu.

Pracovníci sekce pro státní službu budou k systému ISOSS přistupovat přes prostředí CMS.

Objekt/budova Jindřišská bude vybaven IT infrastrukturou od ÚV, bude propojen dedikovanou linkou do sítě ÚV. Tzn. pracovníci sekce pro státní službu v roli uživatelů ISoSS budou k ISoSS přistupovat přes síťové spojení do ÚV -> CMS -> ISoSS.

Pro možnost vzdálené práce v ISoSS bude pracovníkům sekce pro státní službu zřízeno VPN připojení do ÚV, následně bude funkční síťový přístup stejný viz. výše. VPN přístup bude možné využít i v případě technických komplikací při výměně síťové infrastruktury v objektu Jindřišská, VPN přístupy budou vytvořeny v dostatečném předstihu.

Portál

Přístup do produkčního portálu ISoSS bude probíhat standardně přes internet, jelikož je služba publikovaná do internetu.

- Pro přístup do testovacího portálu ISoSS bude rozhraní vypublikováno na adrese testportal.isoss.cms2.cz, služba bude vypublikována jako neveřejná, pouze pro ÚV ČR.

HR / MIS systém

Přístup do HR / MIS systému prostřednictvím klienta SAP GUI bude realizován pomocí komponenty SAPRouter. Na straně ÚV je možné využít stávající SAPRouter používaný pro systém EKISGOV. Na straně ISoSS bude rozhraní SAPRouteru publikováno do CMS jako neveřejná služba pro klienta ÚV. Toto řešení zajistí šifrování spojení mezi oběma saproutery v přenosové síti CMS a zjednoduší požadavky na konektivitu pracovních stanic.

Vývojové prostředí

Přístup koncových uživatelů do vývojového prostředí se nepředpokládá. Toto prostředí zůstane i nadále přístupné pouze z VPN služby Hosting pro pracovníky dodavatele podpory.

3.2.2.5 Kontrola provozu, zadávání požadavků, notifikace

HW infrastruktura je provozována dodavatelem NAKIT. Smluvní vztah na hosting zůstává v režimu MV ČR – NAKIT. Požadavky na úpravu a odstávky jsou realizovány pomocí Helpdesk systému „CA“ v NAKIT, vybraní zaměstnanci MV – OIT do helpdesk systému mají přístup, dostávají z něj v případě výpadků notifikace. Z technických důvodů do systému nemůže být zaveden jiný/další subjekt.

ÚV ČR bude pro zadávání požadavků na HW infrastrukturu spolupracovat s MV – OIT. Pracovníci MV – OIT budou notifikace Helpdesk systému NAKIT, které jsou relevantní k systému ISoSS přeposílat na emailovou adresu IT oddělení ÚV ČR: it@uvcr.cz. IT oddělení ÚV ČR dále zajistí metodiku/způsob přesměrování technických požadavků do svého Helpdesk systému ÚV ČR (Alvao).

3.2.2.6 Požadavky na podporu a rozvoj ISOSS

Samostatnou množinou požadavků na podporu tvoří dotazy externích subjektů:

- od zástupců služebních úřadů z personálních a IT oddělení, kteří ověřují technicko-metodické postupy, případně nefunkčnosti přístupů apod.,
- od zástupců dodavatelů personálních systémů do státní správy, kteří např. testují nové funkcionality a změny svých po novelizaci legislativy.

Požadavky na podporu jsou zasílány na emailovou adresu ServiceDesk ISoSS MV

o vypořádání se starají manažeři nastavení ISoSS, přičemž některé požadavky jsou vyřízeny obratem (cca 40-60% dle aplikačního modulu ISoSS), složitější jsou předávány na další úroveň podpory formou zaevidování v SAP Solution Manager SM3 (viz. popis níže).

Statistika počtu požadavků za období:

- za Q1 2025 - cca 500, zaevidovaných 276 (vlivem změny legislativy k 1.1.2025)
- za rok 2024 - cca 900, zaevidovaných 605
- za rok 2023 - cca 1000, zaevidovaných 690

Emailová adresa SD ISoSS MV bude k datu delimitace sekce pro státní službu přesměrována na adresu IT oddělení ÚV ČR zajistí přístup manažerů nastavení MV OIT k mailové schránce prostřednictvím WEB UI. V průběhu Q1/2026 bude pracovníky IT oddělení ÚV ČR zprovozněno automatické předávání požadavků z mailové schránky do mailové schránky včetně následného automatického zpracování reakcí a vytvoření odpovědí k odeslání původním žadatelům.

3.2.3 Systémy ISoSS

Všechny systémy budou převedeny jako celek ve stavu a konfiguraci po dokončení projektu Upgrade ISoSS.

3.2.3.1 Přehled systémů ISoSS

Funkční celek ISoSS se skládá z několika systémů, které byly aktualizovány na nové verze/nahrazeny novými produkty v rámci projektu S4ISOSS.

Značka	Produkt SAP	Význam
SH	SAP S/4 HANA	Hlavní komponenta, backend systém
EC	SAP Integration Suite Edge Cell	Integrační broker v lokální síti, zajištění veškerých rozhraní na externí systémy
SP	---	Portál ISoSS, prezentační vrstva pro externí uživatele

3.2.3.2 Sdílené systémy – Solution Manager

Agenda evidence požadavků na podporu a rozvoj bude vykonávána v systému SM3.

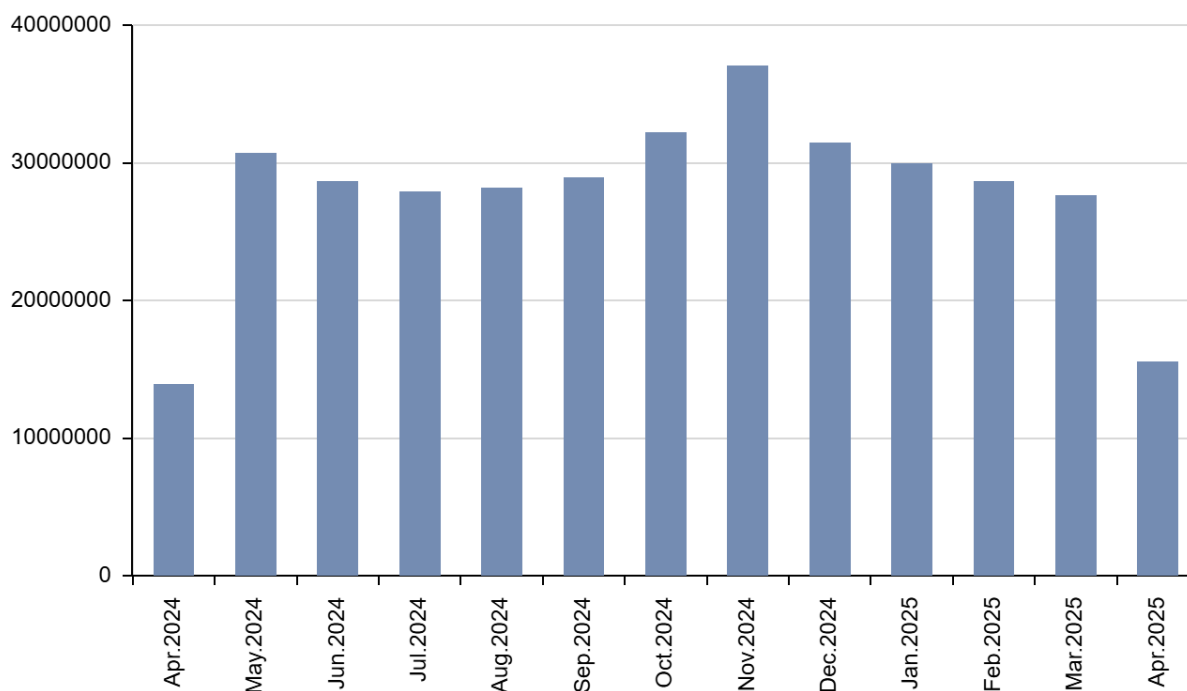
- Generování a údržbu kmenových dat systémů ISoSS zajistí pracovníci MV – OIT ve spolupráci s dodavatelem administrátorských prací, společností NAKIT.

- Evidence HelpDesk požadavků – požadavky ISOSS jsou evidovány samostatně pomocí tzv. „servisní skupiny“ s hodnotou „MV_MN_ISOSS“.
- Bude vytvořen program pro export měsíčního přehledu požadavků na podporu a rozvoj v domluvené struktuře. Exportní dávka bude zasílána automaticky na emailovou adresu mv.oit@mvcr.cz. Program pro export zajistí pracovníci MV OIT, včetně monitoringu jeho měsíčního spuštění.

3.2.3.3 Sdílené systémy – Enterprise Threat Detection

Systém SAP Enterprise Threat Detection bude pro potřeby ISOSS využíván ve stávajícím režimu. Do systému jsou zasílány logy procesů a zpracování standardním nastavením RAL ze systémů SH, SP a SB a dále pak uživatelských akcí na Portálu ISOSS zákaznickým vývojem přes SAP PO. Analýza dat bude prováděna pracovníky MV OIT a to pouze na vyžádání sekce pro státní službu a/nebo pracovníky IT oddělení ÚV ČR.

Za roční období 4/2024 – 4/2025 se pro systémy ISOSS jedná o cca. 350 mil. událostí přenesených ze zdrojových systémů:



Objem přenesených dat bohužel není možné zjistit. Pro představu, v archivovaných záznamech v CSV formátu má jeden záznam (událost) průměrně kolem 1 kB, zdrojová data událostí na výstupu ze SAP systémů mohou ale být vyšší (formátování, režie přenosového protokolu, šifrování atd.).

3.2.3.4 Správa uživatelů systémů ISoSS

Proces zakládání a aktualizace uživatelských účtů v backend systémech ISoSS (systémy SH, integrace) bude nadále zajišťován pracovníky MV – OIT. Požadavky na založení/administraci uživatelských účtů budou zasílány na adresu 

3.2.4 Ostatní systémy a služby s dopadem na provoz ISoSS

3.2.4.1 Domény

Registrované veřejné domény budou převedeny na subjekt Úřad vlády ČR (SB:VP106-RIPE_XX). Změnu iniciuje současný vlastník, ÚV ČR změnu potvrdí.

- Doména isoss.cz (původní doména ISoSS, zde je nutné zajistit rezervaci domény min. 10 let), vlastník MV ČR
- Doména isoss.gov.cz (nová doména v rámci přechodu na GOV domény), registrátor DIA
- Doména isoss.cms2.cz (nová doména pro rozhraní v prostředí CMS), registrátor NAKIT

Jelikož jsou některé neveřejné služby konzumovány ze sítě MV přímo (mimo prostředí CMS), bude nutné zajistit publikování těchto služeb do CMS pro klienty ÚV. Pro způsob publikování bude rozhodující síťové prostředí pracovních stanic uživatelů Sekce pro Státní službu. Publikaci služeb do CMS zajistí NAKIT ve spolupráci s ÚV ČR.

3.2.4.2 Certifikáty

Nasazené komerční a kvalifikované certifikáty budou během roku 2025 obnoveny podle stávajících platností (viz tabulka níže). O obnovu certifikátů zažádá MV - OIT.

V rámci procesu přenosu domény zajistí odbor IT ÚV ČR vydání certifikátů dle tohoto seznamu:

Systém	Platnost do	Předmět	Vydavatel	Použití
SX3, SX4	26.08.2026	serialNumber=S91490,CN=Informační systém o státní službě,O=Ministerstvo vnitra České republiky,organizationIdentifier=NTRCZ-00007064,C=CZ	PostSignum QCA4	el. podpis
SX3	03.12.2026	CN=ISoSS.cz,OU=6618-E/PROD,O=00007064,ST=Ministerstvo vnitra,C=CZ	ISZR CA	x.509 autentizace
SX3	05.06.2026	serialNumber=S91490,CN=ISoSS,OU=Informační systém o státní službě,O=Ministerstvo vnitra České republiky,organizationIdentifier=NTRCZ-00007064,C=CZ	PostSignum PCA4	x.509 autentizace
SX4, SX1, SX2	03.12.2026	CN=ISoSS.cz,OU=6618-E/TEST,O=00007064,ST=Ministerstvo vnitra,C=CZ	ISZR CA TEST	x.509 autentizace
SX4, SX1, SX2	05.06.2026	serialNumber=S91490,CN=ISoSS-TEST,OU=Informační systém o státní službě,O=Ministerstvo vnitra České republiky,organizationIdentifier=NTRCZ-00007064,C=CZ	PostSignum PCA4	x.509 autentizace
SY3	06.10.2026	serialNumber = D91490, CN = ws.isoss.cms2.cz , O = Ministerstvo vnitra České republiky, OID.2.5.4.97 = NTRCZ-00007064, L = Praha, C = CZ	PostSignum PCA5	SSL
SY4	13.10.2026	serialNumber = D91490, CN = t3sww.isoss.gov.cz , O = Ministerstvo vnitra České republiky, OID.2.5.4.97 = NTRCZ-00007064, L = Praha, C = CZ	PostSignum PCA5	SSL
SQ2	13.10.2026	serialNumber = D91490, CN = testportal.isoss.gov.cz , O = Ministerstvo vnitra České republiky, OID.2.5.4.97 = NTRCZ-00007064, L = Praha, C = CZ	PostSignum PCA5	SSL
SQ3	29.09.2026	CN = portal.isoss.gov.cz , O = Ministerstvo vnitra, L = Praha, C = CZ	Thawte TLS CA	SSL

SQ4	13.10.2026	serialNumber = D91490, CN = t3sportal.isoss.gov.cz , O = Ministerstvo vnitra České republiky, OID.2.5.4.97 = NTRCZ-00007064, L = Praha	PostSignum PCA5	SSL
-----	------------	---	-----------------	-----

Vystavení nových certifikátů pod hlavičkou ÚV bude možné až po formálním převedení vlastnictví domén, pro které jsou certifikáty vystaveny, případně převedení dalších služeb a agend. Bylo dohodnuto, že vystavení nových certifikátů zajistí ÚV ČR na konci května 2026 a to pro všechny servery/prostředky. Certifikáty by měly být připravené k 31.5.2026, aby bylo provedeno nasazení v termínu 1.-5.6.2026.

Vystavení certifikátu certifikační autoritou pro přístup k základním registrům bude provedeno jako následný krok po převedení agendy A1761 pod Úřad vlády v RPP. Postup je popsána na stránkách DIA: [Digitální a informační agentura - Připojení agendových informačních systémů k základním registrům](#)

3.2.4.3 Záznamy RPP

Převod na subjekt Úřad vlády ČR bude proveden ve spolupráci s DIA CZ tak, aby dopad do funkčnosti návazných systémů (JIP/KAAS/CAAIS, ISZR) a zejména dopad na koncové uživatele, tj. personalisty služebních úřadů, byl co nejmenší. Převod je předběžně potvrzen se zástupci DIA CZ na 1.1.2026, je veden v ServiceDesk DIA CZ pod číslem 223348.

3.2.4.4 Integrace na externí autentizační službu

Při delimitaci ISOSS a změně konfigurace integrace na JIP/KAAS bude zároveň změněna externí autentizační služba na CAAIS. Technické napojení na CAAIS je plánováno v projektu S4ISOSS. Pokud bude projekt S4ISOSS realizován, bude při delimitaci ISOSS změněn pouze externí subjekt přistupující k CAAIS. Aktivita budou provedeny v návaznosti na změny v RPP, viz. výše.

3.2.4.5 Aditivní datová schránka v ISDS

Současná aditivní datová schránka ISOSS, id. `t88358j` bude datem delimitace zrušena. Zástupci ÚV ČR rozhodli, že v prostředí ISOSS ÚV nebude aditivní datová schránka. Místo toho bude využita hlavní datová schránka ÚV, id. `trfaa33`. K této schránce bude přistupováno pomocí automatizovaného rozhraní dle provozního řádu ISDS (<https://info.mojedatovaschranka.cz/info/cs/80.html>).

K 31.12.2025 bude provedena deregistraci klientského certifikátu z nastavení DS `t88358j`, 1.1.2026 zajistí pracovníci ÚV registraci stejného klientského certifikátu k DS `trfaa33`.

Identifikátor datové schránky bude publikován v aktualizaci dokumentu „Technický manuál ISOSS“, viz. kapitola 3.2.6.

Stejný postup bude proveden i v testovacím prostředí datových schránek <https://info.czebox.cz/info/cs/>, které jsou využívány v prostředí ISOSS T3S.

3.2.4.6 Přístup do ISZR

Seznam IP adres, ze kterých jsou webové služby ISZR volány – vzhledem k variantě ponechání ISOSS v současném hostingu, toto nastavení zůstává.

Generování přihlašovacího certifikátu – požadavek na vystavení nových přístupových certifikátů pro volání webových služeb ISZR musí provést ÚV ČR a to po 1.1.2026, kdy se dle záznamů v RPP stane vlastníkem agendy A1761 (AIS 6618). Požadavek musí být zaslán jak pro produktivní prostředí ISZR, tak samostatně pro testovací prostředí.

Po vydání přístupových certifikátů budou tyto nasazeny nejdříve v testovacím prostředí, po úspěšném otestování v produktivním prostředí.

Po úspěšném přechodu na nové certifikáty zašle ÚV jako nový správce A1761 požadavek na zneplatnění certifikátů, které byly vystaveny na MV. MV OIT tento krok udělat nemůže, protože v době požadavku na zneplatnění již systému RAZR ISZR agendu A1761 neuvidí.

Další informace jsou uvedeny v dokumentech:

https://www.szrcr.cz/images/dokumenty/spr%C3%A1vci_AIS/POL010C-2023_Certifikacni_politika_DIA_pro_AIS.pdf

<https://www.szrcr.cz/cs/dulezite-dokumenty/63-p%C5%99%C3%ADru%C4%8Dka-razr-pro-spr%C3%A1vce-ais>

3.2.4.7 SMTP a emailová adresa ServiceDesk ISoSS

Po delimitaci ISOSS je nutné odesílat notifikace z emailového účtu 

IT oddělení ÚV ČR zajistí dostupnost SMTP serveru pro systémy ES a SH, např. vypublicováním do CMS2 jako privátní službu na nestandardním portu a dále vytvoření účtu, pod kterým se budou notifikace odesílat. E-mailové notifikace odchází ze serverů PO a HR (viz. tabulka přehledu virtuálních serverů). V prostředí CMS je veškerý odchozí provoz z ISoSS překládán na zdrojovou adresu MV - 10.252.16.131.

Nezávisle na výše uvedeném bude na poštovním serveru vytvořena emailová adresa pro Helpdesk ISoSS ve tvaru .cz. Současná adresa, resp. mailový koš s adresou  bude k datu delimitace ISoSS na novou adresu přeměrován.

Práce budou průběžně zařizovány pracovníky odboru IT ÚV od 11/2025. Nastavení by mělo být připraveno k testování k 10.12.2025, aby bylo možné nasadit do produktivního systému k 1.1.2026.

3.2.5 Aktivita ovlivňující landscape a nastavení systému ISOSS

Podobu landscape a technické nastavení ISoSS ovlivní projekt Upgrade ISoSS (S4ISOSS), který je plánován na Q2-4/2025 Q1/2026. Aplikační změny (tj. změny funkčnosti modulů ISoSS), které budou během Upgrade ISoSS žádné nebo minimální, nemají na část TECH vliv.

3.2.5.1 Upgrade na S/4HANA

V rámci upgrade zůstane zachována stávající funkcionality ISoSS.

Z technického pohledu dojde k následujícím změnám:

- Upgrade backend systému SH z SAP R/3 na SAP S/4HANA
- Zánik reportovacího systému SAP NW 7.5 BW a jeho nahrazením pomocí komponenty SAP S/4HANA Embedded Analytics and Reporting v backend systému SH
- Generační změna middleware z SAP NW 7.5 Process Integration na produkt SAP BTP Integration Suite
- Generační změna portálu z SAP NW 7.5 Enterprise Portal na jiný produkt

3.2.6 Publikace změn vyplývající z delimitace ISoSS

Delimitace systému ISoSS, práv a povinností a dalších technických náležitostí, které jsou externími subjekty, tj. služebními úřady, ale i dodavateli personálních systémů, využívány v procesu registrace nebo automatické komunikace, je nutné v dostatečném předstihu publikovat. Technické informace jsou popsány v dokumentu „Technický manuál ISoSS“. Tento dokument bude aktualizován a publikován k 8.12.2025 s účinností od 1.1.2026.

Jan
Doubal

Digitálně podepsal
Jan Doubal
Datum: 2026.01.09
14:13:10 +01'00'

Digitálně podepsal
Petra Fojtíková
Ing. Ivo Rosypal
Datum: 2025.12.10
09:59:03 +01'00'