adna Centrum sdílených služeb, s. p.
nce 915/14, Žižkov, 130 00 Praha 3
www.spcss.cz, info@spcss.cz

PROVÁDĚCÍ SMLOUVA Č. 4

(ev. č. Dodavatele 36/2016/UOM-04)

k Rámcové smlouvě na služby související s přípravou a provozem Elektronické evidence tržeb uzavřené dne 26.5.2016 (ev. č. Dodavatele 36/2016/UOM)

Smluvní strany:

Česká republika – Generální finanční ředitelství

se sídlem:	Lazarská 15/7, 117 22 Praha 1
zastoupena:	Ing. Martinem Janečkem
IČO:	720 80 043
DIČ:	CZ72080043
Bankovní spojení:	Česká národní banka
Číslo účtu:	11122011/0710
ID DS:	p9iwj4f

(dále jen „***Objednatel***“ nebo „***GFŘ***“)

a

Státní pokladna Centrum sdílených služeb, s. p.
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze pod sp.zn. A 76922,

se sídlem:	Na Vápence 915/14, Žižkov, 130 00 Praha 3
zastoupený:	Ing. Vladimírem Dzurillou, generálním ředitelem
IČO:	036 30 919
DIČ:	CZ03630919
Bankovní spojení:	Česká spořitelna, a.s.
Číslo účtu:	6303942/0800, IBAN: CZ12 0800 0000 0000 0630 3942
ID DS:	ag5uunk

(dále jen „***Dodavatel***“ nebo „***SPCSS***“)
(Objednatel a Dodavatel dále jednotlivě též jen „***Smluvní strana***“ nebo společně „***Smluvní strany***“)

uzavírají tuto

Prováděcí smlouvu č. 4

(dále jen „***Smlouva***“)

I. ÚVODNÍ USTANOVENÍ

1.1 Smlouva je uzavírána na základě příslušných ustanovení Rámcové smlouvy na služby související s přípravou a provozem Elektronické evidence tržeb (ev. č. Dodavatele 36/2016/UOM) uzavřené dne 26.5.2016 (dále jen „***Rámcová smlouva***").

1.2 Pojmy uvedené s velkými písmeny, které nejsou ve Smlouvě definovány, mají význam stanovený v Rámcové smlouvě.

II. PŘEDMĚT SMLOUVY

2.1 Předmětem Smlouvy je poskytování Služby EET typu S1 (Příprava provozu) poskytované v oblasti Služeb „Infrastruktura" s identifikačním kódem S1-003 a názvem „Příprava infrastruktury Transakční části a Krátkodobého úložiště EET".

2.2 Předmětem Smlouvy je dále poskytování Služby EET typu S1 (Příprava provozu) poskytované v oblasti Služeb „Služby podpory provozu" s identifikačním kódem S1-004 a názvem „Příprava provozního dohledu Transakční části a Krátkodobého úložiště EET".

2.3 Předmětem Smlouvy je dále poskytování Služby EET typu S1 (Příprava provozu) poskytované v oblasti Služeb „Bezpečnost" s identifikačním kódem S1-005 a názvem „Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET".

2.4 Předmětem Smlouvy je dále poskytování Služby EET typu S3 (Provoz a podpora provozu) poskytované v oblastech Služeb „Infrastruktura" a „Služby podpory provozu" s identifikačním kódem S3-001 a názvem „Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET".

2.5 Předmětem Smlouvy je dále poskytování Služby EET typu S3 (Provoz a podpora provozu) poskytované v oblasti Služeb „Bezpečnost" s identifikačním kódem S3-001 a názvem „Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET".

2.6 Předmětem Smlouvy je dále poskytování Služby EET typu S4 (Odborné služby na vyžádání) poskytované v oblasti Služeb „Systémová integrace" s identifikačním kódem S4-003 a názvem „Odborné služby systémové integrace v období provozu služeb".

2.7 Souhrnný přehled Služeb EET dle odst. 2.1 – 2.6

ID Služby EET	Typ Služeb EET dle odst. 4.3 Rámcové smlouvy	Oblast Služeb EET dle odst. 4.2 Rámcové smlouvy	Název
S1-003	Příprava provozu	Infrastruktura	Příprava infrastruktury Transakční části a Krátkodobého úložiště EET
S1-004	Příprava provozu	Služby podpory provozu	Příprava provozního dohledu Transakční části a Krátkodobého úložiště EET
S1-005	Příprava provozu	Bezpečnost	Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET

S3-001	Provoz a podpora provozu	Infrastruktura Služby podpory provozu	Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET
S3-002	Provoz a podpora provozu	Bezpečnost	Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET
S4-003	Odborné služby na vyžádání	Systémová integrace	Odborné služby systémové integrace v období provozu služeb

2.8 Detailní specifikace předmětu plnění Smlouvy je obsažena v příloze č. 1 Smlouvy (Služba EET S1-003), v příloze č. 2 Smlouvy (Služba EET S1-004), v příloze č. 3 Smlouvy (Služba EET S1-005), v příloze č. 4 Smlouvy (Služba EET S3-001), v příloze č. 5 Smlouvy (Služba EET S3-002) a v příloze č. 6 Smlouvy (Služba EET S4-003).

III. DOBA PLNĚNÍ SMLOUVY

3.1 Detailní věcný a časový harmonogram plnění Smlouvy je pro Služby EET typu S1 (Příprava provozu) obsažen v příloze č. 1 Smlouvy (Služba EET S1-003), v příloze č. 2 Smlouvy (Služba EET S1-004) a v příloze č. 3 Smlouvy (Služba EET S1-005).

3.2 Doba plnění Smlouvy pro Služby EET S3-001 a S3-002 je 60 měsíců od 1.12.2016, tj. po celou dobu platnosti Rámcové smlouvy.

3.3 Doba plnění Smlouvy pro Služby EET S4-003 je do vyčerpání částky uvedené pro tuto Službu EET v odst. 4.9, nebo do konce platnosti Rámcové smlouvy, pokud nastane dříve.

IV. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

4.1 Cena za plnění předmětu Smlouvy je stanovena dohodou Smluvních stran následovně.

4.2 Cena za Službu EET S1-003 je uvedena v tabulce v odst 4.5. Platebním milníkem je termín „Ukončení přípravy infrastruktury Transakční části a Krátkodobého úložiště EET" dle harmonogramu realizace v příloze č. 1 Smlouvy.

4.3 Cena za Službu EET S1-004 je uvedena v tabulce v odst 4.5. Platebním milníkem je termín „Ukončení přípravy provozního dohledu Transakční části a Krátkodobého úložiště" dle harmonogramu realizace v příloze č. 2 Smlouvy.

4.4 Cena za Službu EET S1-005 je uvedena v tabulce v odst 4.5. Platebním milníkem je termín „Zavedení bezpečnostního dohledu Transakční části a Krátkodobého úložiště" dle harmonogramu realizace v příloze č. 3 Smlouvy.

4.5 Cenová tabulka Služeb EET typu S1 (Příprava provozu):

Služba EET	Název	Cena bez DPH
S1-003	Příprava infrastruktury Transakční části a Krátkodobého úložiště EET	**14.385.000,- Kč**
S1-004	Příprava provozního dohledu Transakční části a Krátkodobého úložiště EET	**2.845.000,- Kč**

Služba EET	Název	Cena bez DPH
S1-005	Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET	**1.776.000,- Kč**

4.6 Cena za poskytování Služby EET S3-001 je uvedena v tabulce v odst. 4.8.

4.7 Cena za poskytování Služby EET S3-002 je uvedena v tabulce v odst 4.8.

4.8 Tabulka měsíčních cen Služeb EET typu S3 (Provoz a podpora provozu):

Služba EET	Název	Měsíční cena bez DPH v prvním roce provozu*)	Měsíční cena bez DPH v dalších letech provozu
S3-001	Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET	**5.911.000,- Kč**	**5.246.000,- Kč**
S3-002	Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET	**522.000,- Kč**	**522.000,- Kč**

*) prvním rokem provozu se míní prvních 12 měsíců provozu ode dne zahájení poskytování služby

4.9 Cena za plnění Služby EET S4-003 (Odborné služby systémové integrace v období provozu služeb) je stanovena dohodou Smluvních stran následovně. Denní sazba za jednotlivé role odborných služeb činí částku 15.000,- Kč bez DPH. Cena za Službu EET S4-003 bude stanovena dle skutečného akceptovaného plnění v daném období. Celková cena za poskytnutí Služby EET S4-003 nepřekročí částku **2.000.000,- Kč** bez DPH.

4.10 Akceptace plnění Služby EET S4-003 probíhá způsobem popsaným v Rámcové smlouvě. Faktury za poskytnuté a Objednatelem akceptované plnění budou vystaveny vždy za příslušný kalendářní měsíc, ve kterém bylo plnění dle Zadávacího a pověřovacího listu, a to i částečně, poskytnuto.

4.11 Cenu Služeb, resp. měsíční platby, je po dobu trvání této Smlouvy možno překročit o procento odpovídající míře inflace podle oficiálních údajů Českého statistického úřadu. Míra inflace bude pro účely této Smlouvy vyjádřena přírůstkem průměrného ročního indexu spotřebitelských cen vyhlášeného Českým statistickým úřadem. K navýšení může dojít pouze jednou ročně k 1. dubnu příslušného kalendářního roku, přičemž poprvé může k navýšení dojít k 1. dubnu 2018, a to o míru inflace za období roku 2017.

V. DALŠÍ PODMÍNKY PLNĚNÍ SMLOUVY

5.1 Detailní specifikace součinnosti Objednatele je obsažena v příloze č. 1 Smlouvy (Služba EET S1-003), v příloze č. 2 Smlouvy (Služba EET S1-004), v příloze č. 3 Smlouvy (Služba EET S1-005), v příloze č. 4 Smlouvy (Služba EET S3-001), v příloze č. 5 Smlouvy (Služba EET S3-002) a v příloze č. 6 Smlouvy (Služba EET S4-003).

5.2 V případě ukončení poskytování plnění dle této Smlouvy z důvodu skončení její platnosti, případně její výpovědi jakoukoliv ze Smluvních stran, bude nejpozději 6 měsíců před účinností jejího skončení zahájena v součinnosti obou Smluvních stran příprava činností vedoucích k řádnému ukončení poskytování Služeb dle Smlouvy a následnému předání Objednateli či jeho novému dodavateli (tzv. exit plán). Toto neplatí v případě odstoupení od Smlouvy kteroukoli ze Smluvních stran.

5.3 Činnosti vedoucí k řádnému ukončení poskytování Služeb dle Smlouvy a případnému následnému předání Objednateli či jeho novému dodavateli ve smyslu odst. 5.2 proběhnou následujícím způsobem a v následujícím rozsahu. 6 měsíců před účinností ukončení Smlouvy vznikne společná pracovní skupina Dodavatele a Objednatele, zahrnující zástupce obou stran z oblasti technické, ekonomické i právní. Pracovní skupina vytvoří plán ukončení poskytování Služeb a následného předání Objednateli či jeho novému dodavateli (tzv. Exit plán), který bude nejpozději 3 měsíce před termínem ukončení Smlouvy schválen oběma stranami. Neschválení Exit plánu v uvedeném termínu bude řešeno do 5 pracovních dnů na jednání oprávněných osob Objednatele i Dodavatele ve věcech obchodních a smluvních. Exit plán může obsahovat činnosti provozního, dokumentačního a školicího charakteru, včetně předávání znalostí a podpory migrace, související s předmětem a rozsahem Služeb dle Smlouvy. V období 3 měsíců před ukončením Smlouvy budou oběma stranami vykonávány činnosti obsažené v Exit plánu.

5.4 V případě předčasného ukončení této Smlouvy nebo Rámcové smlouvy, a to bez ohledu na důvod ukončení, se z důvodu rozsáhlých finančních investic Dodavatele na počátku smluvního období, které vynaložil za účelem řádného poskytování služeb Objednateli, Smluvní strany dohodly na úhradě těchto investic v případě, že nebude uzavřena jiná písemná dohoda o způsobu využití nakoupených technologií určených pro poskytování Služeb, které jsou předmětem této Smlouvy. Objednatel se zavazuje, že Dodavateli v závislosti na časovém období, ve kterém k předčasnému ukončení dojde, uhradí na pokrytí těchto investic částku stanovenou v níže uvedené tabulce (viz „Tabulka úhrad"). Objednatel s určenou výší těchto částek souhlasí. Určená částka bude fakturována Dodavatelem Objednateli nejdéle do 30 dnů ode dne účinnosti předčasného ukončení Smlouvy nebo Rámcové smlouvy. Splatnost faktury se řídí ustanoveními Rámcové smlouvy.

Tabulka úhrad

Od	Do	Částka bez DPH
	31.5.2017	80.626.131,56 Kč
1.6.2017	30.11.2017	69.771.720,02 Kč
1.12.2017	31.5.2018	58.917.308,48 Kč
1.6.2018	30.11.2018	54.060.089,78 Kč
1.12.2018	31.5.2019	43.205.678,24 Kč
1.6.2019	30.11.2019	38.348.459,54 Kč
1.12.2019	31.5.2020	27.494.048,00 Kč
1.6.2020	30.11.2020	23.890.459,22 Kč
1.12.2020	31.5.2021	14.289.677,60 Kč
1.6.2021	30.11.2021	10.686.088,82 Kč

VI. OSTATNÍ A ZÁVĚREČNÁ USTANOVENÍ

6.1 Vzhledem k tomu, že ADIS je prvkem kritické informační infrastruktury, Objednatel je vázán zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, a vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (společně dále jen „ZoKB").

6.2 Dodavatel je povinen během plnění předmětu Smlouvy bezodkladně informovat Objednatele o všech zjištěných rizicích v oblasti bezpečnosti informací, které by mohly mít dopad na Objednatele či ohrozit zájmy a bezpečnost Objednatele. Současně je Dodavatel povinen bezodkladně provést kroky směřující k odstranění uvedených rizik. O takto provedených krocích musí Dodavatel Objednatele rovněž bezodkladně informovat. Dodavatel je oprávněn si vyžádat u Objednatele potřebnou součinnost při odstranění uvedeného rizika.

6.3 Objednatel je na základě ZoKB povinen provádět kontrolu a audit kritické informační infrastruktury. Dodavatel se zavazuje poskytnout Objednateli potřebnou součinnost při provádění kontroly a auditu kritické informační infrastruktury.

6.4 Veškerá ujednání Smlouvy navazují na Rámcovou smlouvu a Rámcovou smlouvou se řídí, tj. práva, povinnosti či skutečnosti neupravené ve Smlouvě se řídí ustanoveními Rámcové smlouvy.

6.5 V případě, že ujednání obsažené ve Smlouvě se bude odchylovat od ustanovení obsaženého v Rámcové smlouvě, má ujednání ve Smlouvě přednost před ustanovením obsaženým v Rámcové smlouvě, ovšem pouze ohledně plnění sjednaného ve Smlouvě. V otázkách Smlouvou neupravených se použijí ustanovení Rámcové smlouvy.

6.6 Je-li nebo stane-li se jakékoli ustanovení Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení Smlouvy. Smluvní strany se tímto zavazují nahradit do 5 (pěti) pracovních dnů po doručení výzvy druhé Smluvní strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

6.7 Smluvní strany berou na vědomí, že Smlouva včetně jejích příloh a případných dodatků může být uveřejněna na internetových stránkách Objednatele a na jeho profilu zadavatele, případně v registru smluv, vztahuje-li se na ni povinnost uveřejnění prostřednictvím registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Případné uveřejnění v registru smluv zajistí Objednatel.

6.8 Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem 1. 12. 2016.

6.9 Smlouva je vyhotovena ve 4 (slovy: čtyřech) vyhotoveních, z nichž Objednatel obdrží 2 (slovy: dvě) vyhotovení a Dodavatel 2 (slovy: dvě) vyhotovení.

6.10 Nedílnou součástí Smlouvy jsou následující přílohy:

- Příloha č. 1 – Popis Služby EET S1-003 (Příprava infrastruktury Transakční části a Krátkodobého úložiště EET);
- Příloha č. 2 – Popis Služby EET S1-004 (Příprava provozního dohledu Transakční části a Krátkodobého úložiště EET);
- Příloha č. 3 – Popis Služby EET S1-005 (Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET);
- Příloha č. 4 – Popis Služby EET S3-001 (Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET);
- Příloha č. 5 – Popis Služby EET S3-002 (Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET);
- Příloha č. 6 – Popis Služby EET S4-003 (Odborné služby systémové integrace v období provozu služeb);

Smluvní strany shodně prohlašují, že si Smlouvu před jejím podpisem přečetly a že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.

Za Objednatele:

V Praze dne 30.11.2016

Česká republika – Generální finanční ředitelství

Ing. Martin Janeček, generální ředitel

Za Dodavatele:

V Praze dne 29.11.2016

Státní pokladna Centrum sdílených služeb, s. p.

Ing. Vladimír Dzurilla, generální ředitel

SPCSS

Státní pokladna Centrum sdílených služeb, s. p.
Na Vápence 915/14, Žižkov, 130 00 Praha 3
IČ:03630919 (1)

POPIS SLUŽBY EET S1-003

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S1-003**
Název	**Příprava infrastruktury Transakční části a Krátkodobého úložiště EET**
Oblast Služeb	Infrastruktura
Typ Služeb	Příprava provozu

2. POPIS SLUŽBY

2.1 Účel, architektura a prostředí

Účelem poskytnutí Služby EET S1-003 je příprava infrastruktury Transakční části a Krátkodobého úložiště EET pro poskytování Služby EET S3-001 („Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET", viz příloha č. 3 Smlouvy). Součástí Služby EET S1-003 je pořízení, instalace, konfigurace, testování a pilotní provoz infrastruktury dle popisu v této příloze.

Architektura Transakční části a Krátkodobého úložiště EET je detailně popsána v návrhovém dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET") a sestává z následujících komponent:

- Umístění v Národním datovém centru SPCSS;
- Bezpečné propojení a připojení k Internetu;
- SSL akcelerátory a load balancery;
- XML akcelerátory;
- RISC servery;
- Aplikační komponenty ADIS EETAP a EETDB, včetně aplikačních serverů Tomcat a DB Informix;
- Platforma diskových úložišť a zálohování SPCSS.

V rámci Služby EET S1-003 jsou vybudována čtyři provozní prostředí:

- Produkční prostředí - dvě nezávislá střediska umístěná ve dvou nezávislých místnostech v rámci NDC SPCSS;
- Testovací prostředí – jedno středisko;
- Zkušební prostředí – jedno středisko;
- Vývojové prostředí – zjednodušená verze Transakční části pro účely vývoje úprav konfigurací.

Součástí Služby EET S1-003 je pilotní provoz prostředí Playground. Prostředí Playground bylo vybudováno a samostatně provozováno v rámci Služby EET S1-001 („Playground a podpora

vývojářů", viz příloha č. 1 Prováděcí smlouvy č. 2 Rámcové smlouvy) do termínu zahájení pilotního provozu.

2.2 Rozsah infrastruktury

Rozsah připravované infrastruktury je detailně popsán v návrhovém dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET".

Infrastruktura v majetku Dodavatele, která bude v rámci Služby EET S3-001 poskytována jako služba, včetně služeb podpory provozu:

- Umístění ve dvou nezávislých místnostech v rámci NDC, energie, chlazení, včetně provozních a bezpečnostních služeb NDC v rozsahu potřebném pro níže uvedená zařízení a služby;
- Redundantní vysokokapacitní bezpečné připojení k Internetu a NIX o kapacitě minimálně 1Gb/s a maximálně 10Gb/s;
- Propojení do sítí GFŘ prostřednictvím GOVBONE;
- Bezpečné propojení – 1 zákaznický modul v rozsahu potřebném pro níže uvedená zařízení a služby;
- Stavový firewall – 4 instance;
- SSL akcelerátor a load balancer – 4 instance;
- SAN v rozsahu potřebném pro níže uvedená zařízení a služby – celkově 100 SAN portů;
- RISC servery v celkovém rozsahu 112 core a 1088 GB RAM, rozdělené do 28 virtuálních serverů;
- Disková úložiště v celkovém rozsahu 80 TB hrubé diskové kapacity, což zahrnuje:
  - Disková úložiště pro systémové disky všech virtuálních serverů,
  - Disková úložiště pro produkční prostředí v rozsahu odpovídajícím 6,1TB čistého databázového prostoru a 1TB NFS úložiště pro každé středisko, včetně prostoru pro minimálně 2 snapshoty databáze,
  - Disková úložiště pro databáze testovacího a zkušebního prostředí,
  - Diskový prostor potřebný pro redundance uložení (RAID);
- Zálohovací systém a páskové úložiště v rozsahu odpovídajícím zálohování výše uvedeného systému podle RTO a RPO požadavků popsaných v definici Služby EET S3-001 – celkový rozsah záloh 40TB;
- SW verze XML akcelerátoru běžící na 4 core virtuálního serveru vmWare – po jednom ks pro Playground a vývojové prostředí.

Infrastruktura a SW v majetku Objednatele, která je předána Dodavateli do správy a na které budou v rámci Služby EET S3-001 poskytovány služby podpory provozu:

- XML akcelerátor – 6 ks;
- Diskové pole IBM FlashSystem 900 – 4 ks;
- 2-node diskový systém IBM SVC – 4 ks;
- Aplikační server Apache Tomcat pro aplikační servery všech prostředí;
- DB Informix pro DB servery všech prostředí;
- Aplikační moduly ADIS EETAP a EETDB pro všechna prostředí.

2.3 Aplikační konfigurace a testovací nástroje

Součástí Služby EET S1-003 je i konfigurace aplikačních pravidel XML akcelerátorů ve všech prostředích v souladu s dokumentem „Formát a struktura údajů o evidované tržbě a popis datového rozhraní pro příjem datových zpráv evidovaných tržeb", zveřejněného Objednatelem na web stránkách www.etrzby.cz (sekce IT/Vývojář) a souvisejícími pracovními podklady předanými Objednatelem.

Aplikační konfigurace XML akcelerátoru byla na základě stejné specifikace dlouhodobě spravována a testována na prostředí Playground v rámci služby S1-001.

Součástí Služby EET S1-003 je také vytvoření testovacího nástroje pro zasílání datových zpráv evidovaných tržeb. Nástroj slouží k funkčnímu i regresnímu testování aplikační konfigurace XML akcelerátorů a zasílání testovacích tržeb pro účely testování a ověření funkcionality dalších částí EET. Nástroj je dále obecně použitelný na testování WebServices. Nástroj bude v průběhu přípravy i provozu systému využíván pracovníky Dodavatele i Objednatele. Dodavatel zaručuje, že nástroj neprovádí žádné úkony vyjma těch, která jsou součástí popsané funkčnosti.

Nástroj je vytvořen formou rozšíření a konfiguračních úprav open source aplikace SoapUI (www.soapui.org), distribuované pod EUPL licencí (European Union Public Licence). Spolu s testovacím nástrojem Dodavatel připraví Objednateli Uživatelský a instalační manuál a instalační balík pro distribuci pracovníkům Objednatele.

Podpisem Smlouvy uděluje Dodavatel Objednateli k těmto rozšířením, konfiguračním úpravám a dokumentaci nevýhradní, převoditelnou licenci, s právem udělit podlicenci, s udělením práva na užívání, rozmnožování, provádění úprav či jiných změn, překládání, spojování s jiným dílem a zařazování do děl souborných, a to bez časového, územního nebo množstevního omezení.

2.4 Testování

Rozsah testů infrastruktury je detailně popsán v návrhovém dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET", a zahrnuje následující oblasti testů:

- Testy testovacího nástroje na zasílání tržeb;
- Testy konfigurace Transakční části;
- Testy komponent EETAP a EETDB ADIS;
- Zátěžové testy a testy vysoké dostupnosti;
- Ověření v pilotním provozu.

Testy jsou prováděny s vědomím Objednatele a účastí jeho pracovníků dle potřeby nebo na vyžádání Objednatele. Výstupem z testů bude dokument „Souhrnná zpráva o provedení testů infrastruktury Transakční části a Krátkodobého úložiště EET", který je zároveň formálním výstupem Služby EET S1-003.

2.5 Pilotní provoz

Pilotní provoz EET bude probíhat v listopadu 2016. Pilotní provoz slouží poplatníkům k otestování jejich pokladních zařízení a vlivu EET na jejich prodejní a účetní procesy. Pilotní provoz probíhá v plném rozsahu funkcionality EET, na produkčním prostředí a s využitím produkčních certifikátů poplatníků.

Z pohledu provozu infrastruktury jde o provoz a správu všech prostředí Transakční části a Krátkodobého úložiště EET v kompletním rozsahu uvedeném v této příloze.

Z pohledu služeb podpory provozu jde o kompletní rozsah podpory provozu dle popisu Služby EET S3-001 s tím, že procesy řízení provozu budou v tomto období podléhat řízení Projektu etržby a SLA sankce nebudou uplatňovány.

2.6 Dokumentace

K termínu milníku Ukončení poskytování Služby EET S1-003 bude Objednateli předán dokument „**Technická dokumentace infrastruktury Transakční části a Krátkodobého úložiště EET**". Dokument je aktualizací návrhového dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" a jeho rozšíření o konfigurační dokumentaci.

3. HARMONOGRAM REALIZACE

Milník	Termín
Ukončení přípravy infrastruktury Transakční části a Krátkodobého úložiště EET	30.11.2016

4. DEFINICE VÝSTUPŮ

Formálním výstupem Služby EET S1-003 je dokument **„Souhrnná zpráva o provedení testů infrastruktury Transakční části a Krátkodobého úložiště EET"**, který bude předán k připomínkám Objednateli první pracovní den po termínu ukončení přípravy infrastruktury.

5. ZPŮSOB AKCEPTACE

Akceptační řízení Služby EET S1-003 bude zahájeno k termínu předání dokumentu „Souhrnná zpráva o provedení testů infrastruktury Transakční části a Krátkodobého úložiště EET" a provedeno formou hodnocení a akceptace výstupu typu „dokument" (dále jen „hodnocení dokumentu" a „akceptace dokumentu"), popsanou v této kapitole.

Obecná akceptační kritéria pro typ výstupu „dokument" jsou jednoznačnost, věcná správnost, srozumitelnost a gramatická správnost. Hodnocení a akceptace dokumentu probíhá metodou připomínkového řízení s následujícím postupem:

- Dodavatel předá dokument k hodnocení vedoucímu projektu Objednatele nebo přímo příslušnému hodnotiteli dle Registru kvality Projektu e-tržby Objednatele;
- Příslušný hodnotitel zpracuje do 5 pracovních dnů od předání připomínky k dokumentu a zaznamená je v Protokolu z hodnocení výstupu, který předá Vedoucímu projektu Objednatele a Dodavateli;
- Po zpracování případných připomínek předá Dodavatel dokument společně s Protokolem z hodnocení výstupu a návrhem Akceptačního protokolu vedoucímu projektu Objednatele nebo přímo příslušnému schvalovateli dle Registru kvality Projektu e-tržby Objednatele;
- Schvalovatel zpracuje a podepíše Akceptační protokol.

Objednatel si může vyžádat jako součást připomínkového hodnocení předvedení části testů.

6. POŽADOVANÉ SOUČINNOSTI

- Pro zařízení v majetku Objednatele zajistí Objednatel odborné instalační práce a podporu při testování, předání do správy SPCSS, přístup k L3 produktové podpoře.
- Objednatel je odpovědný za vytvoření a aktualizace dokumentu „Formát a struktura údajů o evidované tržbě a popis datového rozhraní pro příjem datových zpráv evidovaných tržeb" a souvisejících interních podkladů Objednatele popisujících požadovanou funkcionalitu aplikační konfigurace XML akcelerátoru.
- Objednatel je zodpovědný za dodávku a L3 podporu aplikačních modulů ADIS pro Krátkodobé úložiště, včetně dodávky a podpory DB Informix a aplikační podpory při instalaci a testování.
- Objednatel zajistí účast příslušných hodnotitelů a schvalovatelů na akceptačním řízení služby.

POPIS SLUŽBY EET S1-004

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S1-004**
Název	**Příprava provozního dohledu Transakční části a Krátkodobého úložiště EET**
Oblast Služeb	Služby podpory provozu
Typ Služeb	Příprava provozu

2. POPIS SLUŽBY

2.1 Účel a architektura provozního dohledu

Účelem poskytnutí Služby EET S1-004 je příprava provozního dohledu Transakční části a Krátkodobého úložiště EET pro poskytování Služby EET S3-001 („Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET", viz příloha č. 4 Smlouvy). Součástí Služby EET S1-004 je rozšíření, konfigurace a testování platformy provozního dohledu SPCSS dle popisu v této příloze.

Primárním účelem provozního dohledu (monitoringu) v rámci podpory provozu je automatizované sledování funkčnosti a chybových stavů systému v reálném čase, urychlení detekce a tím i řešení incidentů a vad, včetně incidentů a vad ovlivňujících provozní SLA. Sekundárními účely provozního dohledu jsou automatizované sledování stavu a výkonu systému a proaktivní detekce hrozících chybových stavů.

Architektura provozního dohledu Transakční části a Krátkodobého úložiště EET je detailně popsána v návrhovém dokumentu „Návrh provozního dohledu Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy) a využívá následující komponenty platformy provozního dohledu SPCSS:

- CA Spectrum pro dohled síťové infrastruktury;
- CA Unified Infrastructure Monitoring (UIM) pro dohled IT komponent;
- CA Application Performance Management (APM) pro dohled aplikací z pohledu koncového uživatele (E2E, end2end);
- CA Service Operations Insight (SOI) pro dohled komplexních IT služeb.

Architektura provozního dohledu Transakční části a Krátkodobého úložiště EET umožňuje sledovat provozní stavy:

- síťové infrastruktury;
- SAN infrastruktury;
- HW;
- operačních systémů;

- databází;
- aplikací;
- komplexních IT služeb;
- E2E pohledu na služby.

V průběhu implementace provozního dohledu budou zpracovány detailní tabulky metrik a jejich hraničních hodnot, které budou předloženy ke schválení Objednateli a následně se stanou součástí dokumentace.

2.2 Rozsah provozního dohledu

Rozsah připravovaného provozního dohledu je detailně popsán v návrhovém dokumentu „Návrh provozního dohledu Transakční části a Krátkodobého úložiště EET".

Provozní dohled pokryje infrastrukturu a služby Transakční části a Krátkodobého úložiště EET definovanou v popisu Služby EET S1-003 a popsanou detailně v návrhovém dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy), včetně aplikačních komponent ADIS EETAP a EETDB.

Provozní dohled bude provozován v kompletním rozsahu primárně pro provozní prostředí a Playground. Provozní dohled pro testovací a zkušební prostředí může být zjednodušený, ale umožní sledovat stav jednotlivých komponent a stav plnění SLA relevantních pro tato prostředí.

Součástí provozního dohledu bude i poskytování informace o dostupnosti/funkčnosti Transakční části pro automatizované zveřejnění na webu www.etrzby.cz

2.3 Dočasné řešení provozního dohledu

Vzhledem k probíhajícímu projektu konsolidace a rozšíření platformy provozního dohledu SPCSS bude v momentě zahájení poskytování Služby EET S3-001 k dispozici dočasné řešení provozního dohledu založené primárně na platformě CA Spectrum a CA APM. Dočasné řešení poskytne rozsah provozního dohledu omezený na kritické funkce:

- Sledování dostupnosti jednotlivých komponent infrastruktury;
- End2End sledování dostupnosti a odezvy služby Příjem tržeb;
- Sledování a vyhodnocování aplikačních transakcí služby Příjem tržeb.

2.4 Testování

Rozsah testů provozního dohledu je detailně popsán v návrhovém dokumentu „Návrh provozního dohledu Transakční části a Krátkodobého úložiště EET", a zahrnuje následující oblasti testů:

- Testy konfigurace doménových manažerů (CA Spectrum, CA UIM, CA APM);
- Propagace alarmů z doménových manažerů do CA SOI a vyhodnocení vlivu na služby.

Testy jsou prováděny s vědomím Objednatele a účastí jeho pracovníků dle potřeby nebo na vyžádání Objednatele. Výstupem z testů bude dokument „Souhrnná zpráva o provedení testů provozního dohledu Transakční části a Krátkodobého úložiště EET", který je zároveň formálním výstupem Služby EET S1-004.

2.5 Dokumentace

K termínu milníku Ukončení přípravy provozního dohledu bude Objednateli předán dokument „**Technická dokumentace provozního dohledu Transakční části a Krátkodobého úložiště EET**". Dokument je aktualizací návrhového dokumentu „Návrh provozního dohledu Transakční části a Krátkodobého úložiště EET" a jeho rozšíření o konfigurační dokumentaci.

3. HARMONOGRAM REALIZACE

Milník	Termín
Dočasné řešení provozního dohledu Transakční části a Krátkodobého úložiště EET	30.11.2016
Ukončení přípravy provozního dohledu Transakční části a Krátkodobého úložiště EET	31.3.2017

4. DEFINICE VÝSTUPŮ

Formálním výstupem Služby EET S1-004 je dokument „**Souhrnná zpráva o provedení testů provozního dohledu Transakční části a Krátkodobého úložiště EET**", který bude předán k připomínkám Objednatele první pracovní den po termínu Ukončení přípravy provozního dohledu.

5. ZPŮSOB AKCEPTACE

Akceptační řízení Služby EET S1-004 bude zahájeno k termínu předání dokumentu „Souhrnná zpráva o provedení testů provozního dohledu Transakční části a Krátkodobého úložiště EET" a provedeno formou hodnocení a akceptace výstupu typu „dokument" (dále jen „hodnocení dokumentu" a „akceptace dokumentu"), popsanou v této kapitole.

Obecná akceptační kritéria pro typ výstupu „dokument" jsou jednoznačnost, věcná správnost, srozumitelnost a gramatická správnost. Hodnocení a akceptace dokumentu probíhá metodou připomínkového řízení s následujícím postupem:

- Dodavatel předá dokument k hodnocení vedoucímu projektu Objednatele nebo přímo příslušnému hodnotiteli dle Registru kvality Projektu e-tržby Objednatele;
- Příslušný hodnotitel zpracuje do 5 pracovních dnů od předání připomínky k dokumentu a zaznamená je v Protokolu z hodnocení výstupu, který předá Vedoucímu projektu Objednatele a Dodavateli;
- Po zpracování případných připomínek předá Dodavatel dokument společně s Protokolem z hodnocení výstupu a návrhem Akceptačního protokolu vedoucímu projektu Objednatele nebo přímo příslušnému schvalovateli dle Registru kvality Projektu e-tržby Objednatele;
- Schvalovatel zpracuje a podepíše Akceptační protokol.

Objednatel si může vyžádat jako součást hodnocení předvedení části testů.

6. POŽADOVANÉ SOUČINNOSTI

- Pro zařízení v majetku Objednatele (viz popis Služby EET S3-001) a SW komponenty ADIS zajistí Objednatel na vyžádání Dodavatele podklady potřebné pro implementaci provozního dohledu (MIB, struktura logů apod).
- Objednatel zajistí účast příslušných hodnotitelů a schvalovatelů na akceptačním řízení služby.

POPIS SLUŽBY EET S1-005

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S1-005**
Název	**Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET**
Oblast Služeb	Bezpečnost
Typ Služeb	Příprava provozu

2. POPIS SLUŽBY

2.1 Účel a architektura bezpečnostního dohledu

Účelem poskytnutí Služby EET S1-005 je příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET pro poskytování Služby EET S3-002 („Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET", viz příloha č. 5 Smlouvy). Součástí Služby EET S1-005 je rozšíření, konfigurace a testování platformy bezpečnostního dohledu SPCSS dle popisu v této příloze.

Primárním účelem bezpečnostního dohledu (monitoringu) je jeho role jako hlavního podpůrného nástroje pro provozní služby CKB - detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů. Bezpečnostní dohled je dále podstatnou podmínkou pro naplnění požadavků vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

Architektura bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET je detailně popsána v návrhovém dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy) a využívá platformu IBM QRadar.

Primárním zdrojem dat pro bezpečnostní dohled jsou systémové a aplikační logy všech technických zařízení využitých při implementaci Transakční části a Krátkodobého úložiště EET v souladu s dokumentem „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy). Řešení bezpečnostního dohledu pokrývá následující vrstvy systému:

- Aktivní síťové a bezpečnostní prvky;
- XML akcelerátory;
- Servery;
- Databáze;

POPIS SLUŽBY EET S1-005

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S1-005**
Název	**Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET**
Oblast Služeb	Bezpečnost
Typ Služeb	Příprava provozu

2. POPIS SLUŽBY

2.1 Účel a architektura bezpečnostního dohledu

Účelem poskytnutí Služby EET S1-005 je příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET pro poskytování Služby EET S3-002 („Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET", viz příloha č. 5 Smlouvy). Součástí Služby EET S1-005 je rozšíření, konfigurace a testování platformy bezpečnostního dohledu SPCSS dle popisu v této příloze.

Primárním účelem bezpečnostního dohledu (monitoringu) je jeho role jako hlavního podpůrného nástroje pro provozní služby CKB - detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů. Bezpečnostní dohled je dále podstatnou podmínkou pro naplnění požadavků vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

Architektura bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET je detailně popsána v návrhovém dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy) a využívá platformu IBM QRadar.

Primárním zdrojem dat pro bezpečnostní dohled jsou systémové a aplikační logy všech technických zařízení využitých při implementaci Transakční části a Krátkodobého úložiště EET v souladu s dokumentem „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy). Řešení bezpečnostního dohledu pokrývá následující vrstvy systému:

- Aktivní síťové a bezpečnostní prvky;
- XML akcelerátory;
- Servery;
- Databáze;

- Aplikační servery a aplikace;
- Disková úložiště a zálohovací systém.

2.2 Rozsah bezpečnostního dohledu

Rozsah implementace bezpečnostního dohledu je detailně popsán v návrhovém dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET".

Celkový rozsah implementovaného bezpečnostního dohledu odpovídá následujícím počtům licencí QRadar:

- 70 LS (log source – zdrojů dat);
- 5000 EPS (events per second – zpracovaných řádků logu za sekundu);
- 25000 FPM (flow per minute – síťová spojení).

Řešení bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET bude poskytovat následující výstupy:

- Rozhraní pro předávání detekovaných KBU a KBI do ServiceDesku SPCSS;
- GUI rozhraní pro práci analytiků KB, včetně sady uložených dotazů, pohledů a reportů;
- Reporty a souhrnné statistiky transakcí příjmu tržeb.

Konfigurace bezpečnostního dohledu vychází z Analýzy rizik a Technického projektu provedených jako součást „Návrhu bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET".

Rozsah implementace bezpečnostního dohledu pro jednotlivá provozní prostředí (produkční, zkušební, testovací, vývojové a Playground) vyplývá z posouzení primárních aktiv v Analýze rizik.

2.3 Testování

Rozsah funkčních testů bezpečnostního dohledu je detailně popsán v návrhovém dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET".

Testy budou provedeny ve Fázi 1 (viz kapitolu Harmonogram níže). Testy jsou prováděny s vědomím Objednatele a účastí jeho pracovníků dle potřeby nebo na vyžádání Objednatele. Výstupem z testů bude dokument „Souhrnná zpráva o provedení testů bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET", který je zároveň formálním výstupem služby S1-005.

2.4 Pilotní provoz

Pilotní provoz EET bude probíhat v listopadu 2016. Pilotní provoz slouží poplatníkům k otestování jejich pokladních zařízení a vlivu EET na jejich prodejní a účetní procesy. Pilotní provoz probíhá v plném rozsahu funkcionality EET, na produkčním prostředí a s využitím produkčních certifikátů poplatníků.

Z pohledu bezpečnostního dohledu zahrnuje pilotní provoz poskytování služeb dle popisu Služby EET S3-002 v rozsahu odpovídajícím fázi implementace bezpečnostního dohledu. Zejména bude prováděn bezpečnostní dohled na úrovni sledování transakcí služby Příjem tržeb z logů XML akcelerátorů.

Procesy řízení provozu budou v tomto období podléhat řízení Projektu etržby.

2.5 Dokumentace

K termínu milníku Ukončení přípravy bezpečnostního dohledu bude Objednateli předán dokument „**Technická dokumentace bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET**“. Dokument je aktualizací návrhového dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET“ a jeho rozšíření o konfigurační dokumentaci.

3. HARMONOGRAM REALIZACE

Implementace a ladění bezpečnostního dohledu bude probíhat v následujících fázích:

- Fáze 1 – Zavedení bezpečnostního dohledu ve dvou krocích;
  - sběr logů ze všech systémů;
  - nastavení pravidel;
- Fáze 2 - Ladění pravidel;
- Fáze 3 - Průběžné sledování a úpravy konfigurace a pravidel – PDCA cyklus, součást Služby EET S3-002“.

Milník	Termín
Zavedení bezpečnostního dohledu Transakční části a Krátkodobého úložiště (konec Fáze 1)	30.11.2016
Ukončení přípravy bezpečnostního dohledu Transakční části a Krátkodobého úložiště (Ladění pravidel – konec Fáze 2)	28. 2. 2017

4. DEFINICE VÝSTUPŮ

Formálním výstupem služby S1-005 je dokument „**Souhrnná zpráva o provedení testů bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET**“, který bude předán k připomínkám Objednatele první pracovní den po termínu Zavedení bezpečnostního dohledu.

5. ZPŮSOB AKCEPTACE

Akceptační řízení Služby EET S1-005 bude zahájeno k termínu předání dokumentu „Souhrnná zpráva o provedení testů bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET“ a provedeno formou hodnocení a akceptace výstupu typu „dokument“ (dále jen „hodnocení dokumentu“ a „akceptace dokumentu“), popsanou v této kapitole.

Obecná akceptační kritéria pro typ výstupu „dokument“ jsou jednoznačnost, věcná správnost, srozumitelnost a gramatická správnost. Hodnocení a akceptace dokumentu probíhá metodou připomínkového řízení s následujícím postupem:

- Dodavatel předá dokument k hodnocení vedoucímu projektu Objednatele nebo přímo příslušnému hodnotiteli dle Registru kvality Projektu e-tržby Objednatele;
- Příslušný hodnotitel zpracuje do 3 pracovních dnů od předání připomínky k dokumentu a zaznamená je v Protokolu z hodnocení výstupu, který předá Vedoucímu projektu Objednatele a Dodavateli;
- Po zpracování případných připomínek předá Dodavatel dokument společně s Protokolem z hodnocení výstupu a návrhem Akceptačního protokolu vedoucímu projektu Objednatele nebo přímo příslušnému schvalovateli dle Registru kvality Projektu e-tržby Objednatele;
- Schvalovatel zpracuje a podepíše Akceptační protokol.

Objednatel si může vyžádat jako součást hodnocení předvedení části testů.

6. POŽADOVANÉ SOUČINNOSTI

- Pro zařízení v majetku Objednatele (viz popis Služby EET S1-003) a SW komponenty ADIS včetně aplikačních a databázových serverů zajistí Objednatel na vyžádání Dodavatele podklady potřebné pro implementaci bezpečnostního dohledu (struktura logů apod)
- Objednatel zajistí účast příslušných hodnotitelů a schvalovatelů na akceptačním řízení služby.

POPIS SLUŽBY EET S3-001

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S3-001**
Název	**Provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET**
Oblast Služeb	Infrastruktura, Služby podpory provozu
Typ Služeb	Provoz a podpora provozu

2. OBDOBÍ A REŽIM POSKYTOVÁNÍ SLUŽBY EET

Začátek poskytování služby	1.12.2016
Ukončení poskytování služby	30.11.2021
Režim služby/Provozní doba (s výjimkou podpory Playground, vývojářů a poplatníků)	7x24
Režim služby/Provozní doba (podpora Playground, vývojářů a poplatníků)	5x9 (8:00-17:00 pracovní dny)

3. POPIS SLUŽBY

3.1 Zkratky a terminologie

V kontextu tohoto dokumentu jsou používány následující zkratky a termíny

TČ	Transakční část EET (není součástí ADIS)
KÚ	Krátkodobé úložiště (je součástí ADIS)
EET_SPCSS	části EET a ADIS provozované Dodavatelem – TČ a KÚ
ADIS	Automatizovaný daňový informační systém Objednatele
DÚ	Dlouhodobé úložiště ADIS (provozní databáze tržeb)
ePodpora	Technická podpora uživatelů Daňového portálu poskytovaná ze strany Objednatele

3.2 Architektura a prostředí

Účelem poskytování Služby EET S3-001 je provoz infrastruktury a podpora provozu Transakční části a Krátkodobého úložiště EET (EET_SPCSS).

Architektura EET_SPCSS je detailně popsána v návrhovém dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy) a sestává z následujících komponent:

- Umístění v Národním datovém centru SPCSS;
- Bezpečné propojení a připojení k Internetu;
- SSL akcelerátory a load balancery;
- XML akcelerátory;
- RISC servery;
- Aplikační komponenty ADIS EETAP a EETDB, včetně aplikačních serverů Tomcat a DB Informix;
- Platforma diskových úložišť a zálohování.

V rámci Služby EET S3-001 je provozováno pět provozních prostředí:

- Produkční prostředí - dvě nezávislá střediska umístěná ve dvou nezávislých místnostech v rámci NDC SPCSS;
- Testovací prostředí – jedno středisko;
- Zkušební prostředí – jedno středisko;
- Vývojové prostředí – zjednodušená verze Transakční části pro účely vývoje úprav konfigurací XML akcelerátoru;
- Playground – zjednodušená verze Transakční části pro účely veřejného testování vývojářů pokladních zařízení.

Provozní parametry EET_SPCSS vycházejí z návrhu technického řešení EET_SPCSS, popsaného v dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET". Návrh technického řešení EET_SPCSS je založen na high-level návrhu a standardech technického řešení ADIS poskytnutých Objednatelem a zčásti též na konkrétních technických zařízeních poskytnutých Objednatelem (XML akcelerátory, SVC, Flash pole).

3.3 Rozsah infrastruktury a služeb NDC

Rozsah infrastruktury, která je poskytována formou provozní služby, nebo jsou pro ní poskytovány služby provozní podpory, je detailně popsán v návrhovém dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště EET".

Infrastruktura v majetku Dodavatele, která je v rámci Služby EET S3-001 poskytována jako služba, včetně služeb podpory provozu:

- Umístění ve dvou nezávislých místnostech v rámci NDC, energie, chlazení, včetně provozních a bezpečnostních služeb NDC v rozsahu potřebném pro níže uvedená zařízení a služby;
- Redundantní vysokokapacitní bezpečné připojení k Internetu a NIX o kapacitě minimálně 1Gb/s a maximálně 10Gb/s;
- Propojení do sítí Objednatele prostřednictvím GOVBONE;
- Bezpečné propojení – 1 zákaznický modul v rozsahu potřebném pro níže uvedená zařízení a služby;
- Stavový firewall – 4 instance;
- SSL akcelerátor a load balancer – 4 instance;

- SAN v rozsahu potřebném pro níže uvedená zařízení a služby – celkově 100 SAN portů;
- RISC servery v celkovém rozsahu 112 core a 1088 GB RAM, rozdělené do 28 virtuálních serverů;
- Disková úložiště v celkovém rozsahu 80 TB hrubé diskové kapacity, což zahrnuje:
  - Disková úložiště pro systémové disky všech virtuálních serverů;
  - Disková úložiště pro produkční prostředí v rozsahu odpovídajícím 6,1TB čistého databázového prostoru a 1TB NFS úložiště pro každé středisko, včetně prostoru pro minimálně 2 snapshoty databáze;
  - Disková úložiště pro databáze testovacího a zkušebního prostředí;
  - Diskový prostor potřebný pro redundance uložení (RAID);
- Zálohovací systém a páskové úložiště v rozsahu odpovídajícím zálohování výše uvedeného systému podle RTO a RPO požadavků popsaných kapitole 5.1 – celkový rozsah záloh 40TB;
- SW verze XML akcelerátoru běžící na 4 core virtuálního serveru vmWare – po jedné instanci pro Playground a vývojové prostředí.

Infrastruktura a SW v majetku Objednatele, která je předána Dodavateli do správy a pro kterou jsou v rámci Služby EET S3-001 poskytovány služby podpory provozu:

- XML akcelerátor – 6 ks;
- Diskové pole IBM FlashSystem 900 – 4 ks;
- 2-node diskový systém IBM SVC – 4 ks;
- Aplikační server Apache Tomcat pro aplikační servery všech prostředí;
- DB Informix pro DB servery všech prostředí;
- Aplikační moduly ADIS EETAP a EETDB pro všechna prostředí.

Služby NDC obsahují (v rozsahu potřebném pro výše uvedené systémy a služby):

- základní technologie (UPS, WAN, LAN, přídavné chlazení, KVM, trezory pro zálohy, datové rozvaděče – rack);
- vzduchotechnika a chlazení;
- energie pro provoz zařízení a chlazení;
- náhradní zdroje napájení;
- řídicí systémy pro technologie;
- stabilní hasicí zařízení;
- výkon dohledu non-IT technologií v režimu 7 × 24 hod.

Služby zajištění fyzické bezpečnosti ve standardu NDC SPCSS zahrnují:

- elektronický přístupový systém s kontrolou vstupu do jednotlivých bezpečnostních oblastí;
- uzavřený kamerový systém s ukládáním vybraných záznamů po dobu maximálně 2 (dvou) měsíců;
- elektronická zabezpečovací signalizace;
- výkon činnosti ozbrojené ostrahy v režimu turnusových nepřetržitých dvanáctihodinových směn (7 × 24 hod), na úrovni požadované ceninovou výrobou a osvědčením NBÚ pro zpracování utajovaných informací ve stupni „Tajné";
- součástí zajišťování objektové bezpečnosti a řízeného přístupu je i zajištění provozu a servisu SKZO, vytvoření a aktualizace bezpečnostní dokumentace a zajištění bezpečnosti ICT.

Služby Service Desku SPCSS jsou poskytovány v rozsahu potřebném pro podporu provozních služeb a procesů uvedených v tomto dokumentu.

3.4 Provozní podpora infrastruktury a aplikací

V rámci provozu služeb EET_SPCSS zajišťuje Dodavatel správu a podporu výše uvedené infrastruktury v následujícím rozsahu úrovní podpory:

- Správa a podpora služeb bezpečného propojení úrovně L1, L2 a L3;
- Správa a podpora operačních systémů a výpočetního výkonu úrovně L1, L2 a L3;
- Správa a podpora SAN a diskových úložišť úrovně L1, L2 a L3 pro komponenty v majetku Dodavatele;
- Správa a podpora SAN a diskových úložišť úrovně L1 a L2 pro komponenty v majetku Objednatele s využitím L3 podpory výrobce zajištěné Objednatelem;
- Správa a podpora XML akcelerátoru (včetně konfigurace aplikačních pravidel) úrovně L1 a L2, s využitím L3 produktové podpory výrobce zajištěné Objednatelem;
- Správa a podpora databáze Informix úrovně L1 a L2, s využitím L3 produktové podpory zajištěné Objednatelem;
- Správa a podpora Aplikace Krátkodobého úložiště včetně aplikačních a databázových serverů (ADIS moduly EETAP a EETDB) úrovně L1 a L2, s využitím L3 podpory dodavatele aplikačního vývoje ADIS zajištěné Objednatelem.

Při popisu provozních služeb jsou používány následující definice úrovní podpory:

- První úroveň podpory (Level 1, L1, někdy také nazýván "First line" nebo "Front end support") – zajišťuje přímou komunikaci se zákazníkem a uživateli (v definovaném rozsahu), převzetí informací, evidenci požadavků a incidentů v podpůrných nástrojích a prvotní analýzu požadavku nebo incidentu. Odpovídá na jednoduché požadavky na základě znalostní báze nebo na základě stavu aktuálně řešených incidentů. Pokud řešení požadavku převyšuje vědomosti podpory první úrovně, předává požadavek nebo incident vyšší úrovni podpory. V rámci provozních služeb Dodavatele je tato úroveň podpory interně realizována prostřednictvím ServiceDesk SPCSS a pracovištěm IT dohledu SPCSS;
- Druhá úroveň podpory (Level 2, L2) – řeší složitější požadavky a incidenty, jejichž řešení ovšem nevyžaduje hluboké znalosti aplikací, systémů nebo SW/HW a přístup ke zdrojovému kódu nebo náhradním dílům. V rámci provozních služeb Dodavatele je tato úroveň podpory typicky realizována správci aplikací a systémů Dodavatele;
- Třetí úroveň podpory (Level 3, L3, v případě HW/SW produktů rovněž nazývána HW/SW maintenance) - řeší nejsložitější požadavky a incidenty, jejichž řešení vyžaduje hluboké znalosti aplikací, systémů nebo SW/HW a přístup ke zdrojovému kódu nebo náhradním dílům. V rámci provozních služeb Dodavatele je tato úroveň podpory typicky realizována prostřednictvím kontraktů na výrobce/dodavatele jednotlivých platforem.

Činnosti správy a podpory zahrnují:

- řešení provozních incidentů detekovaných prostřednictvím dohledových systémů, hlášených uživateli nebo Objednatelem;
- pravidelné činnosti správy infrastruktury a aplikací, zejména:
  - kontroly logů, zaplněnosti databází, filesystémů a diskových prostorů;
  - sledování stavu zatížení systému;
  - kontrola zálohování a stavu záloh;
  - preventivní údržba;
  - aktualizace firmware a systémového SW;
- provádění drobných provozních změn konfigurace infastruktury a požadavků na součinnost (definice provozních změn a související procesy jsou uvedeny v Řídící dokumentaci);
- instalace a testování změn aplikací Krátkodobého úložiště v produkčním, zkušebním a testovacím prostředí;
- služby business continuity včetně testů obnovy a HA 1x ročně;

- součinnost při realizaci bezpečnostních testů nebo DR testů Objednatele;
- údržba dokumentace;
- řízení a evidence provozních procesů v nástroji ServiceDesk SPCSS.

Kontaktní informace provozní podpory jsou uvedeny v Řídící dokumentaci.

3.5 Podpora konfigurace aplikačních pravidel XML akcelerátoru

Součástí Služby EET S3-001 je i podpora konfigurace aplikačních pravidel XML akcelerátorů ve všech prostředích (včetně prostředí Playground) v souladu s dokumentem „Formát a struktura údajů o evidované tržbě a popis datového rozhraní pro příjem datových zpráv evidovaných tržeb", zveřejňovaného Objednatelem na web stránkách www.etrzby.cz (sekce IT/Vývojář) a souvisejícími pracovními podklady předanými Objednatelem. Konfigurace aplikačních pravidel XML akcelerátoru bude průběžně upravována podle nových verzí tohoto dokumentu formou provozních požadavků nebo změnového řízení (podle rozsahu změn a souvisejících činností).

Provozní podpora aplikační konfigurace XML akcelerátorů zahrnuje:

- Řešení provozních incidentů detekovaných prostřednictvím dohledových systémů, hlášených uživateli nebo Objednatelem;
- Úpravy konfigurace aplikačních pravidel XML akcelerátoru;
- Zálohování konfigurace XML akcelerátoru;
- Úpravy konfigurace bezpečného propojení (zejména FW pravidla) podle potřeb testování vývojářů na prostředí Playground.

3.6 Součinnost Objednatele v oblasti L3 podpory

V rámci řešení EET_SPCSS jsou použity následující komponenty v majetku Objednatele, které byly v rámci řešení EET_SPCSS předány Dodavateli do správy L1 a L2.

- ADIS komponenty EETAP a EETDB, programové vybavení KÚ;
- Aplikační server Tomcat;
- ADIS DB Informix, programové vybavení KÚ;
- XML akcelerátory - HW vybavení TČ;
- SVC a Flash pole - HW vybavení vrstvy SAN a storage.

Pro tyto komponenty zajišťuje L3 podporu Objednatel (formou kontraktů s dodavateli/výrobci těchto komponent) jako součinnost pro plnění provozní podpory Dodavatele. Závady řešené na straně Objednatele, resp. dodavatelů a výrobců těchto komponent, se nepočítají do SLA Dodavatele. Do SLA řešení závad a dostupnosti se nepočítá čas od nahlášení závady na L3 ze strany Dodavatele do jejího vyřešení na úrovni L3 a předání zpět.

ADIS, Tomcat a Informix

Opravy pozáručních chyb a realizace pozáručních zásahů v rámci Základního pozáručního servisu aplikace ADIS jsou podrobně popsány v Řídící dokumentaci.

Požadavky na L3 podporu jsou ze strany Dodavatele předávány prostřednictvím ADIS aplikace SŘA, v případě nedostupnosti aplikace SŘA e-mailem administrátorům ADIS na straně Objednatele.

XML akcelerátor, SVC a Flash pole

L3 produktová podpora HW komponent XML akcelerátor, SVC a Flash pole je zajišťována Objednatelem formou kontraktu na SW a HW mainetanance.

V případě delegování pracovníků Dodavatele pro přímé jednání s L3 produktovou podporou výrobce jsou ze strany Dodavatele požadavky na L3 podporu předávány prostřednictvím rozhraní definovaného výrobcem jménem Objednatele.

V opačném případě je L3 podpora poskytována prostřednictvím pověřených pracovníků Objednatele v Objednatelem určené provozní době. Požadavky na L3 podporu jsou ze strany Dodavatele předávány e-mailem nebo telefonicky.

Detailní podmínky a procesy poskytování součinnosti Objednatele v oblasti L3 podpory jsou upřesněny v Řídící dokumentaci.

3.7 Provozní dohled

Provozní dohled (monitoring) sleduje a vyhodnocuje události na úrovni infrastrukturních komponent, včetně vyhodnocování vlivu jednotlivých událostí na služby (SLA) a sledování výkonnostních parametrů služeb. Primárním účelem provozního dohledu v rámci podpory provozu je automatizované sledování funkčnosti a chybových stavů systému v reálném čase, urychlení detekce a tím i řešení incidentů a vad, včetně incidentů a vad ovlivňujících provozní SLA. Sekundárními účely provozního dohledu jsou automatizované sledování stavu a výkonu systému a proaktivní detekce hrozících chybových stavů.

Provozní dohled je implementován v rámci Služby EET S1-004 (Příprava provozního dohledu Transakční části a Krátkodobého úložiště EET, viz příloha č. 2 této Smlouvy) na základě návrhového dokumentu Návrh provozního dohledu Transakční části a Krátkodobého úložiště EET. Architektura provozního dohledu využívá následující komponenty platformy provozního dohledu SPCSS:

- CA Spectrum pro dohled síťové infrastruktury;
- CA Unified Infrastructure Monitoring (UIM) pro dohled IT komponent;
- CA Application Performance Management (APM) pro dohled aplikací z pohledu koncového uživatele (E2E, end2end);
- CA Service Operations Insight (SOI) pro dohled komplexních IT služeb.

Provozní dohled bude implementován pro kompletní rozsah výše uvedené infrastruktury a aplikačních modulů ADIS a bude provozován v režimu 7x24 na sdílených dohledových platformách SPCSS. Provozní dohled umožňuje sledovat provozní stavy:

- síťové infrastruktury;
- SAN infrastruktury;
- HW;
- operačních systémů;
- databází;
- aplikací;
- komplexních IT služeb;
- E2E pohledu na služby.

Provozní dohled bude provozován v kompletním rozsahu primárně pro provozní prostředí a Playground. Provozní dohled pro testovací a zkušební prostředí může být zjednodušený, ale umožní sledovat stav jednotlivých komponent a stav plnění SLA relevantních pro tato prostředí.

Informace z provozního dohledu budou v provozu zpřístupňovány Objednateli dle oboustranné dohody, minimálně však jednou měsíčně v rámci Zprávy o o úrovni a rozsahu poskytované Služby EET. Součástí provozního dohledu bude i poskytování informace o dostupnosti/funkčnosti Transakční části pro automatizované zveřejnění na webu www.etrzby.cz.

Součástí Služby EET S3-001 je i průběžné ladění pravidel provozního dohledu (PDCA cyklus).

Vzhledem k probíhajícímu projektu konsolidace a rozšíření platformy provozního dohledu SPCSS bude v momentě zahájení poskytování Služby EET S3-001 až do dokončení implementace Služby EET S1-004 k dispozici dočasné řešení provozního dohledu založené primárně na platformě CA Spectrum a CA APM. Dočasné řešení poskytne rozsah provozního dohledu omezený na kritické funkce:

- Sledování dostupnosti jednotlivých komponent infrastruktury;
- End2End sledování dostupnosti a odezvy služby Příjem tržeb;
- Sledování a vyhodnocování aplikačních transakcí služby Příjem tržeb;

3.8 Podpora vývojářů a poplatníků

Podpora koncových uživatelů EET_SPCSS (vývojářů třetích stran, poplatníků i pracovníků Finanční správy) je primárně prováděna Objednatelem. Dodavatel se v rámci této podpory účastní odpovídání na individuální dotazy a připomínky technického charakteru k funkcionalitě a provozu Playgroundu a Transakční části. Dodavatel odpovídá na dotazy agregované na úrovni ePodpory Objednatele, které ePodpora nemůže přímo odpovědět na základě známých odpovědí na časté otázky a předchozí dotazy. Podpora je poskytována písemnou formou v režimu 5x9 (pracovní dny 8:00-17:00) prostřednictvím Service Desku SPCSS a e-mailové integrace s ePodporou Objednatele.

Rozsah odpovědí na individuální dotazy a připomínky odpovídá následující definici Objednatele pro celkový rozsah podpory vývojářů a veřejnosti:

Finanční správa odpovídá na dotazy technického charakteru, které se přímo vztahují ke zveřejněným specifikacím a funkcionalitě Playgroundu a Transakční části EET. Součástí podpory není poradenství k software pokladních systémů, podpůrným knihovnám a vývojovým nástrojům, ani výklad nebo postup při aplikaci obecně platných technických standardů.

Součástí podpory vývojářů a poplatníků je příprava a aktualizace dokumentů **„Přístupové a provozní informace"** pro jednotlivá veřejně provozovaná prostředí. Jde o dokumenty určené pro zveřejnění Objednatelem spolu s dokumentem „Formát a struktura údajů o evidované tržbě a popis datového rozhraní pro příjem datových zpráv evidovaných tržeb" a obsahuje zejména informace o přístupových URL, verzích rozhraní a použitých certifikátech.

Podpora vývojářů dále zahrnuje:

- koordinaci přípravy materiálů pro zveřejnění nových verzí popisu datového rozhraní a přístupových a provozních informací Playgroundu, včetně testovacích certifikátů a vzorových XML zpráv;
- přípravu odpovědí na časté otázky technického charakteru k funkcionalitě a provozu Playgroundu a Transakční části EET a oznámení o provozu Playgroundu a Transakční části EET pro zveřejnění na www.etrzby.cz (sekce IT/Vývojář).

3.9 Dokumentace

Součástí podpory provozu je i údržba dokumentů **„Technická dokumentace infrastruktury Transakční části a Krátkodobého úložiště EET"**, **„Technická dokumentace infrastruktury Playgroundu"** a **„Technická dokumentace provozního dohledu Transakční části a Krátkodobého úložiště EET"**, vytvořených v rámci Služeb EET S1-003, S1-001 a S1-004.

4. SPECIFICKÉ PROVOZNÍ PROCESY

Metodika řízení provozu a další provozní procesy relevantní pro poskytování Služby jsou popsány v Řídící dokumentaci realizace smlouvy pro období provozu služeb v souladu s Přílohou

č. 2 Rámcové smlouvy. Řídící dokumentace a její změny v průběhu provozu jsou oboustranně schvalovány oprávněnými osobami Objednatele a Dodavatele dle Rámcové smlouvy.

Metodika řízení provozních služeb vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000 a zahrnuje:

- Definici řídících struktur;
- Řízení incidentů a požadavků;
- Řízení kvality;
- Řízení rizik;
- Řízení problémů;
- Řízení změn;
- Řízení komunikace;
- Řízení součinností;
- Výkazy o službách.

Procesy řízení provozu služeb jsou řešeny na úrovni Týmu přípravy a provozování služeb (TPP). Procesy provozní podpory jsou řízeny a jejich provádění je evidováno v nástroji Service Desk SPCSS.

5. PROVOZNÍ PARAMETRY A SLA

Měsíční Zpráva o úrovni a rozsahu poskytované Služby EET bude obsahovat informace o reálném plnění parametrů uvedených v této kapitole a bude hodnocena podle jejich souladu s hodnotami uvedenými ve Smlouvě.

5.1 Výkonnostní parametry EET_SPCSS

Uvedené metriky jsou maximální hodnoty za celé období provozu EET_SPCSS. Metriky a požadavky platí pro produkční prostředí a vycházejí z návrhu technického řešení EET_SPCSS.

Uvedené požadavky byly zpracovány do návrhu řešení a ověřeny v zátěžových testech. Tyto parametry budou v průběhu provozu průběžně sledovány nástroji provozního dohledu a v případě větších změn ověřovány opakovanými zátěžovými testy. V případě porušení nebo hrozícího porušení těchto parametrů bude neprodleně vyvoláno jednání Provozovatele s Objednatelem o způsobu řešení.

Popis	Počet	Jednotka	Poznámka
Příjem tržeb (Datové rozhraní pro příjem datových zpráv evidovaných tržeb)			
Maximální počet tržeb za rok	10 500 000 000,00	Ks	
Maximální počet tržeb za den	30 000 000,00	Ks	
Průměrná velikost datové zprávy (s el. podpisem)	8,50	kB	
Průměrná propustnost tržeb	347,00	Ks/sec	
Špičková propustnost tržeb	4 000,00	Ks/sec	
Maximální odezva při špičkové zátěži	2,00	sec	Od přijetí datové zprávy po odeslání potvrzovací zprávy s FIK, resp. chybové zprávy
Dotazy z ADIS do KÚ			
Maximální propustnost dotazů	40	Ks/sec	
Obnova dat KÚ ze zálohy po havárii databáze			Za předpokladu funkčního HW v daném středisku

Recovery Time Objective (RTO)	12	hod	
Recovery Point Objective (RPO)	5	min	Maximální přípustná doba ztráty dat.
Minimální retenční kapacita KÚ	5	dní	Počet dní (při maximálním provozu 30 mil. účtenek za den), po který je schopno krátkodobé úložiště uchovat data, neodebíraná ze strany DÚ.

5.2 SLA parametry

5.2.1 Kategorizace závad

Kritická	závada, při níž není služba použitelná ve svých základních funkcích
Hlavní	závada, kdy je poskytovaná služba ve svých funkcích degradovaná natolik, že tento stav omezuje běžné poskytování služby
Vedlejší	závada, která svým charakterem nespadá do kategorie kritické nebo hlavní a neomezuje běžné poskytování služby

Pro snazší posouzení jednotlivých typů závad a jejich kategorizaci vznikne v rámci Řídící dokumentace oboustranně schvalovaný dokument „Kategorizace závad". Dokument bude zaznamenávat dohody o kategorizaci a způsobu vypořádání konkrétních typů závad, pro budoucí využití při výskytu stejného typu závady.

5.2.2 Dostupnost jednotlivých částí služeb EET_SPCSS

Dostupnost části služeb EET_SPCSS znamená procentuální vyjádření poměru doby, po kterou byla poskytovaná část služeb EET_SPCSS v rámci příslušné provozní doby dostupná, tzn. nevyskytla se žádná kritická závada, a celkové příslušné provozní doby části služeb EET_SPCSS.

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100.\frac{x + n - y}{x}$$

kde

D je dostupnost [%] v daném období (roce provozu),
x vyjadřuje fond provozní doby služby v daném období,
y vyjadřuje počet hodin v daném období, kdy byla část služeb EET_SPCSS nedostupná,
n vyjadřuje počet hodin v daném období, kdy byla služba nedostupná z důvodu závady mimo odpovědnost Dodavatele.

Služba se nepovažuje za nedostupnou v případě, kdy nelze službu využívat z důvodu závady, která není ve správě Dodavatele, nebo po dobu, kdy Dodavatel nemůže odstranit řádně nahlášenou závadu systému z důvodu vylučujících odpovědnost dle § 2913 odst. 2 občanského zákoníku nebo z důvodu prodlení v plnění či neposkytnutí dostatečné součinnosti ze strany objednatele. Služba se zejména nepovažuje za nedostupnou v případě kritických závad, jejichž řešení je součástí součinnosti objednatele – řešení aplikačních závad ADIS (včetně DB Informix),

řešení závad HW komponent dodaných objednatelem (XML akcelerátor, SVC, Flash pole) na úrovni podpory výrobce těchto HW produktů.

Dále se do této doby nepočítá doba, po kterou nemohl Dodavatel závadu odstranit z důvodů na straně Objednatele.

Schválené odstávky nejsou součástí provozní doby.

Požadavky na dostupnost vycházejí z návrhu technického řešení EET_SPCSS. Řešení se skládá ze dvou oddělených datových center/středisek s omezenou vnitřní redundancí, zejména na úrovni KÚ. Testovací a zkušební prostředí jsou umístěny vždy jen v jednom datovém centru/středisku.

Požadavky na roční dostupnost služby pro jednotlivé části služeb EET_SPCSS, pouze pro produkční prostředí:

Část služeb	Roční dostupnost		
	v %	výpadek v hodinách (orientační)	Provozní doba
Příjem tržeb	99,982	1 hod 34 min	7x24
Dotazy z ADIS do KÚ – DC1*	99	87 hod 36 min	7x24
Dotazy z ADIS do KÚ – DC2*	99	87 hod 36 min	7x24
Přenos dat z KÚ do DÚ – DC1*	99	87 hod 36 min	7x24
Přenos dat z KÚ do DÚ – DC2*	99	87 hod 36 min	7x24
Playground	99	22 hod 41 min	5x9 pracovní dny 8:00-17:00

* V případě, že databáze KÚ v daném datovém centru neobsahuje žádná provozní data, nespadají závady služby v daném DC do SLA Roční dostupnost, a tudíž nejsou započítány do nedostupnosti části služeb. Řízené odstávky jednoho datového centra se po přenosu všech dat do DÚ nepočítají do SLA Roční dostupnost.

Do SLA Roční dostupnost se nezapočítává doba, po kterou je incident předán k řešení L3 úrovni podpory, zajišťované Objednatelem, a to v čase od nahlášení závady na L3 ze strany Dodavatele do jejího vyřešení na úrovni L3 a předání zpět.

Schválené odstávky nejsou součástí provozní doby a nepočítají se do SLA.

Plnění těchto parametrů bude vykazováno 1x měsíčně ve Zprávě o úrovni a rozsahu poskytované Služby EET. Celkové vyhodnocení a uplatnění pokut probíhá na konci každého celého roku provozu, počítáno od termínu začátku poskytování služby.

5.2.3 Požadované lhůty pro obnovení služby s výjimkou závad konfigurace aplikačních pravidel XML akcelerátoru

Požadavky na řešení závad v provozní době vycházejí z návrhu technického řešení EET_SPCSS. Řešení se skládá ze dvou oddělených datových center/středisek s omezenou vnitřní redundancí, zejména na úrovni KÚ. Testovací a zkušební prostředí jsou umístěny vždy jen v jednom datovém centru/středisku.

Část služeb	Lhůta pro obnovení služby v hodinách provozní doby		
	Kritická závada	Hlavní závada	Vedlejší závada
Produkční prostředí			
Příjem tržeb	4	8	72
Dotazy z ADIS do KÚ – DC1*	48	120	240
Dotazy z ADIS do KÚ – DC2*	48	120	240
Přenos dat z KÚ do DÚ – DC1*	48	120	240
Přenos dat z KÚ do DÚ – DC2*	48	120	240
Testovací a zkušební prostředí			
Příjem tržeb	72	120	240
Dotazy z ADIS do KÚ	72	120	240
Přenos dat z KÚ do DÚ	72	120	240
Playground	24	40	80

* Pro produkční prostředí: V případě, že databáze KÚ v daném datovém centru neobsahuje žádná provozní data, nespadají závady služby v daném DC do SLA Lhůta pro obnovení služby. Řízené odstávky jednoho datového centra se po přenosu všech dat do DÚ nepočítají do SLA Lhůta pro obnovení služby.

Do lhůty pro obnovení služby se nezapočítává doba, po kterou je incident předán k řešení L3 úrovni podpory, zajišťované Objednatelem, a to v čase od nahlášení závady na L3 ze strany Dodavatele do jejího vyřešení na úrovni L3 a předání zpět.

Schválené odstávky nejsou součástí provozní doby a nepočítají se do SLA Lhůta pro obnovení služby.

V případě časového překryvu více incidentů nebo v případě incidentu, který má vliv na dostupnost více částí služeb, se incident započítává pouze do dostupnosti jedné z těchto části služeb, a to té, která má nejvyšší SLA, resp. nejvyšší smluvní pokutu.

5.2.4 Požadované lhůty pro řešení závad konfigurace aplikačních pravidel XML akcelerátoru

Část služeb	Lhůta pro zahájení řešení v hodinách provozní doby		
	Kritická závada	Hlavní závada	Vedlejší závada
Produkční prostředí			
Příjem tržeb	4	8	72

Lhůta pro zahájení řešení zahrnuje analýzu a vyřešení problému na úrovni infrastruktury a L2 podpory aplikačních pravidel XML akcelerátoru. Do lhůty pro zahájení řešení se nezapočítává doba, po kterou je incident předán k řešení L3 úrovni podpory, zajišťované Objednatelem, a to v čase od nahlášení závady na L3 ze strany Dodavatele do jejího vyřešení na úrovni L3 a předání zpět.

Řešení závad aplikačních pravidel formou úpravy aplikačních pravidel zahrnuje i testování na testovacím prostředí. Řešení kritických závad probíhá bez prodlení, termíny řešení ostatních kategorií závad dle dohody s Objednatelem.

5.2.5 Smluvní pokuty

Smluvní pokuty při nedodržení parametru dostupnosti Služby dle odstavce 5.2.2:

Část služeb	Smluvní pokuty při nedodržení parametru dostupnosti Služby v Kč za každou minutu nad stanovený parametr
Produkční prostředí	
Příjem tržeb	250,-
Dotazy z ADIS do KÚ – DC1	100,-
Dotazy z ADIS do KÚ – DC2	100,-
Přenos dat z KÚ do DÚ – DC1	50,-
Přenos dat z KÚ do DÚ – DC2	50,-

Uvedené pokuty náleží Objednateli za nedodržení parametru dostupnosti Služby v daném roce provozu.

Smluvní pokuty při nedodržení parametru obnovení Služby dle odstavce 5.2.3:

Část služeb	Smluvní pokuty při nedodržení parametru obnovení Služby v Kč za nesplnění v daném dni		
	Kritická závada	Hlavní závada	Vedlejší závada
Produkční prostředí			
Příjem tržeb	30 000,-	15 000,-	5 000,-
Dotazy z ADIS do KÚ – DC1	10 000,-	5 000,-	2 500,-
Dotazy z ADIS do KÚ – DC2	10 000,-	5 000,-	2 500,-
Přenos dat z KÚ do DÚ – DC1	5 000,-	2 500,-	1 000,-
Přenos dat z KÚ do DÚ – DC2	5 000,-	2 500,-	1 000,-

Uvedené pokuty náleží Objednateli za nedodržení parametru obnovení Služby v daném kalendářním dni. V případě nedodržení parametru obnovení služby více částí služeb v jeden kalendářní den se v daný kalendářní den započítává pokuty pouze jednou, a to pro část služeb, která má nejvyšší SLA pokuty.

Smluvní pokuty za nesplnění SLA parametrů poskytování Služby se nevztahují na plnění, realizované Dodavatelem po dobu 3 (tří) měsíců od začátku poskytování Služby. Smluvní pokuty nelze uplatnit na období schválené odstávky části systému (omezení redundance) a čas provádění bezodstávkových instalací vyžádaných nebo schválených objednatelem.

6. POŽADOVANÉ SOUČINNOSTI OBJEDNATELE

- Pro komponenty infrastruktury v majetku Objednatele, aplikační a databázové servery a ADIS komponenty EETAP a EETDB zajistí Objednatel přístup k L3 produktové podpoře způsobem popsaným v kapitole 3.6.
- Objednatel je odpovědný za aktualizace dokumentu „Formát a struktura údajů o evidované tržbě a popis datového rozhraní pro příjem datových zpráv evidovaných tržeb" a souvisejících interních podkladů Objednatele popisujících požadovanou funkcionalitu aplikační konfigurace XML akcelerátoru. Objednatel zpřístupní připravované aktualizace dokumentu Dodavateli s dostatečným předstihem pro přípravu a realizaci změn.
- Objednatel poskytne nezbytnou součinnost při realizaci bezpečnostních testů nebo DR testů Dodavatele

POPIS SLUŽBY EET S3-002

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S3-002**
Název	**Provozní bezpečnostní služby pro Transakční část a Krátkodobé úložiště EET**
Oblast Služeb	Bezpečnost
Typ Služeb	Provoz a podpora provozu

2. OBDOBÍ A REŽIM POSKYTOVÁNÍ SLUŽBY EET

Začátek poskytování služby	1. 12. 2016
Ukončení poskytování služby	30. 11. 2021
Režim služby/Provozní doba	7x24

3. POPIS SLUŽBY

3.1 Účel, architektura a prostředí

Účelem Služby EET S3-002 je poskytování provozních bezpečnostních služeb relevantních pro provoz Transakční části a Krátkodobého úložiště EET v souladu s požadavky zákona 181/2014 Sb., o kybernetické bezpečnosti (dále ZoKB) a vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, pro prvky kritické informační infrastruktury (dále VoKB), konkrétně § 10, 13, 17, 21 – 24 a 30 – 33 z této vyhlášky.

Objednatel prohlašuje, že je připraven v úzké součinnosti s Objednatelem a na základě jeho požadavků optimalizovat parametry poskytované Služby, podílet se na zlepšení celkové bezpečnosti informací v prostředí Objednatele (snížení nepříznivých dopadů na organizaci), zajišťování důkazních prostředků, poskytování vstupních dat pro úpravu politiky bezpečnosti informací a bezpečnostní dokumentace Objednatele.

Klíčovou bezpečnostní službou je detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů. Součástí Služby EET S3-002 je provoz bezpečnostního dohledu (monitoringu) jako hlavního podpůrného nástroje pro poskytování těchto služeb. Bezpečnostní dohled je dále podstatnou podmínkou pro naplnění požadavků § 22 a § 23 VoKB.

Architektura bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET je detailně popsána v návrhovém dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy) a využívá platformu IBM QRadar. Systém bezpečnostního dohledu byl implementován v rámci Služby EET S1-005 („Příprava bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET", viz příloha č 3 Smlouvy).

Primárním zdrojem dat pro bezpečnostní dohled jsou systémové a aplikační logy všech technických zařízení využitých při implementaci Transakční části a Krátkodobého úložiště EET v souladu s dokumentem „Detailní technické řešení Transakční části a Krátkodobého úložiště EET" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy). Řešení bezpečnostního dohledu pokrývá následující vrstvy systému:

- Aktivní síťové a bezpečnostní prvky;
- XML akcelerátory;
- Servery;
- Databáze;
- Aplikační servery a aplikace;
- Disková úložiště a zálohovací systém.

Služby založené na bezpečnostním dohledu jsou dále doplněny službami skenování zranitelností (§24 VoKB), ochrany integrity komunikačních sítí (§17 VoKB), penetračních testů (§24 VoKB) a správy rizik (§4 VoKB).

Služba EET S3-002 je poskytována pro pět provozních prostředí:

- Produkční prostředí - dvě nezávislá střediska umístěná ve dvou nezávislých místnostech v rámci NDC SPCSS;
- Testovací prostředí – jedno středisko;
- Zkušební prostředí – jedno středisko;
- Vývojové prostředí – zjednodušená verze Transakční části pro účely vývoje úprav konfigurací XML akcelerátoru;
- Playground – zjednodušená verze Transakční části pro účely veřejného testování vývojářů pokladních zařízení.

3.2 Rozsah bezpečnostního dohledu

Rozsah implementace bezpečnostního dohledu je detailně popsán v návrhovém dokumentu „Návrh bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET".

Celkový rozsah implementovaného bezpečnostního dohledu odpovídá následujícím počtům licencí QRadar:

- 70 LS (log source – počet zdrojů dat);
- 5000 EPS (events per second – počet zpracovaných řádků logu za sekundu);
- 25000 FPM (flow per minute – počet síťových spojení);
- 15 licencí modulu Vulnerability management (skenování zranitelností – počet částí systémů, které lze skenovat najednou);
- 8 licencí modulu Risk Management (ochrana integrity komunikačních sítí - počet bezpečnostních politik, vůči kterým lze systém skenovat).

Řešení bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET poskytuje následující výstupy:

- Rozhraní pro předávání detekovaných KBU a KBI do ServiceDesku SPCSS;

- GUI rozhraní pro práci analytiků KB, včetně sady uložených dotazů, pohledů a reportů;
- Reporty a souhrnné statistiky transakcí příjmu tržeb.

Konfigurace bezpečnostního dohledu vychází z Analýzy rizik a Technického projektu provedených jako součást „Návrhu bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET".

Rozsah implementace bezpečnostního dohledu pro jednotlivá provozní prostředí (produkční, zkušební, testovací, vývojové a Playground) vyplývá z posouzení primárních aktiv v Analýze rizik.

Rozsah funkcionality poskytované bezpečnostním dohledem je závislý na rozsahu implementovaných bezpečnostních prvků a logování podle návrhu v dokumentu „Detailní technické řešení Transakční části a Krátkodobého úložiště" (výstup Služby EET S1-002 „Návrhové dokumenty Transakční části a Krátkodobého úložiště EET", viz příloha č. 2 Prováděcí smlouvy č. 2 Rámcové smlouvy) a realizovaných v technickém řešení Transakční části a Krátkodobého úložiště EET v rámci Služby EET S1-003 („Příprava infrastruktury Transakční části a Krátkodobého úložiště EET", viz příloha č. 1 Smlouvy). Bezpečnostní dohled může pracovat pouze s informacemi, které jsou k dispozici.

V případě drobných změn technického řešení budou změny bezpečnostního dohledu realizovány buď formou ladění pravidel bezpečnostního dohledu v rámci PDCA cyklu, v případě větších změn technického řešení realizovaných formou změnového řízení bude součástí změnového řízení i úprava bezpečnostního dohledu.

3.3 SW licence

Služby jsou zajištěny pomoc SW nástrojů s následujícími typy a počty licencí, které jsou stanoveny na základě provedení Analýzy rizik. Čerpání licencí je kalkulováno na základě aktuálního použití.

Název licence	Zkratka licence	Licence pro bezpečnostní služby EET_SPCSS
Log Source	LS	70
Events per second	EPS	5000
Flows per minute	FPM	25000
ServiceDesk SPCSS	SD	2
Vulnerability management	VM	15
Risk management	RM	8

- **Log Source (LS)** – Zdroj logů, který generuje logy, které jsou sbírané a vyhodnocované nástrojem SIEM;
- **Events per Second (EPS)** – Události vytvořené zdrojem logů za jednu sekundu;
- **Flows per Minute (FPM)** – Počet uskutečněných spojení, během jedné minuty;
- **Vulnerability management (VM)** – Skenování zranitelností, licence je čerpána na základě právě skenovaných systémů;
- **Risk manager (RM)** – Nástroj pro ochranu integrity sítí, licence jsou čerpány dle počtu bezpečnostních politik, oproti kterým jsou kontrolovány prvky sítě;

- **ServiceDesk SPCSS (SD)** – Prostředí, pro evidenci, řízení a vyhodnocování BH, KBU,KBI
  a SLA. Licence představuje počet současně přihlášených osob do ServiceDesku SPCSS.

3.4 Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů

Nabízená služba je souborem aktivit a procesů v oblastech monitoringu a detekce, jejich vyhodnocování a zvládání, dokumentování kybernetických bezpečnostních událostí, bezpečnostních hlášení a kybernetických bezpečnostních incidentů (KBI), jejich analýzy a návrhů na zlepšování IS KII Objednatele.

Monitoring a detekce kybernetických bezpečnostních událostí (KBU) v režimu 24x7 je zajištěna dohledovým pracovištěm, SIEM nástrojem s integrovaným Log Managementem, expertním týmem CKB-SOC, bezpečným úložištěm zdrojových dat. SIEM nástroj v reálném čase monitoruje a vyhodnocuje probíhající události na sledovaných aktivech, a na základě implementovaných pravidel automaticky sestavuje bezpečnostní výstrahu, která nese informace o narušení bezpečnostního stavu. Tato funkcionalita je zajištěna sběrem událostí v nástroji SIEM z vybraných zdrojů logů, které jsou definovány na základě analýzy rizik. Tím služba naplňuje požadavky § 21 - § 23 VoKB.

Vyhodnocování a klasifikace bezpečnostních incidentů a určování adekvátních reakcí bude prováděno, evidováno a vyhodnocováno v ServiceDesku SPCSS v souladu s § 30 - § 33 VoKB. Nástroj ServiceDesk SPCSS je jednotné prostředí pro řízení procesu, evidenci, sledování řešení a vyhodnocování bezpečnostních hlášení, kybernetických bezpečnostních událostí a incidentů oznámených uživateli, bezpečnostními rolemi, a administrátory nebo detekovaných technickými prostředky. ServiceDesk je prostředím, které slouží jako podklad pro expertní tým CKB - SOC při zvládání kybernetických bezpečnostních událostí a incidentů definovanými procesy „Problem management" a také pro „Change management". Tím služba naplňuje splnění požadavků § 13 VoKB.

Součástí detekce, sběru a vyhodnocování kybernetických bezpečnostních událostí a incidentů je monitoring databází a aplikací. Přináší Objednateli přehled v prostředí monitorovaných informačních systémů dle legislativních požadavků § 24 VoKB.

Logy získané z monitorovaného systému se uchovávají v úložišti systému SIEM po dobu minimálně 3 měsíců, dle § 21, odst. (3) VoKB. Archivace logů nad rámec povinných požadavků dle § 21, odst. 3 VoKB, může být sjednána formou dodatku ke Smlouvě.

3.5 Reputační databáze IP adres

Služba propojuje webovou aplikaci reputační databáze IP adres s nástrojem SIEM a naplňuje informacemi a daty k příslušným IP adresám, webovým stránkám či dalším zdrojům potencionálních kybernetických bezpečnostních událostí a incidentů.

Reputační databáze slouží např.: k blokování známých útočníků, IP adres lokalit, které šíří phishing, spam, remote control, malware a jiné podvodné aktivity. Do této databáze přispívají ostatní uživatelé tohoto nástroje SIEM z celého světa, včetně specializovaného globálního bezpečnostního týmu výrobce.

3.6 Testovací prostředí bezpečnostního dohledu

Slouží Objednateli pro testování nových pravidel, bezpečného nasazování nových patchů (opravy, záplaty) a upgradů (přechod na vyšší verzi). Tato část Služby splňuje § 10 VoKB. Testovací prostředí slouží především pro potřeby testování vydávaných aktualizací nástroje SIEM, testování úprav konfigurací a ověřování jejich vlivu na stávající stav, před jejich nasazením na produkční prostředí, aby v případě chyby nebyl produkční provoz nijak dotčen. Testovací prostředí je realizováno na virtuální platformě u Objednatele. Do tohoto prostředí nemá Objednatel přístup. Přístup má pouze nezbytný počet osob na straně Objednatele a jeho dodavatelů.

3.7 Skenování zranitelností

Služba proaktivně zajišťuje bezpečnost sítí a zranitelnosti aplikací a databází formou skenování systémů a vyhledávání jejich zranitelností. Tato část Služby naplňuje § 24 VoKB. Jedná se o možnost importu informací o zranitelnostech ze zdrojů 3. stran. Těmito informacemi se aktualizuje vlastní databáze SIEM nástroje. Výstupem je přehled o zranitelnostech na monitorovaných systémech, možnost určení závažnosti a hodnocení rizika v kontextu s aktuální síťovou a aplikační architekturou.

Jedná se nejen o možnost identifikace zranitelností, ale především o další práci s nimi, definování jejich priorit a tvorbu korelačních pravidel nad konkrétními zranitelnostmi či assety. Služba umožňuje aktivně vyvolat skenování zranitelností např. na základě přidání nového zařízení do infrastruktury. Služba napomáhá sloučit všechny získané informace do jedné platformy, kde je s nimi možné dále nadstandardně pracovat v kontextu všech bezpečnostních událostí.

3.8 Ochrana integrity komunikačních sítí

Služba napomáhá předcházení útoků pomocí identifikace chybně nastavených pravidel u aktivních prvků síťové infrastruktury, jako jsou firewally, routery, switche nebo IPS Služby. Vytváří a simuluje útoky na síťovou topologii a její prvky, čímž kontroluje správné nastavení vůči bezpečnostním politikám, a to za účelem snížení rizika a zvýšení efektivity činností. Tato část Služby poskytuje podporu pro splnění § 17 VoKB.

Služba umožňuje analyzovat síťovou topologii a porovnávat seznam všech zranitelností s aktuální topologií v síti. Výsledkem této analýzy je seznam všech zařízení, které mohou být zranitelné a jsou například dostupné z internetu, nebo mohou komunikovat s napadeným zařízením. Lze vytvářet vlastní politiky pro vyhledávání hrozeb a určovat jim ohodnocení, dle kterého lze zobrazovat ty nejzávažnější hrozby, které jsou například na kritických systémech, před těmi méně závažnými. Služba automaticky z konfiguračních souborů a routovacích tabulek z routerů vytváří topologii. Vzhledem k tomu, že je topologie vytvářena automaticky z konfiguračních souborů a nevytváří ji uživatel ručně, jsou v ní zahrnuty všechny aktuální trasy mezi jednotlivými sítěmi, které daná konfigurace síťových prvků umožňuje. Služba umožňuje z jednoho místa sledovat konfiguraci všech síťových prvků bez nutnosti procházet několik konfiguračních rozhraní, nebo nutnosti ovládat syntaxi všech zařízení. Toho je docíleno připojením k aktivním síťovým prvkům pomocí základních protokolů a uložením jejich aktuální konfigurace do paměti. Služba umožňuje zobrazovat nejvíce používaná a nejméně používaná pravidla firewallů, což může posloužit k ladění těchto pravidel a zlepšení prostupnosti daných zařízení.

Služba si uchovává všechny verze konfiguračních souborů všech aktivních prvků síťové infrastruktury od doby, kdy bylo zařízení poprvé ve Službě registrováno. Lze tedy pohodlně sledovat historii konfigurace jednotlivých zařízení a také tyto konfigurace porovnávat. Porovnávat lze nejen verze konfigurací u jednotlivých zařízení, ale je možné porovnávat také různé verze

konfiguračních souborů u několika síťových prvků najednou. Služba tedy umožňuje přehledně zobrazit konfigurační soubory od různých zařízení zároveň v různých verzích.

3.9 Penetrační testování

Služba Penetrační testy zajišťuje podklady pro stanovování zranitelností a priorit v rámci problematiky KB v IT infrastruktuře. Penetrační testy jsou pomocným, ale silným nástrojem pro ověřování úrovně kvality bezpečnostní architektury a zjištění slabin z pohledu průniků z vnějšího kyberprostoru. Slouží při hodnocení efektivnosti ochrany sítě a při určování, která aktiva představují bezpečnostní rizika a je třeba je aktualizovat nebo nahradit novými.

Cílem penetračních testů, je ověření úrovně zabezpečení, primárně se zaměřením na ta zranitelná místa a chyby, které pro Zákazníka představují největší riziko. Penetrační testování má několik fází, je rozděleno do kategorií dle způsobu testování, do kategorií dle úrovně znalostí o testovaném cíli.

Penetrační testy budou probíhat v pravidelných šestiměsíčních intervalech.

3.10 Správa rizik

Služba poskytuje Nástroj, který zabezpečuje potřeby klienta v oblasti naplňování legislativy při správě rizik. Umožňuje federativní uspořádání jednotlivých klientů v systému, včetně jednotné správy, reportingu událostí v celém životním cyklu rizika. Nástroj pro správu rizik je integrován do SIEM, jak je výše popsán, a stejně tak integrován do ServiceDesk SPCSS. Toto propojení poté zákazníkovi umožní přehledně sledovat, jak se jednotlivé incidenty propojí ze SIEM nástroje do nástroje pro Správu rizik, a jak jsou na ně poté přiřazeny opatření, a jak jsou opatření řešeny a nasazovány. Obsah databáze nástroje pro Správu rizik bude pravidelně aktualizován v šestiměsíčních intervalech.

3.11 Dokumentace

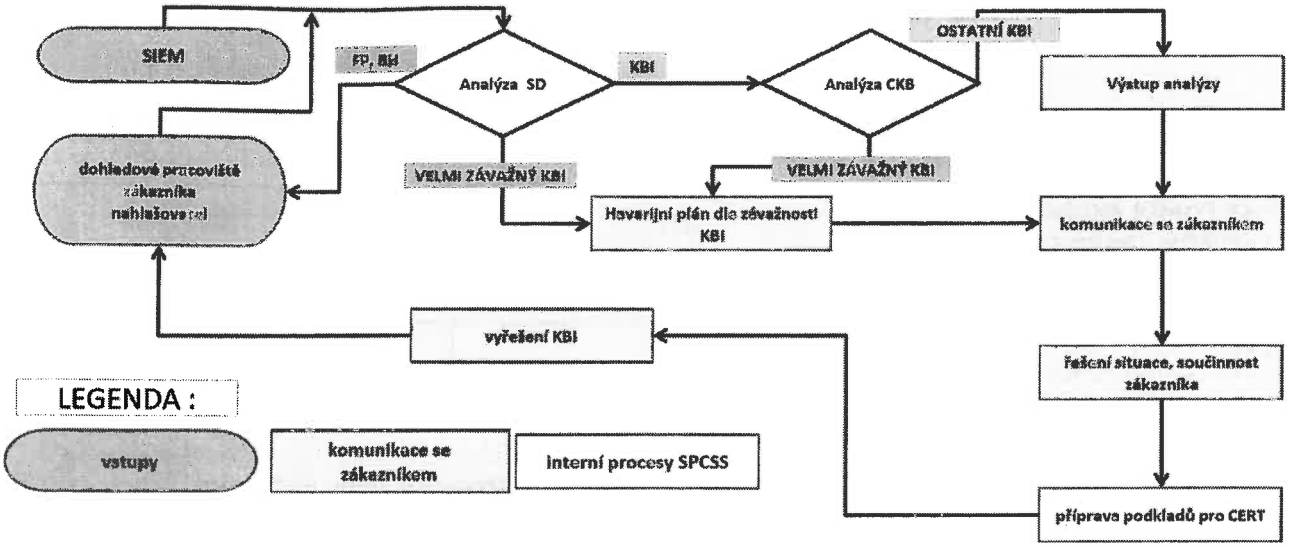
Součástí podpory provozu je i údržba dokumentu **„Technická dokumentace bezpečnostního dohledu Transakční části a Krátkodobého úložiště EET“**, vytvořeného v rámci Služby EET S1-005.

Výstupními dokumenty analýzy rizik jsou Zpráva o hodnocení aktiv a rizik, Plán zvládání rizik a Prohlášení o aplikovatelnosti. Zmíněné dokumenty podléhají aktualizacím v pravidelném šestiměsíčním cyklu.

4. SPECIFICKÉ PROVOZNÍ PROCESY

Metodika řízení provozu a další provozní procesy relevantní pro poskytování Služby jsou popsány v Řídící dokumentaci realizace smlouvy pro období provozu služeb v souladu s Přílohou č. 2 Rámcové smlouvy. Řídící dokumentace a její změny v průběhu provozu jsou oboustranně schvalovány oprávněnými osobami Objednatele a Objednatele dle Rámcové smlouvy.

Procesy bezpečnostních služeb provozu jsou řízeny a jejich provádění je evidováno v ServiceDesku SPCSS, kdy zjednodušený popis procesu je popsán níže na vloženém schématu:



5. PROVOZNÍ PARAMETRY A SLA

Měsíční Zpráva o úrovni a rozsahu poskytované Služby EET bude obsahovat informace o reálném plnění parametrů uvedených v této kapitole a bude hodnocena podle jejich souladu s hodnotami uvedenými ve Smlouvě.

5.1 Kategorizace bezpečnostních událostí

KBI (velmi závažný, závažný, méně závažný)	Kybernetický bezpečnostní incident
KBU	Kybernetická bezpečnostní událost
BH	Bezpečnostní hlášení

Pro snazší posouzení jednotlivých typů bezpečnostních událostí a jejich kategorizaci vznikne v rámci Řídící dokumentace oboustranně schvalovaný dokument „Kategorizace bezpečnostních událostí". Dokument bude zaznamenávat dohody o kategorizaci a způsobu vypořádání konkrétních typů bezpečnostních událostí pro budoucí využití při výskytu stejného typu události.

5.2 Požadovaná doba reakce

Doba reakce úrovně L1 je počítána od zaevidování bezpečnostního hlášení/kybernetické bezpečnostní události/kybernetického bezpečnostního incidentu (BH/KBU/KBI) do ServiceDesku SPCSS. Podpora L1 musí do doby uvedené v tabulce níže přijmout v ServiceDesku SPCSS BH/KBU/KBI na řešení.

Kategorizace	pracovní dny 7 - 18 hod	18 – 7 hod + mimopracovní dny
	Max doba reakce L1 v minutách	Max doba reakce L1 v minutách
KBI (velmi závažný, závažný, méně závažný)	15	15
KBU	15	15
BH	15	15

5.3 Komunikační kanály

Komunikačními kanály jsou ServiceDesk SPCSS, telefon a e-mail, konkrétní adresy a čísla jsou uvedené v Řídící dokumentaci.

5.4 Dostupnost služby a roční dostupnost v přechodném období

Roční dostupnost služeb je uveden v následující tabulce:

Režim poskytování bezpečnostní služby	Roční dostupnost
Nepřetržitá provozní doba 7x24	99,2 %

Plnění těchto parametrů bude vykazováno 1x měsíčně ve Zprávě o úrovni a rozsahu poskytované Služby EET. Celkové vyhodnocení a uplatnění pokut probíhá na konci každého celého roku provozu, počítáno od termínu začátku poskytování služby. Schválené odstávky nejsou součástí provozní doby a nepočítají se do SLA Roční dostupnosti služby.

Odstávky budou Poskytovatelem hlášeny Objednateli minimálně 20 pracovních dnů před požadovanou odstávkou. Objednatel je povinen se vyjádřit k požadavku na odstávku do pěti pracovních dnů od nahlášení požadavku, jinak je požadavek považován za schválený

6. POŽADOVANÉ SOUČINNOSTI OBJEDNATELE

- V oboustranně schválené Řídící dokumentaci stanoví Objednatel kontaktní osoby včetně komunikační matice pro případ řešení kybernetických bezpečnostních událostí a incidentů:
  - Kontaktní místo zákazníka;
  - Manažer kybernetické bezpečnosti;
  - Architekt kybernetické bezpečnosti;
  - Dispečer helpdesku (režim 24x7; možno pohotovostní kontakt/hot line);
  - Oddělení bezpečnosti;

- Objednatel zajistí potřebnou dostupnost nominovaných kontaktních osob pro poskytnutí součinnosti s ohledem na odsouhlasené termíny a vybaví je potřebnými pravomocemi.
- Objednatel poskytne nezbytnou součinnost při realizaci penetračních testů.

POPIS SLUŽBY EET S4-003

1. IDENTIFIKACE SLUŽBY EET

Údaje v následující tabulce identifikují Službu EET ve vazbě oblasti Služeb a typy Služeb definované v předmětu Rámcové smlouvy (odst. 4.2 a 4.3).

ID/číslo	**S4-003**
Název	**Odborné služby systémové integrace v období provozu služeb**
Oblast Služeb	Systémová integrace
Typ Služeb	Odborné služby na vyžádání

2. OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba je poskytována v období zahájeném a ukončeném milníky uvedenými v následující tabulce.

Milník	**Termín**
Zahájení poskytování Služby EET S4-003	1.12.2016
Ukončení poskytování Služby EET S4-003	Do vyčerpání finančních prostředků uvedených ve Smlouvě

3. ROZSAH POSKYTOVÁNÍ SLUŽBY

Časový rozsah služby i rozsah vyžádaných činností bude specifikován v jednotlivých Zadávacích a pověřovacích listech, viz odst. 10.4 Rámcové smlouvy a odst. 3.4.1 přílohy č. 1 Rámcové smlouvy.

4. KONTROLA KVALITY SLUŽBY

Kontrola kvality služby a akceptace částečných plnění bude probíhat formou výkazů činnosti a Akceptačních protokolů, viz odst. 10.4 Rámcové smlouvy a odst. 3.4.1 přílohy č. 1 Rámcové smlouvy.

5. POPIS ODBORNÝCH ROLÍ

Personální zajištění poskytování služby zahrnuje obsazení následujících rolí

5.1 Architekt (senior)

- navrhuje architekturu změn a rozšíření informačního systému;
- zajišťuje specifikaci služeb mezi informačním systémem a jinými okolními systémy a uživateli;

- navrhuje jednotlivé vrstvy informačního systému tak, aby byly vzájemně propojiteln zjišťoval kompaktní výkon;
- vybírá technologické i SW prvky informačního systému;
- podílí se na vedení technického týmu a zajišťuje údržbu technické specifikace informačního systému a přípravu změn;
- podílí se na tvorbě strategie rozvoje, definice a prosazování odpovídajících interních standardů;
- navrhuje metodiku rozvoje, správy a zabezpečení;
- odpovídá za návrh a posuzování technologických řešení;
- odpovídá za rozvoj technické infrastruktury ICT;
- podílí se na systémové integraci a konsolidaci prostředí technické infrastruktury;
- odpovídá za zpracování technických zadání, technických a funkčních specifikací, analytických studií a poptávek.

5.2 Analytik (senior)

- realizuje analýzu odborného zadání změn a rozšíření informačního systému;
- z legislativního a odborného zadání připravuje procesní schémata a specifikace „use cases" pro fungování informačního systému;
- definuje procesy a postupy, které jsou podporovány informačními systémy;
- navrhuje procesy a jejich průběh včetně jednotlivých činností;
- popisuje současný stav podpory procesů informačními systémy;
- popisuje návaznosti na jiné procesy podporované jinými informačními systémy;
- analyzuje potřeby odborných útvarů na podporu a průběh procesů;
- analyzuje požadavky odborných útvarů na nové procesy;
- koordinuje způsob výkonu procesu mezi více orgány veřejné správy a způsob předání dat pro podporu procesu;
- navrhuje způsob administrace procesu včetně případných legislativních potřeb;
- navrhuje řešení vzniklých problémů či kolize procesů;
- specifikuje úkoly pro členy technického týmu při vypracování technické specifikace potřebného HW a SW licencí včetně sizingu.

6. POŽADOVANÉ SOUČINNOSTI

Objednatel bude spolupracovat s Dodavatelem na vytváření dokumentů (písemných výstupů) a předá všechny nezbytné podklady týkající se obsahu zadaných písemných výstupů odborných služeb.

Objednatel bude spolupracovat s Dodavatelem při kontrole rozsahu poskytnutých odborných služeb, zejména formou poskytnutí informací o termínech realizovaných odborných služeb podle evidence přítomnosti specialistů na pracovištích Objednatele.

Další požadované součinnosti specifické pro vyžádané činnosti budou uvedeny v Zadávacích a pověřovacích listech.