Příloha č. 1

Požadavky kladené na systém ISDS

# Obsah

[1 Obsah 1](#_Toc20728058)

[2 Rámcové vymezení požadovaných Služeb 3](#_Toc20728059)

[3 Legislativní rámec – Dotčené právní předpisy 4](#_Toc20728060)

[3.1 Právní předpisy vztahující se k ISDS: 4](#_Toc20728061)

[3.2 Evropské směrnice a Nařízení: 5](#_Toc20728062)

[4 Funkční zadání 6](#_Toc20728063)

[4.1 Funkční požadavky na provoz ISDS 6](#_Toc20728064)

[4.1.1 Nové budoucí funkcionality 27](#_Toc20728065)

[4.2 Funkční požadavky na provoz Aditivních služeb 27](#_Toc20728066)

[4.2.1 Datový trezor 27](#_Toc20728067)

[4.2.2 Poštovní datová zpráva 27](#_Toc20728068)

[4.2.3 SMS notifikace 27](#_Toc20728069)

[4.2.4 Kreditní systém datových schránek 27](#_Toc20728070)

[4.2.5 Nové budoucí funkcionality 27](#_Toc20728071)

[4.2.6 Migrace dat Aditivních služeb 27](#_Toc20728072)

[4.3 Funkční požadavky na provoz podpůrných služeb 27](#_Toc20728073)

[4.4 Podpora dodavatelů aplikací třetích stran 27](#_Toc20728074)

[4.5 Zajištění bezpečného provozu a dostupnosti ISDS 27](#_Toc20728075)

[4.6 Provozní požadavky na provoz podpůrných, obslužných a servisních služeb 27](#_Toc20728076)

[4.6.1 Bezpečnostní monitoring 27](#_Toc20728077)

[4.6.2 Service Desk - služby 27](#_Toc20728078)

[4.7 Požadavky na infrastrukturu 27](#_Toc20728079)

[4.7.1 Vývojové a interní testovací prostředí 27](#_Toc20728080)

[4.7.2 Veřejné testovací prostředí 27](#_Toc20728081)

[4.7.3 Předprodukční prostředí 27](#_Toc20728082)

[4.7.4 Produkční prostředí 27](#_Toc20728083)

[4.8 Obecné požadavky na technickou infrastrukturu 27](#_Toc20728084)

[4.9 Požadavky na zajištění klíčového hospodářství 27](#_Toc20728085)

[4.10 Platnost datových zpráv, dodejek a doručenek 27](#_Toc20728086)

[4.11 Výkonnostní požadavky 27](#_Toc20728087)

[5 Požadavky na datová centra (DC) 27](#_Toc20728088)

[6 Požadavky na počáteční Migraci 27](#_Toc20728089)

[6.1 Rámcový přehled dat pro migraci: 27](#_Toc20728090)

[6.2 Požadavky Objednatele 27](#_Toc20728091)

[6.3 Rozsah poskytnuté součinnosti Objednatele 27](#_Toc20728092)

[7 Požadavky na rozhraní vůči uživateli 27](#_Toc20728093)

[8 Požadavky na testování ISDS před uvedením do provozu 27](#_Toc20728094)

[8.1 Audit návrhové dokumentace a plánu Migrace 27](#_Toc20728095)

[8.1.1 Kritéria auditu pro akceptaci návrhové dokumentace a plánu Migrace 27](#_Toc20728096)

[8.2 Audit bezpečnosti ISDS před provedením Migrace dat a uvedením do Řádného a plného provozu 27](#_Toc20728097)

[8.2.1 Rozsah auditu 27](#_Toc20728098)

[8.2.2 Podmínky provedení auditu 27](#_Toc20728099)

[8.2.3 Kritéria auditu pro akceptaci 27](#_Toc20728100)

[8.3 Funkční, výkonnostní, integrační a bezpečnostní testy ISDS 27](#_Toc20728101)

[8.3.1 Kritéria pro akceptaci funkčních, výkonnostních a integračních testů 27](#_Toc20728102)

[9 Požadavky v oblasti bezpečnosti 27](#_Toc20728103)

[9.1 Legislativní vymezení 27](#_Toc20728104)

[9.2 Požadavky na soulad se Zákonem o kybernetické bezpečnosti 27](#_Toc20728105)

[9.3 Zajištění podmínek a součinnosti při auditu kybernetické bezpečnosti 27](#_Toc20728106)

[9.4 Požadavky na ochranu ISDS před útoky DoS a DDoS a škodlivým kódem 27](#_Toc20728107)

[9.5 Požadavky na provádění pravidelné prověrky obnovy ISDS 27](#_Toc20728108)

[10 Náležitosti měsíční zprávy o provozu 27](#_Toc20728109)

[11 Požadavky na Dokumentaci 27](#_Toc20728110)

# Rámcové vymezení požadovaných Služeb

Služby vycházejí ze stávajícího stavu a jsou specifikovány zejména:

* Provozními příručkami ISDS (funkčním designem ISDS a architekturou aplikace),
* Provozním řádem ISDS,
* Další dokumentací, která je součástí Smlouvy o zajištění provozu a rozvoje ISDS a jejích Příloh,
* Legislativním rámcem uvedeným v kap. 3. této Přílohy.

Služby zahrnují:

* Zpracování **návrhové dokumentace ISDS** a **dokumentace skutečného provedení ISDS**.
* Provedení **bezpečnostní analýzy zdrojových kódů Licencovaného software** a následně po projednání s Objednatelem odstranění případných zjištěných zranitelností ještě před uvedením do Řádného a plného provozu ISDS.
* Kontrolu **úplnosti, správnosti a funkčnosti zdrojových kódů Licencovaného software** a instalačních postupů včetně jejich praktického otestování bez zbytečného odkladu. Poskytovatel je povinen zjištěné neúplnosti, nedostatky a jiné problémy průběžně oznamovat Objednateli včetně popisu konkrétní neúplnosti/nedostatku/problému a jeho předpokládaného dopadu, a to vždy bez zbytečného odkladu po jejich zjištění.
* Poskytnutí služeb **technické infrastruktury** (HW, základní a generický SW, síťové prvky, datové linky, instalace a zprovoznění, implementaci Licencovaného software) pro zajištění **provozu ISDS**.
* Poskytnutí služeb **technické infrastruktury** (HW, základní a generický SW, síťové prvky, datové linky, instalace a zprovoznění, implementaci Licencovaného software) pro zajištění provozu **předprodukčního prostředí a prostředí veřejného testu**.
* Poskytnutí služeb **hostingu** ve dvou samostatných, navzájem propojených geograficky nezávislých datových centrech.
* Vytvoření **vývojového a interního testovacího prostředí** v datovém centru určeném Objednatelem v souladu s Přílohou č. 12 pro účely Služeb Rozvoje, které zahrnuje vytvoření prostředí vhodného pro:
  1. editaci a řízení změn zdrojového kódu,
  2. sestavení binárního kódu,
  3. testování binárních aplikací.
* Vytvoření **plánu Migrace** a provedení Migrace ze stávajícího ISDS na novou infrastrukturu Poskytovatele.
* Zajištění **Služeb Provozu** a s tím související poskytnutí funkčností ISDS oprávněným uživatelům v rozsahu odpovídajícím požadavkům Objednatele a zákonným požadavkům. Součástí Služeb Provozu je také poskytování podpůrných a servisních činností dle této Smlouvy.

Služby Provozu ISDS zahrnují především následující činnosti:

1. Služba zajištění bezpečného provozu a dostupnosti ISDS
2. Služby datových center včetně zajištění datové komunikace
3. Služby Service Desk
4. Služba bezpečnostního monitoringu

* Zajištění
  + - **školení, manuálů a dokumentace** pro využívání aplikace TTS Poskytovatele, a to nejpozději do Dne zahájení provozu ISDS
    - zaškolení v souvislosti s výstupy provozního monitoringu, a to nejpozději do Dne zahájení provozu ISDS
    - odpovídajícího zaškolení v dalších souvisejících procesech, a to nejpozději do Dne zahájení provozu ISDS,
    - aktualizace manuálů a dokumentace případně školení, při zavádění nových funkcionalit ISDS.
* Zpracování **katalogových listů** podle vzoru katalogového listu uvedeného v Příloze č. 8 obsahující detailní popis jednotlivých ICT služeb, které jsou součástí činností tvořících Služby Provozu (např. networking, zálohování, apod.).
* Řešení **bezpečnostních incidentů** v součinnosti se Správcem a Provozovatelem ISDS.
* Provádění **zálohování a obnovy dat ISDS**.
* **Obnovu ISDS** v případě havárie.
* **Odstranění vad** zjištěných při bezpečnostním auditu návrhové dokumentace a plánu Migrace, auditu ISDS před provedením ostrých migrací dat a uvedením do Řádného a plného provozu, a bezpečnostních auditech ISDS v termínech schválených Správcem a oběma smluvními stranami.
* Provádění **profylaxe ISDS** v období provozních odstávek.
* Vytvoření **plánu Migrace** celého ISDS na nového poskytovatele v souvislosti s **ukončením Smlouvy** v souladu s požadavky uvedenými ve Smlouvě.
* Poskytování **Služeb Rozvoje,** které zahrnují realizaci změnových požadavků Objednatele týkajících se Software tvořícího ISDS, jednotlivých komponent ISDS a jejich vzájemného propojení, konfigurace a napojení na externí systémy, a to včetně provedení programátorských prací, testování a implementace do ISDS. Služby Rozvoje se netýkají HW infrastruktury.

Služby Rozvoje zahrnují kompletní realizaci změnových požadavků spočívající ve změnách, úpravách nebo vytvoření nových komponent či funkcionalit ISDS včetně změn Software tvořícího ISDS, včetně Licencovaného software.

ISDS je informační systém kritické informační infrastruktury podle ZKB a obsahuje osobní údaje. Poskytovatel musí zajistit Služby plně v souladu požadavky ZKB a ZOOÚ.

Požadovaná dostupnost celého ISDS je 99,9 % s definovanou kvalitou Služeb. Kvalita a parametry Služeb jsou uvedeny v samostatné SLA (Service Level Agreement) v Příloze č. 6.

# Legislativní rámec – Dotčené právní předpisy

V této části jsou uvedeny právní předpisy a navazující právní akty vztahující se k ISDS, provozu ISDS a požadavkům kladeným na ISDS, které musí ISDS splňovat, a to vždy ve znění pozdějších změn.

## Právní předpisy vztahující se k ISDS:

* Zákon č.101/2000 Sb., o ochraně osobních údajů
* Zákon č.111/2009 Sb., o základních registrech
* Zákon č. 297/2016 Sb., o službách vytvářející důvěru pro elektronické transakce
* Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
* Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
* Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
* Zákon č. 499/2004 Sb., o archivnictví a spisové službě
* Vyhláška č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)
* Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek
* Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
* Usnesení vlády ze dne 25. 05. 2015 – určení prvků kritické informační infrastruktury (KII)
* Usnesení vlády ČR č. 382 ze dne 25. května 2015 k Akčnímu plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020
* Usnesení vlády České republiky č. 390 ze dne 25. května 2015 ke 2. aktualizaci Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu
* Usnesení vlády ČR č. 981-2015 3. aktualizace seznamu KI
* Usnesení vlády ČR č. 889/2015 z 02. 11. 2015 k dalšímu rozvoji informačních a komunikačních technologií služeb veřejné správy
* Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
* Nařízení vlády č. 432/2010 Sb., o kritériích pro určování prvku kritické infrastruktury;
* Nařízení Vlády č. 594/2006 Sb., o přepisu znaků do podoby, ve které se zobrazují v informačních systémech veřejné správy

## Evropské směrnice a Nařízení:

* Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
* Směrnice Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru
* Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů)

# Funkční zadání

V případě, že tato kapitola obsahuje i funkční požadavky, které vychází z legislativy, ale příslušný právní předpis dosud nenabyl účinnosti, je Poskytovatel povinen zprovoznit v rámci Služeb Rozvoje dotčené funkční požadavky po nabytí účinnosti příslušného právního předpisu a na základě písemného požadavku Objednatele za předpokladu, že k tomu Objednatel poskytne potřebnou součinnost. Realizace těchto funkcionalit bude hrazena z Ceny Služeb Rozvoje. Pokud budou výše uvedené funkční požadavky přesahovat rámec stávající Smlouvy, bude před jejich realizací uzavřen potřebný dodatek Smlouvy.

## Funkční požadavky na provoz ISDS

Funkční požadavky na provoz ISDS jsou dány mimo níže uvedeného také Provozním řádem ISDS a Provozními příručkami ISDS - Funkčním designem. V případě rozporu mezi jednotlivými dokumenty má přednost Funkční design.

|  | **Činnosti** | **Zajišťuje** | | | |
| --- | --- | --- | --- | --- | --- |
| **Objednatel - ČP (Správce - MV)** | | **Poskytovatel** | |
| **I** | **Integrace se Základními registry a dalšími ISVS** | | | | |
| **1** | **Údržba a provoz rozhraní pro komunikaci s Informačním systémem základních registrů (ISZR)** | | | | |
|  | Komunikace s ISZR | Zajistí potřebná oprávnění pro Poskytovatele | | Zajistí komunikaci prostřednictvím komunikačního rozhraní ISDS s ISZR.  Zajistí vedení logu ISZR požadavků. | |
|  | Údržba rozhraní s ISZR |  | | Zajistí implementaci změn komunikačního rozhraní ISDS s ISZR | |
| **2** | **Komunikace s registrem obyvatel (ROB)** | | | | |
|  | Získání a ukládání AIFO (Agendový identifikátor fyzické osoby) ROB |  | | V procesu zakládání uživatele ISDS zajistí získání AIFO ROB, pokud bude uživatel ztotožněn vůči ROB a pokud AIFO není již obsaženo v datech, které způsobují založení nebo změnu DS (notifikace z ROS).  Zajistí ukládání AIFO ROB v ISDS pro ztotožněné uživatele ISDS. | |
|  | Identifikátor datové schránky (DS) FO v ROB |  | | Zajistí zápis nebo vymazání identifikátoru DS FO (fyzické osoby) v ROB (Registr obyvatel) kdykoliv je DS FO zpřístupněna nebo znepřístupněna | |
|  | Načítání notifikačních souborů ROB |  | | Zajistí načítání notifikačních souborů ROB | |
|  | Automatická synchronizace dat s ROB |  | | Zajistí zpracování notifikačních souborů ROB a automatickou synchronizaci dat ISDS s ROB po notifikaci změn (Změny dat uživatelů ISDS, znepřístupňování DS FO). | |
|  | Manuální ztotožnění a synchronizace dat uživatelů a DS FO s ROB | Zadává v servisním modulu požadavky | | Zajistí ztotožnění uživatelů a synchronizaci dat uživatelů a DS po přijetí požadavků ze servisního modulu | |
|  | Ztotožňování při změnách údajů |  | | Zajistí vyhledávání a ztotožňování osob v ROB při změnách jména, příjmení, data narození nebo adresy osoby vedené v ISDS pro definované osoby bez AIFO ROB | |
| **3** | **Komunikace s registrem osob (ROS)** | | | | |
|  | Načítání notifikačních souborů ROS |  | | Zajistí načítání notifikačních souborů ROS | |
|  | Iniciace zřizování, znepřístupňování a změn popisu DS na základě údajů z notifikací ROS |  | | Zajistí zpracování notifikačních souborů ROS, automatické zakládání DS určených právních forem OVM (Orgán veřejné moci) a PO (dle odst. 1 § 5 a § 6 ZEU), znepřístupňování a změny popisu DS. Při určených změnách údajů zajistí zneplatňování přístupových údajů a příp. i generování dat pro odeslání nových přístupových údajů uživatelů DS. | |
|  |  |  | |  | |
|  | Identifikátor DS v ROS |  | | Zajistí zápis nebo vymazání identifikátoru DS v ROS kdykoliv je DS zpřístupněna nebo znepřístupněna | |
|  | Manuální synchronizace dat DS s ROS | Zadává v servisním modulu požadavky | | Zajistí synchronizaci dat DS po přijetí požadavků na synchronizaci s ROS ze servisního modulu | |
|  | Kukátko do ROS |  | | Zajistí v servisním modulu možnost porovnání dat ROS a ISDS pro IČO náležející k DS | |
| **4** | **Komunikace s registrem územní identifikace (RUIAN)** | | | | |
|  | Získávání adres z RUIAN |  | | Zajistí pro osoby vedené v ROS získávání adres explicitním dotazem na RUIAN s identifikátorem adresního místa přečteným z ROS. | |
| **5** | **Komunikace s registrem práv a povinností (RPP)** | | | | |
|  | Vkládání záznamu do RPP |  | | Zajistí vkládání záznamu do RPP při každém zápisu nebo vymazání identifikátoru DS do nebo z ROB nebo ROS. | |
| **6** | **Komunikace s  dalšími systémy a subjekty** | | | | |
|  | Rozhraní na centrálu Czech POINT | Zajistí potřebná oprávnění pro Poskytovatele | | Vytvoří a bude provozovat rozhraní na centrálu Czech POINT pro předávání dat žádostí jednotlivých agend ISDS na kontaktních místech Czech POINT.  Zajistí přebírání těchto dat do ISDS. | |
|  | Rozhraní na subjekty s povinností informovat (§15, odst.2-8, §16 ZEU) | Zajistí součinnost dotyčných subjektů | | Vytvoří a bude provozovat rozhraní na subjekty s povinností informovat (§15, odst.2 - 8, § 16 ZEU) pro předávání dat, která nelze předávat prostřednictvím základních registrů.  Zajistí přebírání těchto dat do ISDS. | |
|  | Rozhraní na ISEO (Informační systém evidence obyvatel) | Zajistí potřebná oprávnění pro Poskytovatele | | Vytvoří a bude provozovat rozhraní na ISEO pro předávání dat, která nelze předávat prostřednictvím základních registrů.  Zajistí přebírání těchto dat do ISDS. | |
|  | Komunikace ISDS a ISEO | Zajistí podmínky k využívání této služby | | Zajistí funkcionalitu, kdy na zásah uživatele (pracovníci Správce v servisním modulu) se správným pověřením bude umožněna aktualizace osobních údajů majitele datové schránky vůči ISEO. | |
|  | Rozhraní na SOVM (aplikace Seznam OVM), aktualizace dat schránek OVM (u kterých je editorem SOVM) | Zajistí potřebná oprávnění pro Poskytovatele | | Vytvoří a bude provozovat rozhraní na SOVM pro předávání dat, která nelze předávat prostřednictvím základních registrů.  Zajistí přebírání těchto dat do ISDS a aktualizace dat v ISDS. | |
|  | Komunikace s ROVM (rejstříkem OVM, součást RPP) | Zajistí potřebná oprávnění pro Poskytovatele | | Zajistí načítání notifikačních souborů ROVM a jejich zpracování. | |
|  | Iniciace zřizování, znepřístupňování a změn popisu DS na základě údajů z notifikací ROVM |  | | Zajistí zpracování notifikačních souborů ROVM, automatické zakládání DS určených právních forem OVM (dle § 6 odst. 1 ZEU), znepřístupňování a změny popisu DS. Při určených změnách údajů zajistí zneplatňování přístupových údajů a příp. i generování dat pro odeslání nových přístupových údajů uživatelů DS. | |
|  | Rozhraní Veřejného rejstříku (MSp) - Iniciace zřízení, odebrání oprávněné osoby – likvidátor | Zajistí potřebná oprávnění pro Poskytovatele | | Vytvoří a bude provozovat rozhraní na IS VR (Informační systém veřejných rejstříků) pro předávání dat, která nelze předávat prostřednictvím základních registrů.  Zajistí přebírání těchto dat do ISDS. | |
| **II** | **ZŘÍZENÍ, ZNEPŘÍSTUPNĚNÍ, ZRUŠENÍ DS** | | | | |
| **1** | **Zřízení DS OVM (běžné) § 6 odst. 1** | | | | |
|  | Získání dat o nově založených OVM |  | | Zajistí zpracování notifikací ROS a později ROVM, příp. jiných elektronicky přístupných evidencí, získání potřebných dat pro založení nových schránek v ISDS. | |
|  | Žádost o založení DS |  | | Vygenerování žádosti o zřízení DS | |
|  | Schválení žádosti, vytvoření DS |  | | ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám | |
|  |  |  | |  | |
| **2** | **Zřízení DS právnické osoby (PO) (běžné) § 5 odst. 1.** | | | | |
|  | Získání dat o nově založených PO |  | | Zajistí zpracování notifikací ROS, příp. jiných elektronicky přístupných evidencí, získání potřebných dat pro založení nových schránek v ISDS. | |
|  | Žádost o založení DS |  | | Vygenerování žádosti o zřízení DS | |
|  | Schválení žádosti, vytvoření DS |  | | ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám | |
| **3** | **Zřízení DS podnikající fyzické osoby (PFO) advokáta, daň. poradce, atd. (běžné)** | | | | |
|  | Získání dat o nově vzniklých subjektech advokátů, daňových poradců a insolvenčních správců, statutárních auditorů (dle §4 odst. 3 ZEU) |  | | Zajistí zpracování notifikací ROS, příp. jiných elektronicky přístupných evidencí, získání potřebných dat pro založení nových schránek v ISDS. | |
|  | Žádost o založení DS |  | | Vygenerování žádosti o zřízení DS | |
|  | Schválení žádosti, vytvoření DS |  | | ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám | |
| **4** | **Zřízení DS PFO na žádost** | | | | |
|  | Příjem žádosti PFO | | Zajistí vstupní kanály pro příjem žádosti | | Zajistí potřebné funkcionality pro příjem žádostí, a dále potřebná komunikační rozhraní |
|  | Předání ke zpracování do systému ISDS | | MV zajistí vstupní kanály pro příjem žádosti | | Zajistí příslušnou funkcionalitu, zajistí komunikační rozhraní pro přebírání dat |
|  | Kontrola dat v žádosti | |  | | Zajistí rozhraní do ROB, ROS, ISEO či do jiné elektronicky vedené přístupné evidence, pro kontrolu údajů v žádosti, případně pro jejich doplnění |
|  | Kontrola na existenci DS | |  | | ISDS, provede kontrolu |
|  | Vytvoření identifikátoru | |  | | Přidělí systém ISDS |
|  | Schválení žádosti, vytvoření DS | | MV prostřednictvím servisního modulu ISDS schválí žádost o založení DS | | ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám |
|  | Vytvoření DS | | MV prostřednictvím servisního modulu ISDS zadá požadavek na vytvoření DS | | ISDS online zpracuje požadavek na vytvoření DS |
|  | Ukládání žádosti PFO | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí archivaci příslušných záznamů |
| **5** | **Zřízení DS fyzické osoby (FO)** | | | | |
|  | Příjem žádosti FO | | MV zajistí vstupní kanály pro příjem žádosti | | Zajistí potřebné funkcionality pro příjem žádostí, a dále potřebná komunikační rozhraní |
|  | Předání ke zpracování do systému ISDS | | MV zajistí vstupní kanály pro příjem žádosti | | Zajistí příslušnou funkcionalitu |
|  | Kontrola dat v žádosti | |  | | Zajistí rozhraní do ROB, ISEO či do jiné el. vedené přístupné evidence, pro kontrolu údajů v žádosti, případně pro jejich doplnění |
|  | Kontrola na existenci DS | |  | | ISDS, provede kontrolu |
|  | Vytvoření identifikátoru | |  | | Přidělí systém ISDS |
|  | Schválení žádosti, vytvoření DS | | MV prostřednictvím servisního modulu ISDS schválí žádost o založení DS | | ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám |
|  | Ukládání žádosti FO | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí archivaci příslušných záznamů |
| **6** | **Zřízení DS PO na žádost (§ 5 odst. 2.) a DS OVM na žádost (§ 6 odst. 2.)** | | | | |
|  | Příjem žádosti PO, OVM | | MV zajistí vstupní kanály pro příjem žádosti | | Zajistí příslušnou funkcionalitu v servisním modulu a komunikační rozhraní |
|  | Předání ke zpracování do systému ISDS | | MV zajistí vstupní kanály pro příjem žádosti | | Zajistí příslušnou funkcionalitu v servisním modulu |
|  | Kontrola dat ve formuláři | |  | | Zajistí rozhraní do ROB, ROS či do jiné el. vedené přístupné evidence, pro kontrolu údajů v žádosti, případně pro jejich doplnění |
|  | Kontrola na existenci DS | |  | | ISDS, provede kontrolu |
|  | Vytvoření identifikátoru | |  | | Přidělí systém ISDS |
|  | Schválení žádosti, vytvoření DS | | MV prostřednictvím servisního modulu ISDS schválí žádost o založení DS | | ISDS online zpracuje požadavek na vytvoření DS, založí DS, založí přístupové účty a vygeneruje přístupové údaje primárním oprávněným osobám |
|  | Ukládání žádosti PO, OVM | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí archivaci příslušných záznamů |
| **7** | **Znepřístupnění a opětovné zpřístupnění DS FO, PFO na žádost** | | | | |
|  | Příjem žádosti, oznámení | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí rozhraní a funkcionality pro příjem žádostí |
|  | Kontrola dat | |  | | ISDS (funkcionalita servisního modulu) - předá informace podstatné pro operaci znepřístupnění či opětovného zpřístupnění |
|  | Zpracování žádostí | |  | | ISDS online zpracuje požadavek na znepřístupnění či zpřístupnění DS |
|  | Oznámení o znepřístupnění DS dotčeným subjektům | |  | | ISDS prostřednictvím určeného rozhraní zašle zprávu o znepřístupnění či opětovném zpřístupnění |
|  | Ukládání | |  | | ISDS zajistí archivaci příslušných záznamů |
| **8** | **Znepřístupnění a opětovné zpřístupnění DS PO na žádost (§ 5 odst. 2.) a DS OVM na žádost (§ 6 odst. 2.)** | | | | |
|  | Příjem žádosti, oznámení | | MV zajistí vstupní kanály pro příjem žádosti | |  |
|  | Kontrola dat | |  | | ISDS (funkcionalita servisního modulu) - předá informace podstatné pro operaci znepřístupnění či opětovného zpřístupnění |
|  | Rozhodnutí o znepřístupnění | | Zadání žádosti prostřednictvím rozhraní servisního modulu | | ISDS online zpracuje požadavek na znepřístupnění či zpřístupnění DS |
|  | Oznámení o znepřístupnění DS dotčeným subjektům | |  | | ISDS prostřednictvím určeného rozhraní zašle zprávu o znepřístupnění či opětovném zpřístupnění |
|  | Ukládání | |  | | ISDS zajistí archivaci příslušných záznamů |
| **9** | **Znepřístupnění DS PO a OVM (zřízených dle § 5 odst. 1. a § 6 odst. 1.)** | | | | |
|  | Získání dat o datových schránkách PO a OVM pro znepřístupnění | |  | | Zajistí zpracování notifikací ROS, příp. jiných elektronicky přístupných evidencí, získání potřebných dat pro znepřístupnění schránek PO nebo OVM v ISDS. |
|  | Znepřístupnění | |  | | ISDS provede znepřístupnění DS automaticky ve stanovené lhůtě |
|  | Oznámení o znepřístupnění DS dotčeným subjektům | |  | | ISDS prostřednictvím určeného rozhraní zašle zprávu o znepřístupnění |
|  | Ukládání | |  | | ISDS zajistí archivaci příslušných záznamů |
| **10** | **Zrušení DS FO, PFO** | | | | |
|  | Zrušení DS | |  | | ISDS provede automaticky ve stanovené lhůtě 3 let po znepřístupnění, dle § 13 ZEU |
|  | Likvidace dat - obsah datové schránky | |  | | ISDS zajistí automaticky (výmaz obsahu datových zpráv, logy zůstávají) |
| **11** | **Zrušení DS PO** | | | | |
|  | Zrušení DS | |  | | ISDS provede automaticky ve stanovené lhůtě |
|  | Likvidace dat - obsah datové schránky | |  | | ISDS zajistí automaticky (výmaz obsahu datových zpráv, logy zůstávají) |
| **12** | **Zrušení DS OVM** | | | | |
|  | Zrušení DS | |  | | ISDS provede automaticky ve stanovené lhůtě |
|  | Likvidace dat - obsah datové schránky | |  | | ISDS zajistí automaticky (výmaz obsahu datových zpráv, logy zůstávají) |
| **III** | **SPRÁVA PŘÍSTUPU K DS** | | | | |
| **1** | **Definice postupu přihlašování** | | | | |
|  | Náležitosti přístupových údajů a elektronické prostředky k přihlášení.  Technické podmínky a bezpečnostní zásady přístupu do DS | | MV vydává a upravuje vyhlášku dle zmocnění v § 9 odst. 3 a 4 ZEU | | Zpracovává technické podklady pro přípravu vyhlášky |
| **2** | **Generování nových přístupových údajů** | | | | |
|  | Při zřízení DS – dle §10 ZEU | |  | | ISDS zajistí generování přístupových údajů nebo přístupových účtů (automatický proces při zřízení DS) |
|  | Při oznámení dle odst. 3 §12 ZEU | | MV pro určené právní formy OVM zajišťuje aktualizace dat v SOVM | | ISDS zajistí generování přístupových údajů (automatický proces při zpracování notifikací z ROS, ROVM, příp. předání dat z SOVM) |
|  | Při zmocnění pověřených osob - § 8, odst. 6 a 7 ZEU | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí generování přístupových údajů (na základě přijaté žádosti prostřednictvím servisního modulu). ISDS přijme žádost o zřízení přístupu. |
|  | Ukládání žádostí | |  | | ISDS zajistí archivaci příslušných záznamů |
|  | Zavedení účtu osoby do systému | |  | | ISDS zavede účet osoby do systému, generuje přístupové údaje a pokud mají být předány, zajistí jejich předání buď formou pro tisk, nebo zasláním elektronické výzvy a využitím virtuální obálky |
|  | Oznámení o zavedení další osoby | |  | | Datová zpráva do vlastních rukou |
| **3** | **Zneplatňování přístupových údajů** | | | | |
|  | Při změně – odst. 2 a 3 § 12 ZEU | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí zneplatňování přístupových údajů (automatický proces při zpracování notifikací z ROS, ROVM, příp. předání dat z SOVM).  ISDS zajistí zneplatňování přístupových údajů (na základě přijaté žádosti prostřednictvím servisního modulu) |
| **4** | **Zneplatnění přístupových údajů a vydání nových** | | | | |
|  | Při ztrátě, odcizení, atp. – odst. 1  § 12 ZEU | | MV zajistí vstupní kanály pro příjem žádosti | | ISDS zajistí proces zneplatňování přístupových údajů a vydání nových buď na základě přijaté žádosti dle příslušných právních předpisů, nebo prostřednictvím servisního modulu. |
|  | Ztotožnění s osobou vedenou v systému | |  | | ISDS (funkcionalita servisního modulu) - zpracuje žádost, ověří údaje a oprávnění osoby |
|  | Kontrola na opětovné vydání PÚ | |  | | ISDS (funkcionalita servisního modulu) zjistí interval od předchozího vydání přístupových údajů a vrátí odpověď pro určení, jestli má být vybírán správní poplatek |
|  | Výběr správního poplatku | | MV, kontaktní místo Czech POINT | | Po příslušné změně ZEU ISDS umožní výběr správního poplatku |
|  | Zneplatnění starých, vydání nových přístupových údajů | |  | | ISDS zajistí zneplatnění starých, generuje nové přístupové údaje a předá je pro tisk, zásilka do vlastních rukou, příp. „virtuální obálka“ |
| **5** | **Předávání údajů pro tisk obálek s přístupovými údaji a dalšími informacemi** | | | | |
|  | Generování údajů pro tisk | | Objednatel určuje typy a pořadí priorit výběru adres pro odesílání obálek s přístupovými údaji a dalšími informacemi. Změny priorit na základě realizace změnových požadavků. | | ISDS zajistí generování údajů pro tisk obáleks přístupovými údaji a dalšími informacemi, ve struktuře dat dle dokumentu Funkční design.  Adresy pro obálky jsou předávány v souladu s Objednatelem schválenými typy a pořadím priorit výběru adres. ISDS udržuje aktualizované číselníky států a potřebných poskytovaných poštovních služeb, určuje typy obálek k odeslání dle dokumentu schválených procesů pro odesílání obálek s přístupovými údaji (Typy a texty PÚ) |
|  | Předání údajů | |  | | ISDS v dohodnutých termínech předá přístupové údaje pro tisk do externího systému hybridní pošty. |
|  | Řazení zásilek s PÚ | |  | | Zajistí u zásilek systémem ISDS rozpoznaných jako zásilky do zahraničí a zásilky automaticky rozpoznané jako problémové (např. chybí nebo neznámé PSČ nebo je nestrukturovaná adresa) řazení do speciální fronty zásilek, která bude předávána systému hybridní pošty 1x týdně v samostatné dávce. |
| **IV** | **Distribuce přístupových údajů nebo informací ke změnám přístupových účtů** | | | | |
| **1** | **Hybridní pošta** | | | | |
|  | Převzetí dat připravených pro tisk | |  | | Zajistí technický import dat, připravených pro výrobu obálek a tisk, do systému hybridní pošty |
|  |  | |  | |  |
| **2** | **Virtuální obálky** | | | | |
|  | Vydání přístupových údajů elektronickým způsobem | |  | | Zajistí možnost vydávání nových přístupových údajů formou tzv. „virtuální obálky“ pro osobně podávané žádosti na kontaktním místě Czech POINT - přístupové heslo pro první přihlášení do systému resp. přístupové heslo při znovu vydávání přístupových údajů. Součástí rozhraní pro aktivační portál (potřebný pro získání přístupových údajů virtuální obálky uživatelem) bude i zpětná vazba do systému ISDS, která bude zaznamenávat informace o „doručení“ přístupových údajů formou virtuální obálky. |
|  | Zobrazení informací o virtuální obálce | |  | | Zajistí, aby v rámci servisního modulu byly zobrazeny informace o tom, že přístupové údaje k příslušné datové schránce byly odeslány na emailovou adresu a o jakou e-mailovou adresu se jedná (identifikace). |
|  | Napojení na aktivační portál Czech POINT | |  | | Zajišťuje napojení na aktivační portál pro předávání přístupových údajů formou virtuálních obálek. |
| **V** | **PROVOZ DS** | | | | |
| **1** | **Přístup k DS (portál ISDS, webové služby ISDS)** | | | | |
|  | Přístup k datové schránce | |  | | ISDS umožní přístup prostřednictvím portálu po úspěšném přihlášení do systému ISDS.  ISDS umožní přístup prostřednictvím specifického rozhraní (webové služby) po úspěšném přihlášení do systému ISDS. |
|  | Přístup do znepřístupněné datové schránky | |  | | Zajistí uživatelům možnost přístupu do znepřístupněné datové schránky v režimu „read-only“. T.j. mohou si přečíst a stáhnout doručené zprávy, ale do datové schránky již nemůže být dodáváno ani nelze zprávy odesílat. |
| **2** | **Přijetí zprávy** | | | | |
|  | Přijetí datové zprávy | |  | | ISDS zajistí přijetí zprávy systémem a vyrozumění vlastníka DS o dodání určeným způsobem, dle nastavení notifikací u DS. |
| **3** | **Náhled datové zprávy** | | | | |
|  | Funkce "Náhled" datové zprávy | |  | | Zajistí v rámci webového portálu pro uživatele DS funkci „Náhled“, která dovolí otevřít kompletní obálku datové zprávy a zpřístupní přílohy obsažené v datové zprávě. Požadované operace se zprávou: tisk obálky, odeslání ke konverzi; požadované operace s přílohami: stažení jednotlivě, stažení najednou v ZIP, odeslání ke konverzi. |
| **4** | **Zpřístupnění adresáře DS, identifikace vlastníků** | | | | |
|  | Zpřístupnění adresáře DS, identifikace vlastníků DS | | MV schvaluje podobu adresáře | | ISDS poskytne služby, které umožní zjistit, zda zadaný subjekt má DS nebo nemá, zda je DS přístupná či nikoliv, zda lze do DS obecně doručovat či nikoliv |
|  | Vedení veřejného seznamu dle §14b ZEU | |  | | Zajistí vedení veřejného seznamu dle §14b ZEU přístupného způsobem umožňujícím dálkový přístup. Zajistí vytvoření webové stránky seznamu datových schránek. |
| **5** | **Validace existence DS adresáta** | | | | |
|  | Validace existence DS adresáta | |  | | ISDS poskytne službu, která umožní validovat existenci adresáta v ISDS (resp. předá informaci o existenci DS zadaného subjektu) |
| **6** | **Odeslání a dodání zprávy** | | | | |
|  | Odeslání a dodání DZ | |  | | ISDS zajistí dodání zprávy do DS adresáta, pokud tato existuje a není v daný časový okamžik znepřístupněna |
|  | Garantovaná doba dodání DZ | |  | | ISDS zajistí dodání řádně podané datové zprávy z datové schránky odesílatele do datové schránky adresáta v garantované době do 4 hodin, v rozsahu 0:00 – 24:00 (24x7). Za úspěšně dodanou datovou zprávu se považuje datová zpráva, u které doba dodání nepřevýší 4 hodiny. Do garantované doby se nezapočítává vyhrazená doba. |
| **7** | **Doručení zprávy** | | | | |
|  | Doručení DZ | |  | | ISDS zaznamenává informaci, zda zpráva byla doručena přímo (přihlášením uživatele s právy číst zprávu do DS adresáta, dle ZEU) nebo zda vypršela lhůta pro doručení fikcí |
| **8** | **Systémová datová zpráva** | | | | |
|  | Odeslání systémové DZ | |  | | Zajistí možnost zasílat systémové zprávy Správce a systémové zprávy Objednatele dle jeho volby, zadávání odesílání zpráv prostřednictvím servisního modulu. Systémová zpráva nemá charakter DZ, systémové zprávy se nebudou objevovat ve statistikách. |
| **9** | **Notifikace pro adresáta** | | | | |
|  | Notifikace pro adresáta | |  | | ISDS zajistí notifikace předepsané zákonem (a další požadované Správcem a Provozovatelem) a to prostřednictvím definovaných informačních prostředků (e-mail,SMS, systémové zpráva) |
| **10** | **Oznámení o doručení** | | | | |
|  | Oznámení o doručení | |  | | ISDS zajistí oznámení o dodání, doručení a změně na nedoručitelnou prostřednictvím DS odesilatele |
| **11** | **Vedení postupu doručení** | | | | |
|  | Vedení postupu doručení | |  | | ISDS - automatický proces zajišťující vedení evidence o změnách stavů zpráv - podání, dodání, doručení, způsobu doručení (přímé, uplynutí lhůty), dni a času změn stavů, atd. |
| **12** | **Dohledání postupu doručení** | | | | |
|  | Dohledání postupu doručení | |  | | Prostřednictvím servisního modulu ISDS bude možné získat veškeré informace vztahující se k doručení určité datové zprávy včetně průběhu doručování a příslušných důkazních materiálů |
|  | Doručenka a její formát | |  | | Zajistí, aby k informaci o stavu doručení měl přístup odesílatel i adresát. Podoba doručenky ve formě logu, tzn. postupně zaznamenán čas podání, čas dodání, doručení, případně čas znedoručitelnění. Doručenku lze exportovat v PDF nebo v podepsaném XML (ZFO) |
| **13** | **Změna přístupových údajů uživatelem (změna hesla)** | | | | |
|  | Změna přístupových údajů uživatelem | |  | | ISDS zajistí uživatelskou možnost změny přístupových údajů prostřednictvím rozhraní portálu a prostřednictvím veřejných webových služeb |
| **14** | **Změna přístupových údajů uživatelem (zavedení elektronického prostředku pro přihlašování) § 9 odst. 3 ZEU** | | | | |
|  | Změna přístupových údajů uživatelem | | schvaluje podmínky | | ISDS zajistí uživatelskou možnost zavedení či změny přístupových údajů prostřednictvím rozhraní portálu - zavedení elektronického prostředku pro přihlášení. |
| **15** | **Třetí autentizační metoda** | | | | |
|  | Autentizace uživatelů pro přístup do DS | |  | | Zajistí pro autentizaci uživatelů volitelný způsob přihlašování s využitím jednorázového kódu, zasílaného prostřednictvím SMS nebo vygenerovaného určenou aplikací na zařízení uživatele. |
| **16** | **Nepovinná změna hesla po 90 dnech (přístupového hesla)** | | | | |
|  | Změna hesla | |  | | Zajistí možnost uživatelům v uživatelském rozhraní ISDS zrušit omezení platnosti hesla (90 dnů) na časově neomezenou dobu. Primárně bude periodicita změny hesla po devadesáti dnech nastavena jako „true“. Uživatel bude mít volbu toto nastavení odstranit a zpětně zaktivovat, přičemž bude viditelně upozorněn, že se tím snižuje úroveň bezpečnosti hesla. |
| **17** | **Seznamy DZ v portálovém zobrazení** | | | | |
|  | Seznam DZ v datové schránce | |  | | Zajistí přístup k seznamům došlých a odeslaných DZ uložených v datové schránce, včetně DZ uložených v Datovém trezoru. Umožní filtrování a výběr dle definovaných podmínek. |
|  | Seznamy archivních záznamů o DZ | |  | | Zajistí přístup k seznamům archivních záznamů o smazaných DZ, v dělení na došlé a odeslané, včetně exportu seznamu. Zajistí stažení informace o postupu doručování i pro archivní záznamy. |
| **18** | **Optimalizace rozhraní pro mobilní zařízení** | | | | |
|  | Optimalizovaný webový portál ISDS | |  | | Zajistí přístup ke službám ISDS prostřednictvím webového rozhraní ISDS optimalizovaného pro mobilní zařízení (přístup prohlížečem) |
| **19** | Vytvoření přílohy DZ přímo ve webovém portálu | | | | |
|  | Vytvoření textových příloh na webovém portálu ISDS | |  | | Webový portál ISDS umožní při přípravě nové zprávy k odeslání vytvořit přílohu DZ přímo z vepsaného textu (který bude převeden do formátu PDF a připojen jako příloha DZ). |
| **VI** | **Další funkce** | | | | |
| **1** | **Logování informací v bezpečném logu** | | | | |  |  | kontroluje své pracovníky a postupy i pracovníky a postupy Subdodavatele |
|  | Logování dalších událostí spojených s provozem ISDS | | MV definuje události k logování | | Zajistit v bezpečném logu vedení informací i o cca 100 různých událostech provozu ISDS.  Minimální požadavky na bezpečný log jsou:   * Zajistit log proti neoprávněnému přístupu * Zajistit log proti neoprávněnému mazání * Zajistit log proti neoprávněným změnám v záznamech |
| **2** | **Řízení a konfigurování ISDS s možnosti identifikovat původce těchto činností** | | | | |  |  | Zajistí v servisním modulu v části Forenzní vyhledávání přístup k datům bezpečného logu |
|  | Blokování konfigurace ISDS bez možnosti jednoznačné identifikace původce | |  | | Zajistí, aby uživatelé oprávnění ke vstupu do interní sítě ISDS přes VPN (virtuální privátní síť) nemohli obejít Access Manager při provádění řízení a konfigurování ISDS |
| **3** | **V nastavení eDirectory blokovat anonymní přihlášení** | | | | |  |  | Zajistí v servisním modulu v části Forenzní vyhledávání přístup k datům bezpečného logu |
|  | Blokování anonymních přihlášení | |  | | Zajistí, aby uživatel se síťovým přístupem neměl možnost se přihlásit do eDirectory bez uvedení jména a hesla |
| **4** | **Pravidla směrování na síťových prvcích vnitřních sítí ISDS** | | | | |  |  | Zajistí v servisním modulu v části Forenzní vyhledávání přístup k datům bezpečného logu |
|  | Blokování anonymních přihlášení | |  | | Zajistí, aby uživatel se síťovým přístupem neměl možnost se přihlásit do eDirectory bez uvedení jména a hesla |
| **5** | **Report přístupů do datových schránek** | | | | |  |  | Zajistí v servisním modulu v části Forenzní vyhledávání přístup k datům bezpečného logu |
|  | Report přístupů do datových schránek | |  | | Zajistí evidenci a výpis informací o tom, kdo měl v daném čase přístup do datové schránky. |
| **6** | **Přidávání časových razítek do DZ - (** datová zpráva) | | | | |  |  | Zajistí v servisním modulu v části Forenzní vyhledávání přístup k datům bezpečného logu |
|  | Komunikační rozhraní mezi ISDS a TSA | | Zajistí funkčnost komunikačního rozhraní TSA pro vydávání časových razítek | | Zajistí propojení ISDS s primární a záložní lokalitou TSA. Zajistí přednostní využití přímého propojení ISDS s primární lokalitou TSA. |
|  | Proxy časového razítka | |  | | Zajistí v případě detekování nedostupnosti časového razítka z primární lokality TSA automatické přepnutí na odběr časových razítek ze záložní lokality TSA |
|  | Vložení podacího časového razítka | |  | | Zajistí, aby dle § 20 odst. 1 ZEU při příjmu DZ do systému bylo do vzniklé datové zprávy přidáno podací časové razítko, zajišťující integritu DZ a časový údaj o podání. |
|  | Doplňování časového razítka do obálky DZ | |  | | Zajistí, aby ve vnější obálce uložené DZ nebo dodejky (po aplikaci elektronické značky MV) bylo obsaženo časové razítko, které umožní zahájit trvalou archivaci souboru mimo ISDS. |
| **7** | **Zajištění dlouhodobé platnosti datových zpráv a možnosti potvrzení autenticity datových zpráv** | | | | |  |  |  |
|  | Dlouhodobá platnost datových zpráv | |  | | Umožní zajištění dlouhodobé platnosti a průkaznosti elektronické značky (nebo elektronické pečetě) a elektronických časových razítek a jejich časové kontinuity v datových zprávách i pro případy, kdy jsou uživatelem uloženy mimo ISDS, např. aby podle ZEU bylo možné provést konverzi elektronického dokumentu do listinné podoby. |
|  | Potvrzení autenticity datových zpráv | |  | | Umožní prověření autenticity datových zpráv – ověření, jestli jakákoliv konkrétní datová zpráva, vytvořená v ISDS a uložená mimo ISDS, byla vygenerována systémem ISDS a jestli její obsah nebyl po výstupu z ISDS změněn. Ověřující uživatel nemusí být odesílatelem ani adresátem ověřované zprávy. |
|  | Zpřístupnit všem uživatelům ISDS informace, které jsou o nich v ISDS vedeny | |  | | Umožní oprávněnému uživateli vidět základní data, která jsou o něm v ISDS vedena. |
|  | Dlouhodobá možnost čtení obsahu datových zpráv, dodejek a doručenek | |  | | Zajistí bezplatnou dostupnost softwarového nástroje pro uživatele ISDS k zobrazení obsahu jakékoliv datové zprávy, dodejky a doručenky, vytvořené v ISDS a uložené mimo ISDS, a to i zpětně pro všechny dostupné verze zpráv, dodejek a doručenek. Součástí nástroje je i kontrola a analýza CAdES úrovně podpisu. |
| **8** | **Zabezpečení systému proti ztrátě datových zpráv a neoprávněnému přístupu k nim** | | | | |  |  |  |
|  | Způsob odeslání zpráv | |  | | Zajistí způsob odesílání (tj. podání) zpráv:   * uživatel odesílá zprávu prostřednictvím uživatelského rozhraní (webový portál nebo web services) * při podání je zkontrolována integrita a formát zprávy v souladu s § 20 odst. 2 ZEU * zpráva je synchronně ukládána do trvalého souborového úložiště renomovaného výrobce ve dvou geograficky oddělených replikách a navíc do dočasného úložiště * dokud není zpráva uložena v obou replikách, není potvrzeno uložení * potvrzení o přijetí zprávy ke zpracování je vydáno uživateli po dokončení ukládání zprávy v obou lokalitách, kontrole integrity a formátu a zápisu popisných informací * úložiště v obou lokalitách jsou nezávisle zálohována * soubor je odstraněn z dočasného úložiště pro příjem zpráv po provedení plné zálohy trvalého úložiště |
|  | Vyzvednutí zprávy | |  | | Zajistí pro vyzvedávání zpráv:   * Uživatel má plný přístup ke zprávě po stanovený počet dnů pro opětovné stažení * Notifikační zprávy jsou uživatelům odesílány až po bezpečném dokončení procesů. * Všechny operace jsou logovány a logy ukládány bezpečným způsobem * V případě potřeby forenzního dohledávání a dokazování bude poskytnuta součinnost |
|  | Zabezpečení datových zpráv | |  | | Pro naplnění ustanovení § 14, odst. 5 a 6 ZEU zabezpečí ochranu datových zpráv proti neoprávněnému přístupu následujícími opatřeními:   * Obsah datových zpráv je před neoprávněným přístupem zabezpečen šifrováním – šifruje se vlastní obsah datových zpráv prostřednictvím odpovídajících mechanizmů * Datové zprávy jsou v datovém poli uloženy výhradně v šifrované podobě – pokud je nezbytná jakákoliv manipulace s datovou zprávou, která vyžaduje dešifraci, děje se tak výhradně v rámci přesně definovaných procesů (např. antivirová kontrola) a pouze v operační paměti * V procesu přijímání nebo odesílání zprávy jsou veškeré komunikační kanály šifrovány (HTTPS, VPN) takže přístup neoprávněné osoby k datům je vyloučen |
| **9** | **Povolení příjmu zpráv s přílohou až 50 MB u vybraných schránek** | | | | |
|  | Povolení příjmu zpráv s přílohou až 50 MB | |  | | Systém umožní prostřednictvím webového portálu ISDS a webových služeb ISDS přijímat a odesílat zprávy se souhrnnou velikostí příloh až 50 MB do schránek, které byly zřízeny podle § 6 odst. 2 zákona o elektronických úkonech a autorizované konverzi dokumentů po 31. říjnu 2018, dle podmínek, stanovených SLA (v Příloze 6 Smlouvy). |
| **10** | **Mazání datových zpráv po 3 letech** | | | | |
|  | Výmaz dodaných zpráv nejdříve 3 roky ode dne, kdy byla datová zpráva dodána do datové schránky | |  | | Systém umožní, v souladu s ust. § 6 vyhlášky č. 194/2009 Sb., vymazat ze systému datové zprávy nejdříve po 3 letech ode dne, kdy byla datová zpráva dodána do datové schránky |
| **11** | **Přihlašování s použitím klientského certifikátu** | | | | |
|  | Přihlašování s použitím klientského certifikátu | |  | | Systém umožní uživatelům přihlášení s použitím přístupového jména, hesla a osobního přístupového certifikátu, vydaného těmto fyzickým osobám certifikačními autoritami majícími v ČR akreditaci. |
| **12** | **Informovanost uživatelů ISDS o tom, jaké osobní údaje o nich systém DS drží a zpracovává dle článku 15 Nařízení (EU) 2016/679 (GDPR).** | | | | |
|  | Stránka Portálu o osobních údajích | |  | | Systém umožní v rámci záložky na stránce **Nastavení** nazvané **Osobní údaje** zpřístupnit uživateli DS jakožto subjektu údajů přehled zpracovávaných osobních údajů o jeho osobě. |
|  | Export dat | |  | | Systém umožní uživateli export sestavy zpracovávaných osobních údajů pro potřebu uživatele, popř. pro přenos dat mezi informačními systémy. Výstup je ve formátu PDF, elektronicky podepsaný s využitím certifikátu Správce. Každé stažení souboru je zaznamenáno v safelogu. |
| **13** | **Přihlašování k ISDS prostřednictvím Národní identitní autority** | | | | |
|  | Přihlášení k systému | |  | | Systém umožní přihlášení prostřednictvím autentizační brány Národní identitní autority ( dále jen „NIA“) |
|  | Zakázání / Povolení přihlášení prostřednictvím NIA pro celé ISDS | |  | | Systém umožní v rámci nastavení zakázat/povolit přihlášení prostřednictvím NIA pro celé ISDS. |
|  | Zakázání / Povolení přihlášení prostřednictvím NIA pro uživatele schránky | |  | | Systém umožní, aby přihlášený uživatel pro svůj účet nebo uživatel s oprávněním administrátor pro všechny účty schránky mohl zakázat/povolit přihlašování prostřednictvím NIA |
|  | Zrušení (výmaz) existujících pseudonymů | |  | | Systém umožní, aby přihlášený uživatel u svého účtu nebo uživatel s oprávněním administrátor u všech účtů schránky mohl provést výmaz pseudonymů uložených v ISDS, a tím znemožnit jejich použití pro přihlášení. |
| **14** | **Přihlašování k ISDS prostřednictvím Mobilního elektronického prostředku (MEP)** | | | | |
|  | Přihlášení uživatele ke klientskému portálu (nebo odesílací bráně, autentizační službě) | |  | | Systém umožní přihlášení prostřednictvím elektronického prostředku **založeného na použití mobilních zařízení** |
|  | Aplikace MEP pro mobilní zařízení | | Správce zajistí zveřejnění aplikace | | Zajistí vývoj, údržbu a distribuci softwarové aplikace pro mobilní zařízení na platformě Android a iOS, umožňující přihlašování k ISDS prostřednictvím MEP |
|  | Zálohování profilů MEP | |  | | Uživatel bude mít k dispozici nástroje pro vytvoření bezpečnostně chráněné zálohy dat (profilu**)** aplikace MEP a pro její obnovení v jiném mobilním zařízení. |
|  | Možnost zablokování MEP | |  | | Systém umožní zablokování prostředku MEP vzdáleně, bez nutnosti návštěvy kontaktního místa veřejné správy |
|  | Možnost zákazu přihlašování metodami využívajícími jméno/heslo pro uživatele s aktivovaným MEP | |  | | Systém umožní, aby si uživatel s aktivovaným MEP zakázal/povolil pro svůj uživatelský účet přihlašování metodami využívajícími jméno/heslo |
|  | Přihlášení aplikací třetích stran k uživatelskému účtu | |  | | Systém umožní podporu přihlašování prostřednictvím MEP i v rámci webových služeb |
|  | Notifikační služby | |  | | Systém umožní notifikace na mobilním zařízení alespoň o:   * nových DZ * odeslaných DZ, které nelze dodat/doručit * přihlášení pomocí jedné z metod používajících jméno/heslo (bez MEP) * aktivitách spojených s MEP (aktivace dalšího MEP, deaktivace MEP, provedení zálohy MEP, obnovení zálohy atd.) |

### Nové budoucí funkcionality

Poskytovatel je povinen zprovoznit na základě písemného požadavku Objednatele tyto funkcionality:

1. **Nezávislá autentizační služba**

ISDS v současné době poskytuje službu tzv. ExtIS, která umožňuje obecným informačním systémům autentizovat své uživatele prostřednictvím přístupových údajů do datové schránky. Dostupnost služby ExtIS je přímo závislá na celkové dostupnosti systému ISDS. V ISDS probíhá řada změn, které vyžadují odstávku celého systému.

Poskytovatel je povinen zajistit bezvýpadkový provoz služby ExtIS pro externí systémy i v případě odstávek systému ISDS. Primární komponenty, které jsou nezbytné pro běh služby ExtIS, jsou: AGW, eDirectory, síťová infrastruktura a bezpečný log.

Tuto funkcionalitu Poskytovatel zprovozní do 8 měsíců ode dne, kdy obdrží písemný požadavek Objednatele.

## Funkční požadavky na provoz Aditivních služeb

### Datový trezor

|  |  |  |  |
| --- | --- | --- | --- |
| **Procesy** | | **Zajišťuje** | |
| **Objednatel (ČP)** | **Poskytovatel** |
| **I** | **Zajištění funkcí služby Datový trezor** | | |
| **1** | Služba Datový trezor |  | ISDS umožní (dle §20, odst.4 ZEU)na žádost držitele datové schránky uložení dodané datové zprávy v datové schránce po dobu delší, než je doba stanovená vyhláškou. Za uložení dodané datové zprávy v datové schránce po dobu delší, než je doba stanovená vyhláškou, náleží Provozovateli informačního systému datových schránek odměna, která se stanoví podle cenových předpisů – ISDS umožní ČP účtování a inkasování uvedené odměny. |
| **2** | Funkce služeb Datových trezorů |  | Zajistí funkce ISDS pro uložení datových zpráv v datové schránce po dobu delší, než je stanovena vyhláškou, tzv. služby Datového trezoru dle specifikací v provozní příručce Funkční design, část Dlouhodobé úložiště zpráv – Datový trezor a související. |
| **3** | Neveřejné webové služby ISDS pro službu Datový trezor |  | Zajistí funkce webových služeb pro službu DT dle specifikací v provozní příručce Funkční design, Dlouhodobé úložiště zpráv – Datový trezor a související. |
| **4** | Veřejné webové služby ISDS pro službu Datový trezor |  | Zajistí funkce webových služeb pro službu DT dle specifikací v Provozním řádu, části WS\_ISDS\_Vyhledavani\_datovych\_schranek.pdf |
| **5** | Kreditní DT | ČP zajistí předání potřebných parametrů pro výpočet ceny kreditního DT, schvaluje způsob výpočtu ceny kreditního DT. | ISDS zajistí výpočet ceny služby, zřízení služby na základě pokynu uživatele a odečtení příslušného kreditu |
| **6** | Smluvní DT | ČP zajistí uzavření smlouvy s uživatelem a vydání pokynu pro zřízení smluvního DT | ISDS umožní ČP prostřednictvím specifického rozhraní (webové služby) zadávání požadavků na nastavení smluvních DT pro určené datové schránky.  ISDS zajistí zřízení služby DT na základě pokynu ČP. |
| **7** | Změna typu služby | ČP stanovuje požadavky na možnosti změn typů DT a na vlastnosti a parametry akčních DT | ISDS zajistí možnost změny typu služby mezi Kreditní DT a Smluvní DT ke dni expirace původního typu služby, nastavení a ukončení platnosti dalších typů DT (akčních) na základě požadavku ČP nebo uživatele. |
| **8** | Zrušení DT uplynutím doby | ČP stanovuje požadavky na ISDS pro mazání zpráv pro jednotlivé typy DT | ISDS zajistí pro určené typy DT smazání zpráv starších 90 dnů (od doručení přihlášením) z DS uživatele k určenému termínu po expiraci služby DT |
| **9** | Zrušení DT z rozhodnutí ČP | ČP zadává přes webovou službu požadavek na zrušení DT ke konkrétnímu ID DS | ISDS umožní ČP prostřednictvím specifického rozhraní (webové služby) zadávání požadavků na zrušení DT.  ISDS zajistí smazání zpráv starších 90 dnů (od doručení přihlášením) z DS uživatele k určenému termínu po zadání požadavku na zrušení DT. |
| **10** | Uložení zprávy |  | ISDS zajistí uložení datové zprávy (do DT) po dobu delší, než vyplývá ze ZEU, pokud má uživatel v ISDS aktivovánu službu DT a v rámci služby DT dostatečnou kapacitu. |
| **II** | **Uživatelské rozhraní** | | |
| **1** | Přístup k DT (portál, interface) |  | ISDS umožní uživatelům přístup k datovým zprávám uloženým v DT (náležejícím jejich DS) prostřednictvím Portálu ISDS a prostřednictvím veřejných webových služeb po úspěšném přihlášení do systému ISDS |
| **2** | Smazání zprávy |  | ISDS umožní smazání zprávy, která je umístěna v DT, uživateli s příslušnými oprávněními |
| **III** | **Notifikace** | | |
| **1** | Uživatelské nastavení notifikací | ČP stanoví podmínky pro notifikace služby DT a texty notifikačních systémových zpráv | ISDS umožní v nastavení datových schránek zapnout nebo vypnout určený typ notifikací pro události DT |
| **2** | Notifikace služby Datový trezor | ČP stanovuje podmínky pro notifikace služby DT a texty notifikačních systémových zpráv | Zajistí funkce notifikací dle specifikací v provozní příručce Funkční design |
| **IV** | **Informování uživatelů služby** | | |
| **1** | Informování uživatelů služby | ČP rozhodne o způsobu a detailech předávání informací uživatelům ISDS o možnostech a funkcionalitách služby DT.  ČP stanoví okruh subjektů, na které se bude informační akce vztahovat. | ISDS zajistí realizaci dle konkrétní informační akce |
| **V** | **Stanovení ceny pro koncové zákazníky** |  |  |
|  |  | Stanovení ceny pro koncové zákazníky je plně v kompetenci ČP. |  |

### Poštovní datová zpráva

|  |  |  |  |
| --- | --- | --- | --- |
| **Procesy** | | **Zajišťuje** | |
| **Objednatel (ČP)** | **Poskytovatel** |
| **I** | **Zajištění funkcí Poštovních datových zpráv (PDZ)** | | |
| **1** | Služba Poštovní datová zpráva |  | ISDS umožní dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob dle §18a ZEU - umožní na žádost fyzické osoby, podnikající fyzické osoby nebo právnické osoby dodávání dokumentů z datové schránky jiné fyzické osoby, podnikající fyzické osoby nebo právnické osoby do datové schránky této osoby. ISDS umožní ČP účtování a inkasování odměny dle §18a, odst. 3. |
| **2** | Funkce služeb Poštovních datových zpráv |  | Zajistí funkce ISDS pro nakládání s Poštovními datovými zprávami dle specifikací v provozní příručce Funkční design, část Poštovní datové zprávy a související. |
| **3** | Povolení příjmu PDZ |  | ISDS zajistí možnost nastavení povolení příjmu PDZ na základě pokynu uživatele, specifikací v provozní příručce Funkční design, část Poštovní datové zprávy. |
| **4** | Neveřejné webové služby ISDS pro Poštovní datové zprávy |  | Zajistí funkce webových služeb pro Poštovní datové zprávy dle specifikací v provozní příručce Funkční design, část Poštovní datové zprávy a související. |
| **5** | Veřejné webové služby ISDS pro Poštovní datové zprávy |  | Zajistí funkce webových služeb pro Poštovní datové zprávy dle specifikací v Provozním řádu, části WS\_ISDS\_Vyhledavani\_datovych\_schranek.pdf |
| **II** | **Uživatelské rozhraní** | | |
| **1** | Přístup k PDZ (portál, interface) |  | ISDS umožní přístup k PDZ prostřednictvím Portálu ISDS a prostřednictvím veřejných webových služeb po úspěšném přihlášení do systému ISDS |
| **2** | Odeslání a uložení PDZ |  | ISDS zajistí odeslání a uložení PDZ po dobu vyplývající ze zákona |
| **3** | Fakturace smluvních PDZ koncovým zákazníkům | ČP zajistí fakturaci smluvním zákazníkům | ISDS umožní ČP prostřednictvím webových služeb získávání dat pro vyúčtování smluvních PDZ koncovým zákazníkům. |
| **III** | **Informování uživatelů služby** | | |
| **1** | Informování uživatelů služby | ČP rozhodne o způsobu a detailech předávání informací uživatelům ISDS o možnostech a funkcionalitách služby PDZ.  ČP stanoví okruh subjektů, na které se bude informační akce vztahovat. | ISDS zajistí realizaci dle konkrétní informační akce |
| **IV** | **Stanovení ceny pro koncové zákazníky** |  |  |
|  |  | Stanovení ceny pro koncové zákazníky je plně v kompetenci ČP. |  |

### SMS notifikace

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Procesy** | | **Zajišťuje** | | |
| **Objednatel (ČP)** | **Poskytovatel** | |
| **I** | **Zajištění funkcí SMS notifikace** | | | |
| **1** | Služba SMS notifikací |  | ISDS umožní (dle §20, odst. 1 písmena d) ZEU) vyrozumění adresáta o dodání datové zprávy do jeho datové schránky prostřednictvím Premium SMS. | |
| **2** | Zajištění funkce Notifikačního serveru |  | Zajistí požadované funkce Notifikačního serveru pro předávání dat potřebných pro odesílání Premium SMS poskytovateli Premium SMS, dle specifikací v provozní příručce Funkční design, část Notifikační server v ISDS a související. | |
| **II** | **Uživatelské rozhraní** | | | |
| **1** | Nastavení notifikací na klientském portálu ISDS |  | ISDS zajistí pro uživatele ISDS možnost nastavení funkcionalit služby SMS notifikací na klientském portálu ISDS, dle uživatelské příručky portálové aplikace ISDS DATOVE\_SCHRANKY.docx, kapitola 10.6.2. | |
| **III** | **Stanovení ceny pro koncové zákazníky** |  | |  | |
|  |  | Stanovení ceny pro koncové zákazníky je plně v kompetenci ČP. | |  | |

### Kreditní systém datových schránek

|  |  |  |  |
| --- | --- | --- | --- |
| **Procesy** | | **Zajišťuje** | |
| **Objednatel (ČP)** | **Poskytovatel** |
| **I** | **Zajištění funkcí kreditního systému ISDS** | | |
| **1** | Služba kreditní systém |  | ISDS umožní služby kreditního systému:   * Dobíjení kreditu pro konkrétní datovou schránku * Vedení kreditů k datovým schránkám * Umožnění čerpání kreditu při aktivaci služby kreditní DT * Umožnění čerpání kreditu při odesílání PDZ hrazených kreditem * Notifikaci při nízkém stavu kreditu a při blížící se expiraci kreditu * Vedení podrobného a bezpečného logu o všech pohybech kreditů * Možnost stažení přehledů čerpání kreditu * Umožnit každému uživateli datové schránky vidět hodnotu kreditu a historii kreditních transakcí * ČP může kredit nabíjet/vybíjet prostřednictvím WS |
| **2** | Funkce kreditního systému |  | Zajistí funkce kreditního systému dle specifikací v provozní příručce Funkční design, část Kreditní systém a související. |
| **3** | Neveřejné webové služby ISDS pro kreditní systém |  | Zajistí funkce webových služeb pro kreditní systém dle specifikací v provozní příručce Funkční design, část Kreditní systém a související. |
| **4** | Veřejné webové služby ISDS pro kreditní systém |  | Zajistí funkce webových služeb pro kreditní systém dle specifikací v Provozním řádu, části WS\_ISDS\_Vyhledavani\_datovych\_schranek.pdf |
| **II** | **Uživatelské rozhraní** | | |
| **1** | Změny výše kreditu | ČP zajistí možnost nabití kreditu přes externí aplikaci napojenou na ISDS přes neveřejné webové služby | Systém ISDS na základě pokynu ČP upraví stav kreditu v DS.  ISDS umožní ČP prostřednictvím specifického rozhraní (webové služby) zadávání změn kreditu pro určené datové schránky, získávání informací o změnách kreditu a získávání potřebných dat pro vyúčtování kreditu.  Umožní uživatelům získávání informací o pohybech výše kreditu u vlastní datové schránky. |
| **2** | Notifikace kreditního systému |  | Zajistí funkce notifikací dle specifikací v provozní příručce Funkční design, kap. 8.3.5 – upozornění na nízký stav kreditu a na blížící se expiraci kreditu |
| **III** | **Informování uživatelů služby** | | |
| **1** | Informování uživatelů služby | ČP rozhodne o způsobu a detailech předávání informací uživatelům ISDS o možnostech a funkcionalitách služby kreditní systém.  ČP stanoví okruh subjektů, na které se bude informační akce vztahovat. | ISDS zajistí realizaci dle konkrétní informační akce |
| **IV** | **Stanovení ceny pro koncové zákazníky** |  |  |
|  |  | Stanovení ceny pro koncové zákazníky je plně v kompetenci ČP. |  |

### Nové budoucí funkcionality

Poskytovatel neobdrží od Objednatele k níže uvedeným funkcionalitám zdrojové kódy, ale je povinen je zprovoznit do 12-ti měsíců od zahájení Řádného a plného provozu ISDS za předpokladu, že k tomu Objednatel poskytne potřebnou součinnost. Realizace těchto funkcionalit je hrazena z ceny Služeb Rozvoje.

**Přesunutí evidence kreditů mimo perimetr ISDS, do výhradní správy ČP**

Poskytovatel je povinen na výzvu Objednatele realizovat úpravy funkcionality systému ISDS související s využíváním kreditu tak, že bude využívána evidence kreditů k datovým schránkám, umístěná v určeném systému Objednatele mimo perimetr ISDS, přičemž budou pro uživatele zachovány všechny funkcionality kreditního systému. Poskytoval je dále povinen poskytnout potřebnou součinnost při migraci dat kreditů do systému Objednatele.

### Migrace dat Aditivních služeb

|  |  |  |  |
| --- | --- | --- | --- |
| **Procesy** | | **Zajišťuje** | |
| **Objednatel (ČP)** | **Poskytovatel** |
| **1** | Jednorázová migrace dat Aditivních služeb |  | Poskytovatel zajistí k začátku poskytování plnění služeb zajištění provozu ISDS přenos veškerých dat, parametrů a funkcionalit, týkajících se Aditivních služeb, do nového systému ISDS, bez dopadu na konečné uživatele Aditivních služeb. |

## Funkční požadavky na provoz podpůrných služeb

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Činnosti** | **Zajišťuje** | |
| **Objednatel - ČP (Správce - MV)** | **Poskytovatel** |
| **I** | **OBSLUŽNÉ A SERVISNÍ ČINNOSTI** | | |
| **1** | **Testovací prostředí pro dodavatele aplikací a širokou veřejnost** | | |
|  | Provoz testovacího prostředí pro dodavatele aplikací - veřejné testovací prostředí | Správce schvaluje žádosti o přístup do testovacího prostředí | Zajistí, aby dodavatelům aplikací po schválení požadavku Správcem byl umožněn přístup do testovacího prostředí ISDS  ( <https://www.datoveschranky.info/o-datovych-schrankach/vyzkousejte-si-datovou-schranku>, <https://www.czebox.cz/> ) |
|  | Vytvoření a provoz interaktivního demo-prostředí pro širokou veřejnost | Zajistí umístění odkazu ke spuštění na www.datoveschranky.info | Zajistí provoz interaktivního demo-prostředí dostupného na internetové adrese určené Objednatelem s ukázkami funkcí ISDS pro širokou veřejnost |
| **2** | **Napojení Spisových služeb (interface, testovací prostředí, součinnost Poskytovatele)** | | |
|  | Napojení na spisové služby (interface, testovací prostředí, součinnost Poskytovatele) | Zajistí součinnost dotyčných subjektů | Bude zajištěn přístup prostřednictvím portálu a rovněž interface WS (webové služby) pro spisové služby (SS) a velkých PO.  Zajistí testovací prostředí pro testování napojení spisových služeb na interface WS |
| **3** | **Rozhraní pro přístup aplikací internetových provozovatelů do ISDS dle § 14a ZEU** | | |
|  | Rozhraní pro přístup aplikací internetových provozovatelů do DS |  | Zajistí podklady pro výpočet poplatků za využití přístupového rozhraní. |
|  | Podklady pro výpočet poplatků za využití přístupového rozhraní |  | Umožní Správci vést seznam poskytovatelů internetových služeb, kteří využívají přístupové rozhraní, a zveřejňovat je dálkovým způsobem. |
|  | Seznam poskytovatelů internetových služeb | Zajistí vedení veřejného seznamu poskytovatelů internetových služeb (dle §14a ZEU). | Umožní Správci vést seznam poskytovatelů internetových služeb, kteří využívají přístupové rozhraní, a zveřejňovat je dálkovým způsobem. |
| **4** | **Design rozhraní ISDS** | | |
|  |  |  |  |
|  | Formát přístupových údajů |  | Zajistí generování nových přístupových údajů (přístupové heslo pro první přihlášení do systému resp. přístupové heslo při opakování vydávání přístupových údajů) ve tvaru, který nebude obsahovat speciální znaky, jež se vyskytují mimo rozložení „české“ klávesnice |
|  | Formát a tvar CAPTCHA |  | Pro přihlašování na portálu ISDS jménem a heslem zajistí použití formátu a tvaru CAPTCHA, který bude nejméně limitující pro slabozraké |
| **5** | **Servisní modul** | | |
|  | Možnosti ukládání dat |  | Zajistí možnost ukládání dat (provozních statistik systému ISDS) ve formátu CVS a XLS. |
|  | Možnosti exportu tabulek |  | Zajistí možnost exportu dat (provozních statistik systému ISDS) ve formátu CVS a XLS |
|  | Poskytování informace o datu zpřístupnění a znepřístupnění DS |  | Zajistí v servisním modulu možnost zobrazení informace o datu zpřístupnění a znepřístupnění datové schránky |
|  | Poskytování informace o okamžiku znepřístupnění datové schránky |  | Zajistí v servisním modulu možnost zobrazení v seznamu žádostí záznamu s datem znepřístupnění datové schránky na žádost |
|  | Poskytování informace o znepřístupněných a zrušených DS |  | Zajistí poskytování informace o znepřístupněných a zrušených datových schránkách v seznamu žádostí Správci ve stejném rozsahu jako informace o aktivních datových schránkách |
|  |  |  |  |
|  | Generování výpisů o dodaných a odeslaných DZ |  | Zajistí dodatkovou funkci poskytování výpisů z DS o dodaných či odeslaných zprávách za určité období (výpis z logu – základní údaje o zprávě). |
|  | Poskytování informací o datových zprávách uživatelům SM (Servisní modul) |  | Zajistí uživatelům servisního modulu možnost zjistit podrobné informace o konkrétní datové zprávě (např. adresát, odesilatel, čas dodání, doručení, stav zprávy apod.) |
|  | Zobrazení informací o počtech zásilek v SM a reportech |  | Zajistí v Servisním modulu možnost generování reportů o zásilkách předávaných systému hybridní pošty a stavech jejich doručení. |
|  | Zobrazení informací ve „Stavu žádosti“ |  | Zajistí v servisním modulu možnost zobrazení informací ve „Stavu žádosti“, včetně jména a příjmení osoby a data, kdy byla operace provedena, včetně textového popisu. |
|  | Report interních uživatelů |  | Zajistí uživatelům servisního modulu s nejvyššími právy možnost generovat report interních uživatelů včetně rolí |
|  | Zpřístupnění informací o odesílajících osobách osobách způsobujících doručení DZ |  | Dle § 14, odst. 3, písm. d) ZEU umožnit získávat seznamy DZ určité DS pro interní uživatele ISDS. V tabulkách uvnitř ISDS bude uváděna i osoba, která odeslala a osoba, která způsobila doručení. |
| **6** | **Portál Poskytovatelů dat** | | |
|  | Možnosti |  | Zajistí funkčnost formulářů pro správu schránek pro ty poskytovatele dat, kteří nevyužívají rozhraní webových služeb. |
| **7** | **Výstupy forenzní funkcionality** | | |
|  | Forenzní vyhledávání |  | Zajistí funkčnost vyhledávání a výpis událostí bezpečného logu k dané datové schránce |
|  | Výstupy forenzní funkcionality |  | Zajistí, aby auditní výpis událostí datové schránky ze servisního modulu, který je předáván na základě speciálních právních předpisů mimo ISDS ve formátu XLS, neuváděl uživatelské identifikátory jiných uživatelů, než z auditované datové schránky. |
|  | Forenzní šetření | Spolupracuje s Poskytovatelem na definici procesu | Výstupem je proces přístupů pověřených osob MV k podkladovým informacím ISDS pro potřeby realizace forenzního šetření |
| **8** | **Call centrum (CC) – Informační linka a Service Desk (SD)** | | |
|  | Přijetí požadavku CallCentrem | Je vlastníkem kontaktní informační linky. Je provozovatelem CC. Řeší příjem všech požadavků/incidentů od uživatelů DS (datových schránek) | Zajistí poskytování služeb II. úrovně podpory pro CC Objednatele v souladu s definovanými SLA |
|  | Přijetí požadavku Service Deskem SD |  | Zajistí poskytování služeb SD Poskytovatele pro Objednatele v souladu s definovanými SLA |
|  | Proces reklamace v SD |  | V aplikaci TTS pro potřeby evidence incidentů zajistí vedení kategorie „R“, která je určena pro incidenty koncových uživatelů. Zajistí zpracování ticketů v rámci jednotlivých skupin řešitelů, možnost dohledu Incident Managera nad incidenty přes všechny řešitelské skupiny Správce, Objednatele a Poskytovatele. |
|  | Události v SD |  | Umožní určeným pracovníkům Objednatele náhled nad incidenty přes všechny řešitelské skupiny Správce, Objednatele a Poskytovatele. |
| **9** | **Interní správa a auditování systému** | | |
|  | Interní správa, monitoring, auditování systému |  | Zajistí dohled, monitoring a správu systému ISDS včetně bezpečnostní správy, kontrolu monitorovacích zpráv |
|  | Rozšířený monitoring poskytovaných služeb |  | Zajistí možnost vykazování následujících parametrů:   * Počet dodaných datových zpráv za měřené období dodaných do 1 minuty od podání * Počet datových zpráv za měřené období nedodaných do 1 minuty od podání * Celkový počet podaných datových zpráv * Počet dodaných datových zpráv do 60 minut od podání * Počet datových zpráv nedodaných do 60 minut od podání * Počet zřízených DS * Počet přijatých požadavků k vytvoření DS * Počet zrušených DS za měřené období * Počet zrušených DS ve stanovené lhůtě za měřené období * Seznam jednotlivých případů zrušení DS, u kterých nebyla splněna garantovaná doba vyřízení, s uvedením skutečného času zrušení DS * Počet znepřístupněných DS za měřené období * Počet DS znepřístupněných včas za měřené období * Počet přijatých požadavků na znepřístupnění DS za měřené období * Počet zneplatněných přístupových údajů za měřené období * Počet zneplatněných přístupových údajů ve lhůtě do 60 minut, za měřené období * Počet přijatých požadavků na zneplatněných přístupových údajů za měřené období * Počet přijatých požadavků na vytvoření přístupových údajů * Počet přístupových údajů vytvořených včas za měřené období * Počet stažených datových zpráv za měřené období * Počet datových zpráv za měřené období, připravených včas ke stažení * Počet stažených dodejek a doručenek za měřené období * Počet dodejek a doručenek za měřené období, připravených včas ke stažení * Počet požadavků na Call centrum přijatých v časovém limitu |
| **10** | **Definování provozních parametrů (identifikátor, formáty, příst. údaje atd.)** | | |
|  | Definice provozních parametrů | Schvaluje a vydává vyhlášku | Vypracovává a předkládá návrhy příslušných parametrů (případně jejich struktury) pro vyhlášku |
| **11** | **Bezpečnostní monitoring** | | |
|  | Bezpečnostní monitoring |  | Prostřednictvím specializovaného nástroje zaznamenává činnosti systému ISDS, jeho uživatelů a administrátorů v souladu s požadavky vyhlášky 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti |
| **12** | **Bezpečnostní audit** | | |
|  | Bezpečnostní audit | Iniciace  Kontroluje své pracovníky a postupy i pracovníky a postupy subdodavatele | Připravuje podklady a zajišťuje bezpečnostní audit |
| **13** | **Kontrola dodržování zákona č. 101/2000 Sb.** | | |
|  | Kontrola dle zákona č. 101/2000 Sb., | Kontroluje své pracovníky a postupy | Kontroluje své pracovníky a postupy i pracovníky a postupy subdodavatelů a nastavuje technická a organizační opatření v souladu s požadavky zákona 101/2000Sb. |

## Podpora dodavatelů aplikací třetích stran

|  |  |
| --- | --- |
| Určení služby: | Zajištění podpory Poskytovatelem komunitě vývojářů - dodavatelů aplikací třetích stran - využívajících aplikační rozhraní ISDS. Podpora bude poskytována formou diskuzního fóra v rámci webové aplikace určené Objednatelem. |
| Parametry služby: | Reakční doba 1 pracovní den |
| Reporting: |  |
| Režim služby: | 9x5 |

## Zajištění bezpečného provozu a dostupnosti ISDS

Základním cílem zajištění provozu a dostupnosti ISDS je zajištění provozu ISDS a s tím související poskytnutí funkčností tohoto systému oprávněným uživatelům v rozsahu pokrývajícím zákonné požadavky viz. bod 3. Přílohy č. 1 Smlouvy.

|  |  |
| --- | --- |
| Určení služby: | Služba je určena pro zajištění bezpečného, bezporuchového a bezvýpadkového provozu a dostupnosti systému ISDS za předpokladu definované součinnosti v souladu s definovanými SLA uvedenými v Příloze č. 6. |
| Parametry služby: | Služby provozu ISDS jsou poskytovány na serverech a dalších technických prostředcích výhradně určených pro provoz ISDS a mají garantovanou dostupnost nepřetržitě v režimu 24×7.   * Maximální velikost datové zprávy dodávané do datové schránky je definována Dotčenými právními předpisy. * Lhůta uchovávání datových zpráv, u nichž bylo doručení vykonáno přihlášením adresáta dle příslušných ustanovení vyhlášky č. 194/ 2009 Sb. do jeho datové schránky, je 90 dní ode dne přihlášení. * Lhůta uchovávání datových zpráv, které byly dodány do datové schránky, ale nedošlo k přístupu do datové schránky, tj. nedošlo k doručení jedním ze způsobů přístupu do datové schránky, je 3 roky ode dne, kdy byla datová zpráva dodána. V systémovém logu budou o těchto událostech uchovávány veškeré záznamy po dobu o tři roky delší než maximální dobu požadovanou právními předpisy. |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti systému. |
| Režim služby: | 24x7 |

## Provozní požadavky na provoz podpůrných, obslužných a servisních služeb

### Bezpečnostní monitoring

|  |  |
| --- | --- |
| Určení služby: | Monitoring účinnosti bezpečnostních opatření. |
| Parametry služby: | Služba je poskytována prostřednictvím specializovaného nástroje pro zaznamenávání činností ISDS, jeho uživatelů a administrátorů.  zajistí především:   * 1. sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a   2. ochranu získaných informací před neoprávněným čtením nebo změnou.   Pomocí nástroje jsou zaznamenávány následující činnosti   1. přihlášení a odhlášení uživatelů a administrátorů, 2. činnosti provedené administrátory, 3. činnosti vedoucí ke změně přístupových oprávnění, 4. neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů, 5. zahájení a ukončení činností technických aktiv ISDS, 6. automatická varovná nebo chybová hlášení technických aktiv, 7. přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.   Součástí nástroje je i specifikace, ve kterých kontrolních bodech bude monitoring a bezpečnostní dohled prováděn, jaké indikátory (alerty) dohledu budou použity a jaké metriky budou vykazovány.  Z důvodu interoperability s Dohledovým centrem eGovernmentu MV bude součástí nástroje specifikace, jak organizačně a procesně bude spolupráce s dotčenými stranami realizována.  Záznamy činností jsou uchovávány nejméně po dobu 3 měsíců. |
| Reporting: | Součástí služby je i pravidelný měsíční report |
| Režim služby: | 24x7 |

#### Další požadavky Objednatele na zajištění bezpečnostního monitoringu:

Umožnit pracovníkům Objednatele na technologické infrastruktuře Poskytovatele prostřednictvím konzolí systému sledování bezpečnostních událostí a incidentů a stavy jejich řešení. Poskytovatel zajistí školení pro pracovníky Objednatele.

### Service Desk - služby

|  |  |
| --- | --- |
| Určení služby: | Předmětem poskytované služby je poskytnutí jednotného kontaktního místa (SpoC – Single Point of Contact) pro Správce, Objednatele a Poskytovatele podle definovaných rolí a oprávnění k přístupu. |
| Parametry služby: | Služba je poskytována komunikačními kanály. (řazení není podle priority využívaného kanálu):   * Telefon   + standardní telefonní kontakt na Service Desk Poskytovatele   + eskalační telefonní číslo na manažera Service Desku   + záložní telefonní kontakt na Service Desk Poskytovatele (nezávislý na přenosových trasách standardního telefonického kontaktu). * Elektronická pošta * Trouble Ticket Systém (TTS) - aplikace pro evidenci, správu a řešení incidentů/požadavků, Slouží pro předávání požadavků/incidentů od Objednatele k Poskytovateli a zpětnou reakci Poskytovatele na řešení, průběh a vyřešení případu. Na základě dohodnutých technických parametrů. |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých servisních požadavků dle jejich typu a služeb, kterých se požadavky týkají a stavu, v jakých se řešení požadavků/incidentů nachází |
| Režim služby: | 24x7 |

#### Další požadavky Objednatele na zajištění provozního monitoringu:

Umožnit pracovníkům Objednatele sledování stavu všech parametrů souvisejících s plněním SLA na technologické infrastruktuře Poskytovatele prostřednictvím monitorovacích stanic, umístěných v lokalitách určených Objednatelem, jejichž nastavení provádí dle požadavků Objednatele Poskytovatel. Bude prováděno:

* pravidelné nezávislé sledování dostupnosti a výkonu IT infrastruktur prostřednictvím nástroje, který zvolí a implementuje Poskytovatel Služeb.
* pravidelná analýza specifických reportů nad daty ukládanými monitorovacím nástrojem do databáze.
* sledování záznamů, klasifikace a řešení všech incidentů zaznamenaných do TTS, který zvolí a implementuje Poskytovatel Služeb.
* pravidelná analýza specifických reportů nad daty v databázi Service Desku.

Poskytovatel:

* zajistí odpovídající prostředí pro nezávislý monitoring
* připraví manuál
* zajistí školení pro pracovníky Objednatele v rozsahu, který je nutný k porozumění monitorovacího nástroje, sledovaných parametrů a procesů řešení.

#### II. úroveň podpory pro CC Objednatele

|  |  |
| --- | --- |
| Určení služby: | Zajištění technické podpory formou II. úrovně podpory v případech technických požadavků/incidentů. Poskytovatel bude od Objednatele přijímat veškeré technické požadavky/incidenty, samostatně je řešit a informovat Objednatele o způsobu nebo stavu řešení. Rozsah níže je uveden orientačně a může být rozšířen   * + nastavení prohlížeče u uživatele   + problematika přístupových údajů   + nastavení zabezpečení na straně uživatele – proxy, firewall, antivir,   + propojení ISDS pomocí WS se systémy třetích stran (nejčastěji spisových služeb, … )   + problematika formátů dat, příloh, ZFO… spolupracujících s ISDS   + podpora uživatelů Servisního modulu DS   + zajištění reportingu statistik ticketů uživatelů |
| Parametry služby: | * webový formulář – slouží uživateli DS pro zadání dotazu/požadavku/incidentu. Poskytovateli bude přesměrována ta část problematiky, která se bude týkat technických oblastí. Agenda bude vedena v TTS nástroji Poskytovatele tak, aby byly případy dostupné pro náhled určených pracovišť Objednatele – viz podmínky v bodě 4.6.2.1 * Poskytovatel bude počítat s nutností přizpůsobit komunikaci vlastního řešení TTS tak, aby bylo možno požadavky/incidenty prokazatelně a vzájemně předávat s tím, že veškeré životní cykly požadavků/incidentů budou on-line transparentní. Například propojením TTS nástrojů nebo přímým, bezpečnostně garantovaným vstupem, do TTS nástroje Objednatele |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých požadavků dle jejich typu a služeb, kterých se požadavky týkají a stavu, v jakých se řešení požadavků/incidentů nachází |
| Režim služby: | Webový kontakt 24x7, telefonní kontakt 12x5 |

#### Řešení provozních incidentů

|  |  |
| --- | --- |
| Určení služby: | Předmětem poskytované služby je řešení incidentů v provozním prostředí IS s garantovanou reakční dobou na straně Poskytovatele. Incident je událost, která není součástí standardního provozu IS a která způsobuje či může způsobovat přerušení nebo omezení kvality dané služby ISDS. |
| Parametry služby: | Kategorizace incidentů podle dopadu a naléhavosti Agenda bude vedena v TTS nástroji Poskytovatele tak, aby byly případy dostupné pro náhled určených pracovišť Objednatele – viz podmínky v bodě 4.6.2.1 |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých incidentů dle jejich kategorie.  Součástí reportu je přehled počtu nahlášených incidentů za měsíc, počet vyřešených incidentů v daném měsíci a celkový přehled otevřených incidentů na konci měsíce. |
| Režim služby: | 24x7 |

#### Řešení provozních problémů

|  |  |
| --- | --- |
| Určení služby: | Předmětem služby je řešení a správa problémů v provozním prostředí IS. Správa problémů (Problem management) se snaží nalézt neznámou hlavní příčinu incidentů a následně tuto příčinu odstranit. |
| Parametry služby: | Určení priority problému na základě dopadu, naléhavosti a existence náhradního řešení. Agenda bude vedena v TTS nástroji Poskytovatele tak, aby byly případy dostupné pro náhled určených pracovišť Objednatele – viz podmínky v bodě 4.6.2.1 |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující počty jednotlivých problémů dle jejich klasifikace.  Součástí reportu je přehled počtu nahlášených problémů za měsíc, počet vyřešených problémů v daném měsíci a celkový přehled otevřených problémů na konci měsíce. |
| Režim služby: | 9x5 |

## Požadavky na infrastrukturu

Definice prostředí, ve kterém probíhá provozovávání ISDS:

**Produkční prostředí**

**Neprodukční prostředí ISDS**

Kromě produkčního prostředí ISDS (PROD) existují další prostředí neprodukční, nazvaná:

* Prostředí vývojové a interní testovací (DEV)
* Prostředí veřejné testovací (VT)
* Prostředí předprodukční (PRED)

Datové zprávy zaslané v neprodukčním prostředí nejsou platné datové zprávy. Tyto zprávy nelze zaměnit ani ověřit na Produkčním prostředí. Neprodukční prostředí mohou být výrazně jednodušší v infrastruktuře, nejsou napojena na produkční externí systémy (pokud externí systémy mají testovací verze, mohou být napojena na ně – ISZR, Czech POINT). K dalším odlišnostem patří:

* Nekomunikuje se s PostServisem, nevytvářejí se dopisy s přístupovými údaji;
* Odlišné napojení na TSA;
* Při vytvoření uživatele se přístupové údaje vrací do WS nebo do Portálu;
* Při vytváření schránek jsou nastaveny některé vlastnosti (např. posílání PDZ) defaultně;
* Při vytváření DS lze zadat duplicitní IČ – vygeneruje se náhradní;
* Lze si libovolně na Portálu „nabíjet“ kredit;
* Lze si zaregistrovat k přihlašování Testovací certifikát certifikační autority PostSignum;
* Neprobíhá indexování safelogů (na DEV ano, ale jen omezeně a ne zabezpečeně).

### Vývojové a interní testovací prostředí

|  |  |
| --- | --- |
| Určení služby: | Předmětem služby je:   * poskytnutí a instalace HW, * poskytnutí a instalace základního a generického SW (produkty třetích stran), * implementace zdrojových kódů Licencovaného software, vytvoření vývojového a interního testovacího prostředí pro účely Služeb Rozvoje, které zahrnuje vytvoření prostředí vhodného pro:  1. editaci a řízení změn zdrojového kódu včetně systému verzování zdrojového kódu ve vhodném SW nástroji s komentářem kódu po dobu platnosti Smlouvy. Objednatel si může při každém novém Releasu – nasazení změn – vyžádat kontrolu změn, 2. sestavení binárního kódu, 3. testování binárních aplikací.  * administrace a správa prostředí, * vedení historie Releasů.   Slouží pro zajištění úprav a rozvoje Licencovaného software, programátorského testování a vytvoření binárních kódů určených pro předání do veřejného testovacího, předprodukčního a produkčního prostředí ISDS.  Vývojové a interní testovací prostředí je provozováno v datovém centru určeném Objednatelem.  Předmětem služby je dále   * příprava bezpečného rozhraní pro konektivitu vývojového prostředí do sítě internet.   Zajištění konektivity do Internetu není předmětem služby |
| Parametry služby: | Dostupnost technologické infrastruktury ve vybrané lokalitě Objednatele – není stanovena |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti infrastruktury  Informace o provedených změnách Licencovaného software  Vydané verze Licencovaného software včetně testovacích protokolů |
| Režim služby: | 24x7 |
| Připojení do Internetu | viz. Příloha č. 12 Smlouvy |

Poskytovatel umožní Objednateli přístup ke kompletní historii Releasů.

### Veřejné testovací prostředí

|  |  |
| --- | --- |
| Určení služby: | Předmětem služby je provozování:   * technologické infrastruktury HW dodané Poskytovatelem, * základního a generického SW (produkty třetích stran) dodaného Poskytovatelem, * aplikačního SW, * vedení historie Releasů a Patchů.   Slouží pro ověření nové verze aplikace a k ověření integrace (s dalšími testovacími systémy) apod. Na tomto testovacím prostředí mohou být prováděny testy funkční, výkonnostní, bezpečnostní a integrační.  Veřejné testovací prostředí je umístěno v jednom datovém centru a je dostupné na webové adrese [www.czebox.cz](http://www.czebox.cz). |
| Parametry služby: | Dostupnost technologické infrastruktury – 97% - v souladu s definovanými SLA uvedenými v Příloze č. 6. |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti infrastruktury. |
| Režim služby: | 24x7 |
| Připojení do Internetu | Konektivita ISDS do sítě internet s dostatečnou kapacitou |

### Předprodukční prostředí

|  |  |
| --- | --- |
| Určení služby: | Předmětem služby je provozování:   * technologické infrastruktury HW dodané Poskytovatelem, * základního a generického SW (produkty třetích stran) dodaného Poskytovatelem, * aplikačního SW * vedení historie Releasů a Patchů   Předprodukční prostředí je provozováno v jednom datovém centru a není vyžadována stejně výkonná technická infrastruktura jako u prostředí produkčního.  Předprodukční prostředí slouží pro ověření nových verzí aplikace, splňuje všechny funkční i nefunkční požadavky tj. využití povinných služeb, bezpečnost atd. Jedná se o prostředí se stejnou HW a SW architekturou, funkčně i bezpečnostně identické s prostředím produkčním. Případné konkrétní odlišnosti od produkčního prostředí musí být definovány nejpozději před zahájením nasazení prostředí. Na prostředí je nasazena verze určená ke schválení a následnému nasazení na produkční prostředí. Předprodukční prostředí pracuje s testovacími daty.  Předmětem služby je dále   * konektivita ISDS do sítě internet s dostatečnou kapacitou. * napojení na externí systémy, které disponují testovacím prostředím. |
| Parametry služby: | * Dostupnost technologické infrastruktury – není stanovena |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti infrastruktury. |
| Režim služby: | 24x7 |
| Připojení do Internetu | Objednatel doporučuje realizovat linkou o kapacitě nejméně 1 Gbps |

Poskytovatel umožní Objednateli přístup ke kompletní historii Releasů a Patchů.

Poskytovatel stanoví komponenty vypovídající o dostupnosti služby a umožní Objednateli jejich napojení na dohledové centrum Objednatele, provozní a bezpečnostní dohled.

### Produkční prostředí

Provoz ISDS (nevztahuje se na neprodukční prostředí) bude zajištěn ve dvou nezávislých geografických clusterech (v režimu ACTIVE-ACTIVE), které budou umístěny ve dvou datových centrech s klasifikací TIER III, splňujících požadavky stanovené v  části „Požadavky na datová centra“. Fyzické prostředí pro umístění produkčních systémů musí splňovat požadavky ZKB.

|  |  |
| --- | --- |
| Určení služby: | Předmětem služby je provozování:   * technologické infrastruktury HW dodané Poskytovatelem, * základního a generického SW (produkty třetích stran), * aplikačního SW.   pro zajištění bezpečného provozu systému ISDS ve dvou nezávislých geografických clusterech (v režimu ACTIVE-ACTIVE), které budou umístěny ve dvou datových centrech Poskytovatele splňujících požadavky  na TIER III.  Toto prostředí slouží pro provoz aplikace, splňuje všechny funkční i nefunkční požadavky, tj. výkon, dostupnost, využití povinných služeb, bezpečnost atd. Na prostředí je nasazena poslední schválená otestovaná stabilní verze. Prostředí pracuje s platnými daty.  Předmětem služby je dále   * konektivita ISDS do sítě internet s dostatečnou kapacitou, Poskytovatel přitom zajistí, aby nemohlo dojít k prostupu mezi CMS a internetovou přípojkou. * příprava rozhraní (portů 1 Gbps) pro připojení do sítě Centrálního místa služeb (CMS) * služby ISDS budou plnohodnotně dostupné protokolem IPv4 i IPv6 * propojení do CMS protokolem IPv4. |
| Parametry služby: | * Dostupnost technologické infrastruktury v primární lokalitě – 99,9 % * Dostupnost technologické infrastruktury v sekundární lokalitě – 99,9 % |
| Reporting: | Součástí služby je i pravidelný měsíční report zahrnující informace o dostupnosti infrastruktury a o míře využití přípojek systému ISDS do sítě CMS prostřednictvím monitoringu portů |
| Režim služby: | 24x7 |
| Připojení do CMS | Objednatel doporučuje realizovat linkou o kapacitě nejméně 1 Gbps |
| Připojení do Internetu | Objednatel doporučuje realizovat linkou o kapacitě nejméně 10 Gbps |

## Obecné požadavky na technickou infrastrukturu

Objednatel nepřipouští možnost využití cloudového řešení či použití datových center mimo území ČR.

## Požadavky na zajištění klíčového hospodářství

Objednatel požaduje, aby Poskytovatel zajistil řádné provádění klíčového hospodářství a technickými a organizačními prostředky zajistil ochranu všech šifrovacích klíčů a případného dalšího kryptografického materiálu použitého pro ochranu Datových zpráv spravovaných v ISDS a při šifrování komunikací. Objednatel pro bezpečné zajištění klíčového hospodářství doporučuje zvážit použití HW řešení.

## Platnost datových zpráv, dodejek a doručenek

Poskytovatel je povinen zajistit, že způsob zajišťování dlouhodobé platnosti a prověřování autenticity datových zpráv a způsob podepisování dodejek a doručenek v ISDS bude v souladu s aktuálně platnými prováděcími rozhodnutími Evropské komise, kterými se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru a návaznými aktuálně platnými technickými normami ETSI.

## Výkonnostní požadavky

Minimální počet odeslaných datových zpráv za 1 minutu: 2 000, garantované hodnoty jsou uvedeny v Příloze č. 6 Smlouvy

Minimální počet úspěšných přístupů do ISDS za 1 minutu: 25 000, garantované hodnoty jsou uvedeny v Příloze č. 6 Smlouvy

Minimální počet stahování datových zpráv za 1 minutu: 4 000

# Požadavky na datová centra (DC)

|  |  |
| --- | --- |
| **Požadavek** | **Požadovaná hodnota** |
| **Požadavek na budovu** |  |
| Odolnost dveří DC proti ohni | Minimálně 45min |
| Šířka vstupních dveří do prostoru DC | Minimálně 1m šíře do technologické místnosti a prostor NDC |
| Prostor DC místnost nemá okna | Ano |
| Prostor DC je fyzicky oddělen od ostatních prostor DC | Ano |
| Vstup do prostoru DC je monitorován | Ano |
| Příruční a přijímací místnost pro DC (fyzicky oddělená) | Ano |
| Nosnost podlahy v prostoru DC | min. 12 kN/m2 |
|  |  |
| **Zabezpečení a kamerový monitoring** |  |
| Všechny vstupy do budovy jsou evidovány | Ano |
| DC je přístupný pouze na přístupovou kartu a evidován | Ano |
| Místnosti s UPS, telekomunikačním propojením jsou přístupné pouze na přístupovou kartu a evidovány | Ano |
| Příruční a místnost je přístupná pouze na přístupovou kartu a evidován | Ano |
| Do prostoru NDC vede monitorovaná přístupová cesta | Ano |
| Okolí budovy a parkoviště je kamerově monitorováno | Ano |
| Záložní zdroje elektřiny (UPS + diesel agregáty) jsou kamerově monitorovány | Ano |
| Prostory DC jsou kamerově monitorovány | Ano |
|  |  |
| **Rozvody elektřiny** |  |
| Počet vstupních napájecích cest budovy | 1 aktivní + 1 pasivní |
| Počet fází pro RACK | min. 2 |
| Automatické přepnutí elektrické energie na záložní zdroje napájení při výpadku elektřiny | Ano |
| Rozvodná sít má bypass funkcionalitu pro bezvýpadkový servis jednotlivých prvků záložních zdrojů | Ano |
| PDU v RACK pro každou fázi | Ano |
| Infrastruktura DC je kompletně uzemněna | Ano |
| Vnitřní/vnější ochrana proti blesku | Ano |
|  |  |
| **Záloha napájení** |  |
| Celková zásoba paliva pro záložní zdroj napájení (při plném zatížení) | 12 h |
|  |  |
| **Chlazení** |  |
| Redundance chladících jednotek | Minimálně jedna redundantní chladící jednotka pro prostory NDC |
|  |  |
| **Detekční a protipožární systémy** |  |
| Kouřové senzory | Ano |
| Senzory úniku vody | Ano |
| Nevodivý zhášecí systém | Ano |
|  |  |
| **Kabelové rozvody** |  |
| Minimální kapacita přenosu po měděných kabelech | 1000 Mbit/s |
| Minimální kapacita přenosu po optických kabelech | 10000 Mbit/s |
|  |  |
| **Provozní podmínky** |  |
| Regulovaná teplota () | 20℃ +-6℃ |
| Regulovaná relativní vlhkost () | 30-70% |
| Systém detekce požáru | ano |
| Automatický hasicí systém | ano |

Umístění datových center:

Hostingové centrum Nagano

K Červenému dvoru 25/3156

130 00 Praha 3 - Strašnice

a

*Hostingové centrum Chodov*

*V lomech 2339/1*

*149 00 Praha 4 - Chodov*

# Požadavky na počáteční Migraci

## Rámcový přehled dat pro migraci:

Podrobnější vymezení migrovaných dat vyplývá z funkčního designu v Dokumentaci, která bude Poskytovateli předána.

**APLIKAČNÍ DATA**

* + **STATICKÉ DATOVÉ SOUBORY TYPU ČÍSELNÍKŮ PSČ APOD**
  + **LOGY TRVALÉHO CHARAKTERU**
  + **DOČASNÉ PROVOZNÍ SOUBORY**

**DATABÁZOVÁ DATA**

* + **DATA O ŽIVÝCH DATOVÝCH ZPRÁVÁCH (VČETNĚ TREZOROVÝCH ZPRÁV)**
  + **DATA O ARCHIVNÍCH DATOVÝCH ZPRÁVÁCH**
  + **DATA O DATOVÝCH SCHRÁNKÁCH A OSOBÁCH S PŘÍSTUPEM DO SCHRÁNEK**
  + **DATA O HISTORII OPERACÍ V ISDS**
  + **DATA KE KOMERČNÍ ČINNOSTI PROVOZOVATELE**
  + **PROVOZNÍ DATA**
  + **DATA POPISUJÍCÍ UŽIVATELSKÉ PREFERENCE**
  + **PROVOZNÍ DATA PRO KOMUNIKACI S UŽIVATELI**

**ADRESÁŘOVÁ DATA**

* + **ÚDAJE O DATOVÝCH SCHRÁNKÁCH A UŽIVATELÍCH**
  + **DATA PRO AUTENTIZACI UŽIVATELŮ**
  + **UŽIVATELSKÉ KONFIGURACE**

**SOUBOROVÁ DATA**

* + **PŘÍLOHY ŽIVÝCH DATOVÝCH ZPRÁV**
  + **DENNĚ GENEROVANÉ SEZNAMY SCHRÁNEK**
  + **PŘÍLOHY ROZPRACOVANÝCH DATOVÝCH ZPRÁV A NAČTENÉ DATOVÉ ZPRÁVY**
  + **SOUBORY ULOŽENÉ UŽIVATELI V SYSTÉMU**
  + **AKTUÁLNÍ VÝSTUPY FORENZNÍHO VYHLEDÁVÁNÍ**

**LOGOVACÍ DATA**

* + **LOGY VYŽADOVANÉ ZE ZÁKONA OBSAHUJÍCÍ OSOBNÍ ÚDAJE**.

## Požadavky Objednatele

Objednatel vyžaduje následující postup při přípravě a provádění Migrace ISDS do nového prostředí:

1. Poskytovatel zpracuje analýzu postupu provedení Migrace na základě Dokumentace předané dle Přílohy č. 9.
2. Poskytovatel zpracuje plán provedení a ověření Migrace a předloží ho Objednateli k vyjádření. V plánu Migrace budou uvedeny všechny potřebné náležitosti pro provedení Migrace včetně procedur pro ověření úspěšnosti Migrace a požadovaných součinností od Objednatele. Plán Migrace musí obsahovat kontrolní termíny, které umožní kontrolovat průběh plnění.
3. Objednatel se vyjádří k plánu Migrace.
4. Poskytovatel provede případné úpravy v plánu Migrace.
5. Poskytovatel provede zkušební Migraci podle předloženého plánu Migrace.
6. Poskytovatel provede za účasti zástupců Objednatele ověření úspěšnosti provedení zkušební Migrace.
7. Poskytovatel zpracuje přesný časový plán Migrace a předloží ho Objednateli k vyjádření.
8. Poskytovatel provede Migraci a za účasti zástupců Objednatele provede kontroly úplnosti a správnosti provedené Migrace.

Objednatel požaduje:

1. Migrace údajů nesmí ohrozit bezpečnost stávajícího provozu ISDS.
2. Musí být zachována důvěrnost dat uživatelů.
3. V průběhu Migrace bude zajištěna bezpečnost všech výše uvedených typů dat a bude dodrženo zejména ustanovení §14 odst. 6 ZEU.
4. Při Migraci bezpečného logu (safelogu) bude zachována soudní průkaznost a nepopiratelnost informací, které budou z tohoto logu po provedení Migrace poskytovány orgánům činným v trestním řízení.
5. Migrace identit uživatelů datových schránek bude provedena tak, že nebude nutno většině uživatelů rozesílat nové přístupové údaje.

## Rozsah poskytnuté součinnosti Objednatele

Exporty dat v požadovaném formátu a struktuře, pokud to umožní stávající technologie, bezpečnostní požadavky a nedojde k ohrožení či výraznému omezení provozu ISDS.

Objednatel nezaručuje poskytnutí součinnosti k vybudování ISDS nebo jeho částí Poskytovatelem s použitím tvorby image serverů a jiných komponent systému provozovaného stávajícím poskytovatelem služeb provozu ISDS.

Objednatel nepřipouští jakýkoli souběh více systémů ISDS po Dni zahájení provozu ISDS.

# Požadavky na rozhraní vůči uživateli

Poskytovatel je povinen zajistit, aby při uvedení ISDS do Řádného a plného provozu byly vzhled a funkčnost rozhraní vůči uživatelům ISDS shodné se stávajícím rozhraním.

# Požadavky na testování ISDS před uvedením do provozu

## Audit návrhové dokumentace a plánu Migrace

Poskytovatel umožní Objednateli, resp. Objednatelem určené třetí osobě, provést předběžný audit v následujícím rozsahu.

Ověření, že návrhová dokumentace ISDS obsahuje návrhy všech technických a organizačních opatření vyžadovaných ZKB a vyhláškou o kybernetické bezpečnosti stanovené pro prvky kritické informační infrastruktury.

Ověření, že technická a organizační opatření/řešení popsaná v návrhové dokumentaci ISDS mohou zajistit efektivní ochranu datových zpráv a celého ISDS (tzv. proof of design).

Ověření, že plán Migrace ISDS obsahuje postupy a opatření, které zajistí ochranu migrovaných dat.

### Kritéria auditu pro akceptaci návrhové dokumentace a plánu Migrace

Jako kritérium pro akceptaci návrhové dokumentace a plánu Migrace ISDS bude použita míra rizik, kterým by byl vystaven Provozovatel ISDS v případě, že by nedostatky zjištěné auditem nebyly odstraněny.

Vady návrhové dokumentace a plánu Migrace ISDS s využitím kritéria míry rizik bude Objednatel kategorizovat následovně:

|  |  |  |
| --- | --- | --- |
| Kategorie | Stav akceptace | Popis kritérií |
| A | Neakceptováno | Neodstranitelná vada, která vystavuje Provozovatele ISDS riziku, jehož míra je hodnocena jako vysoké nebo kritické riziko. |
| B | Neakceptováno do doby odstranění vady | Odstranitelná vada, která vystavuje Provozovatele ISDS riziku, jehož míra je hodnocena jako střední, vysoké nebo kritické riziko. |
| C | Akceptováno s výhradou | Neodstranitelná vada, která vystavuje Provozovatele ISDS riziku, jehož míra je hodnocena jako nízké nebo žádné riziko. |
| D | Akceptováno bez  výhrad |  |

Doba trvání auditu návrhové dokumentace a plánu Migrace je 20 dnů.

## Audit bezpečnosti ISDS před provedením Migrace dat a uvedením do Řádného a plného provozu

Poskytovatel umožní Objednateli, resp. Objednatelem určené třetí osobě, provést předběžný audit v následujícím rozsahu.

### Rozsah auditu

Auditován bude ISDS ve stavu před Migrací dat, budou auditovány i procesy a organizace administrování ISDS. Budou provedeny následující činnosti:

1. externí penetrační testy perimetru ISDS,
2. interní penetrační testy z vnitřních zón ISDS,
3. kontroly nastavení bezpečnostních mechanismů ISDS,
4. kontroly nastavení přístupových oprávnění tzv. silných uživatelů,
5. kontroly nastavení způsobů a postupů administrace.

### Podmínky provedení auditu

1. Poskytnutí dokumentace skutečného provedení ISDS.
2. Provedení pracovních jednání k upřesnění informací uvedených v dokumentaci skutečného provedení ISDS.
3. Součinnost při plánování provedení technických prověrek.
4. Součinnost při provedení penetračních testů spočívající v:
   1. Koordinace postupů v případě bezpečnostního incidentu vyvolaného v průběhu penetračních testů.
   2. Technická asistence při provádění interních penetračních testů.
5. Součinnost při provedení kontroly nastavení bezpečnostních mechanismů spočívající v:
   1. Ověření nástrojů pro provádění kontroly nastavení bezpečnostních mechanismů ISDS.
   2. Ověření nástrojů pro provádění kontroly nastavení přístupových oprávnění tzv. silných uživatelů.
   3. Asistence při provádění kontroly nastavení bezpečnostních mechanismů.
   4. Asistence při provádění kontroly nastavení přístupových oprávnění tzv. silných uživatelů ISDS.
   5. Uložení, zabezpečení, sanitizování a předání dat získaných pomocí nástrojů pro provádění kontroly nastavení bezpečnostních mechanismů ISDS a nástrojů pro provádění kontroly nastavení přístupových oprávnění tzv. silných uživatelů ISDS.

### Kritéria auditu pro akceptaci

Jako kritérium pro akceptaci ISDS před provedením Migrace dat a uvedením do Řádného a plného provozu bude použita míra rizik, kterým by byl vystaven Provozovatel ISDS.

Vady ISDS před provedením Migrace dat a uvedením do Řádného a plného (produkčního) provozu s využitím kritéria míry rizik bude Objednatel kategorizovat následovně:

|  |  |  |
| --- | --- | --- |
| Kategorie | Stav akceptace | Popis kritérií |
| A | Neakceptováno | Neodstranitelná vada, která vystavuje Provozovatele ISDS riziku, jehož míra je hodnocena jako vysoké nebo kritické riziko.  Odstranitelná vada, která vystavuje Provozovatele ISDS riziku, jehož míra je hodnocena jako střední, vysoké nebo kritické riziko. |
| B | Akceptováno s výhradou | Neodstranitelná vada, která vystavuje Provozovatele ISDS riziku, jehož míra je hodnocena jako nízké nebo žádné riziko.  Odstranitelná vada, která vystavuje provozovatele ISDS riziku, jehož míra je hodnocena jako nízké nebo žádné riziko. |
| C | Akceptováno bez  výhrad |  |

Audit bude proveden za 40 dní od předání dokumentace skutečného provedení ISDS.

## Funkční, výkonnostní, integrační a bezpečnostní testy ISDS

Poskytovatel navrhne postup testování, kde je doporučeno vytvořit  - **Cíle testování, Seznam plánovaných oblastí k testování, Kategorie testů, Požadavky na testovací data, harmonogram plánovaných testů.**Objednatel schválí postup testování. Poskytovatel připraví vše potřebné dle postupu testování, následně ve spolupráci s Objednatelem provede v plánovaných termínech příslušné testy. Výstupem testování budou průkazné protokoly dokumentující průběh a výsledky testů.

Testování Poskytovatel navrhne pro veřejné testovací prostředí, předprodukční prostředí a produkční prostředí.

### Kritéria pro akceptaci funkčních, výkonnostních a integračních testů

|  |  |  |
| --- | --- | --- |
| Kategorie | Stav akceptace | Popis kritérií |
| A | Neakceptováno | Kritická vada funkčnosti k termínu provedení Migrace dat do produkčního prostředí – nesplnění zadání dle Smlouvy, nebo vada, která zásadně ovlivňuje klíčovou funkci ISDS, nebo koncoví uživatelé nemají ke službám ISDS přístup. Ve svých důsledcích může Objednateli způsobit velké finanční nebo jiné škody. |
| B | Neakceptováno do doby odstranění vady | Kritická vada funkčnosti – nesplnění zadání dle Smlouvy, nebo vada, která zásadně ovlivňuje klíčovou funkci ISDS, nebo koncoví uživatelé nemají ke službám ISDS přístup. Ve svých důsledcích může Objednateli způsobit velké finanční nebo jiné škody. |
| C | Akceptováno s výhradou, a požadavkem na odstranění | Závažná vada funkčnosti – odstranitelná vada, která zásadně neovlivňuje klíčovou funkci ISDS, neomezuje běžný provoz ISDS, nebo je zasažena nepříliš významná část funkcionality ISDS.  Vada, která nebyla zařazena ani mezi vadu kategorie A a B, která nebrání užívání ISDS, anebo má zcela minimální vliv na řádné užívání nebo funkčnost ISDS. |
| D | Akceptováno bez  výhrad |  |

V případě ukončení auditu nebo testování se statutem akceptováno s výhradou bude v akceptačním protokolu, v případech, kdy to Objednatel uzná za vhodné, uveden termín pro odstranění nedostatků (vad).

# Požadavky v oblasti bezpečnosti

## Legislativní vymezení

Poskytovatel realizuje opatření, která  vyplývají z požadavků ZEU, Vyhlášky, ZKB, ZISVS a ZOOÚ.

## Požadavky na soulad se Zákonem o kybernetické bezpečnosti

Poskytovatel je povinen realizovat opatření nutná k zajištění souladu ISDS s požadavky ZKB a ostatních právních předpisů o kybernetické bezpečnosti. V případě změny právních předpisů v oblasti kybernetické bezpečnosti je Poskytovatel povinen navrhnout a po schválení Objednatelem realizovat potřebná opatření v souladu s příslušnými právními předpisy a oprávněnými požadavky Správce. Pokud budou tato opatření znamenat změny ISDS definované touto Smlouvou v části Služeb Rozvoje, budou řešeny v rámci Služeb Rozvoje. Jedná se především o:

1. **Technická opatření** požadovaná ZKB, která musí být zvolena a implementována s ohledem na architekturu a požadované technické provedení ISDS:

* fyzické bezpečnosti dle §16 vyhlášky č. 316/2014,
* nástroj pro ochranu integrity komunikačních sítí dle §17 vyhlášky č. 316/2014,
* nástroj pro ověřování identity uživatelů dle §18 vyhlášky č. 316/2014,
* nástroj pro řízení přístupových oprávnění dle §19 vyhlášky č. 316/2014,
* nástroj pro ochranu před škodlivým kódem dle §20 vyhlášky č. 316/2014,
* nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů dle §21 vyhlášky č. 316/2014,
* nástroj pro detekci kybernetických bezpečnostních událostí dle §22 vyhlášky č. 316/2014 ,
* nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí dle §23 vyhlášky č. 316/2014,
* aplikační bezpečnosti dle §24 vyhlášky č. 316/2014,
* kryptografické prostředky dle §25 vyhlášky č. 316/2014,
* nástroj pro zajišťování úrovně dostupnosti dle §26 vyhlášky č. 316/2014.

1. **Organizační opatření** požadovaná ZKB, která musí být navržena, zavedena a prováděna s ohledem na model provozování ISDS:

* systém řízení bezpečnosti informací dle §3 vyhlášky č. 316/2014,
* řízení rizik dle §4 vyhlášky č. 316/2014,
* bezpečnostní politika dle §5 vyhlášky č. 316/2014,
* organizační bezpečnost dle §6 vyhlášky č. 316/2014, určení manažera a architekta kybernetické bezpečnosti,
* řízení aktiv dle §8 vyhlášky č. 316/2014,
* bezpečnosti lidských zdrojů dle §9 vyhlášky č. 316/2014,
* řízení provozu a komunikací dle §10 vyhlášky č. 316/2014,
* řízení přístupu a bezpečné chování uživatelů dle §11 vyhlášky č. 316/2014,
* akvizice, vývoj a údržba dle §12 vyhlášky č. 316/2014,
* zvládání kybernetických bezpečnostních událostí a incidentů dle §13 vyhlášky č. 316/2014,
* řízení kontinuity činností dle §14 vyhlášky č. 316/2014.

## Zajištění podmínek a součinnosti při auditu kybernetické bezpečnosti

1. Poskytovatel zajistí, aby testovací (auditní) datové schránky nastavené a spravované v produkčním prostředí pro potřeby auditu byly:
   1. typu FO, PFO, PO, OVM,
   2. přístupné po dobu provádění auditu auditorovi, kterého určí Objednatel a za tímto účelem mu předá bezpečným způsobem příslušné přihlašovací údaje,
   3. po ukončení auditu budou příslušné přihlašovací údaje k testovacím (auditním) datovým schránkám změněny.
2. Poskytovatel zřídí ve veřejném testovacím prostředí   datové schrány základních typů (FO, PFO, PO, OVM) a nastaví příslušné přístupová údaje pro držitele těchto DS, které předá auditorovi.
3. Poskytovatel zajistí, aby v době provádění auditu byly ve veřejném testovacím prostředí  ISDS implementovány a řádně nastaveny všechny bezpečnostní funkce stejně, jako ve verzi produkčního prostředí, ke které je prováděn bezpečnostní audit.
4. Poskytovatel umožní auditorovi v době provádění auditu provést prověrku konfigurací HW, základního a generického SW, síťových prvků, datových linek, Licencovaného software a Software vytvořeného Poskytovatelem (dále jen prověrky konfigurací), které tvoří produkční prostředí ISDS a při tom mu poskytl potřebnou součinnost, která spočívá v následujícím:
   1. poskytnutí veškeré interní dokumentace skutečného provedení ISDS.
   2. ověření, že nástroje, postupy a procedury navržené auditorem k provedení prověrek konfigurací nemohou narušit bezpečnost produkčního prostředí ISDS a způsobit jeho nedostupnost na dobu delší než je plánovaná doba na provedení prověrky konfigurací.
   3. schválení, že je možné použít nástroje, postupy a procedury navržené k provedení prověrek konfigurací.
   4. za asistence auditora spustí nástroje a provede postupy a procedury navržené a schválené k provedení prověrek konfigurací.
   5. zabezpečí data, která vznikla během nástrojů a provedením postupů a procedur navržených a schválených k provedení prověrek konfigurací. Zabezpečení dat spočívá v
      1. vytvoření otisků pomocí kryptografických hash funkcí ke každému vzniklému datovému souboru,
      2. ověření, že vzniklé datové soubory mají obsah, který odpovídá vytvořeným otiskům,
      3. uložení datových souboru a jejich otisků na výměnné datové medium (DVD),
      4. předání otisků auditorovi.
   6. provede sanitizaci dat, která vznikla během nástrojů a provedením postupů a procedur navržených a schválených k provedení prověrek konfigurací. Sanitizace spočívá v odstranění všech osobních údajů z těchto dat. Dále vytvoří otisky pomocí kryptografických hash funkcí ke každému vzniklému sanitizovanému datovému souboru. Soubory společně s otisky umístí na výměnné datové medium (DVD) a jeho kopii předají auditorovi.
   7. Pokud auditor v průběhu vyhodnocení předaných dat vyjádří odůvodněnou pochybnost o provedené sanitizaci dat, provede pověřený zástupce Poskytovatele a auditora v prostředí Poskytovatele zkoušku, ve které použijí příslušné původní datové soubory, příslušné sanitizované soubory, jejich integritu ověří pomocí dříve vytvořených otisků. Zkouška prověří, zda sanitizace byla provedena řádně či nikoliv. V případě negativního výsledku se provede nová vytvoření sanitizovaných dat a jejich předání auditorovi.
   8. Poskytovatel je povinen se seznámit s vybranými výsledky prověrky konfigurací a vyjádřit se k nim.
   9. Poskytovatel je povinen na pokyn Objednatele navrhnout, jakým způsobem odstraní prověrkou zjištěné nedostatky v konfiguraci ISDS.

* Poskytovatel umožní auditorovi provést externí a interní penetrační testy produkčního prostředí ISDS a při tom mu poskytne potřebnou součinnost, která spočívá v následujícím:
  1. poskytnutí dokumentaci vnitřní sítě ISDS
  2. zajištění účasti na připomínkování plánu provedení externích a interních penetračních testů
  3. předání auditorovi informace o adresách (rozsazích adres) vstupních bodů bezpečnostního perimetru ISDS, přes které budou vedeny externí penetrační testy
  4. předání auditorovi informací o adresách (rozsazích adres) ve vnitřních sítích, přes které budou vedeny interní penetrační testy, a o fyzických portech na zařízeních interní sítě, kde mohou být zapojena zařízení, ze kterých budou prováděny interní penetrační testy.
  5. Poskytovatel zajistí v průběhu penetračních testů zvýšené monitorování kybernetických bezpečnostních událostí a incidentů a v případě, že zjistí vznik závažného nebo velmi závažného kybernetického incidentu, tak informuje neprodleně Objednatele a auditora. Auditor neprodleně pozastaví provádění penetračních testů do doby, kdy se rozhodne o jejich pokračování.
  6. Poskytovatel zajistí v průběhu penetračních testů zvýšené monitorování provozních událostí a mezních stavů a v případě, že zjistí překročení nastavených mezních hodnot, informuje Objednatele a auditora. Auditor neprodleně pozastaví provádění penetračních testů do doby, kdy se rozhodne o jejich pokračování.
  7. Poskytovatel je povinen se seznámit s vybranými výsledky penetračních testů a vyjádřit se k nim.
  8. Poskytovatel je povinen na pokyn Objednatele navrhnout, jakým způsobem odstraní penetračním testováním zjištěné nedostatky v zabezpečení ISDS a na vlastní náklady je odstranit.

## Požadavky na ochranu ISDS před útoky DoS a DDoS a škodlivým kódem

Objednatel požaduje, aby Poskytovatel zajistil efektivní ochranu před všemi známými útoky typu DoS a DDoS, která umožňují takové útoky rozpoznat a reagovat na ně tak, aby nebyla ohrožena bezpečnost Datových schránek. Objednatel požaduje, aby navržený systém ochrany byl dostatečně adaptivní a byl schopen chránit i před nově vyvinutými útoky DoS/DDoS.

Dále se požaduje, aby Poskytovatel v návrhové dokumentaci podrobně popsal, které komponenty ISDS budou před DoS a DDOS chráněny, jakými metodami a nástroji (vlastními, třetích stran nebo kombinací), jak bude zajištěna prevence, detekce a eliminace s minimálním dopadem na dostupnost ISDS.

Objednatel požaduje, aby Poskytovatel zajistil efektivní provádění kontroly příloh Datových zpráv na přítomnost škodlivého kódu v souladu s Vyhláškou i ZKB tak, aby:

* 1. navrhovaný koncept provádění antivirové ochrany efektivně odhalil a zablokoval doručování datových zpráv, ve kterých je vložen škodlivý kód všech známých typů,
  2. navrhovaný koncept provádění antivirové ochrany byl adaptivní a byl schopen odhalovat nově vzniklé škodlivé kódy,
  3. bylo dodrženo zejména ustanovení §14 odst. 6 ZEU.

## Požadavky na provádění pravidelné prověrky obnovy ISDS

Objednatel požaduje, aby Poskytovatel prováděl pravidelně prověrku obnovy všech prostředí ISDS dle zpracovaných havarijních plánů a ověřoval tak připravenost na zvládnutí havárie.

Plány musí obsahovat:

* podrobný popis komponent (částí) ISDS, které budou nejcitlivější na potencionální výpadky včetně toho, které budou nejvíce výkonově zatíženy nebo nejčastěji zasaženy změnami systému,
* popis metodiky, případně nástroje, které budou pro prověrku obnovy ISDS použity, musí být uvedena časová náročnost na požadovanou výluku ISDS. S tím souvisí i deklarace zajištění součinnosti poskytovatele datového centra při simulování výpadků jeho infrastruktury při testování prověrek obnovy.

Provedení, výsledky této prověrky a opatření na odstranění zjištěných nedostatků Poskytovatel bude dokumentovat a zprávu o jejím provedení pravidelně předkládat Objednateli.

# Náležitosti měsíční zprávy o provozu

Poskytovatel předkládá vždy do 7. dne v měsíci pravidelnou měsíční zprávu o provozu za uplynulý měsíc (měřené období), která obsahuje požadované údaje reportingu uvedené v Příloze č. 6 a dále následující informace:

Limitní parametry (dle Přílohy č. 6) – časový průběh hodnot limitních parametrů (mimo vyhrazenou dobu), průběh maximálních, průměrných a minimálních hodnot.

Časové průběhy počtu stahování datových zpráv (DZ/min, průběh maximálních, průměrných a minimálních hodnot)

Výsledky získávání časového razítka - přehled dostupnosti služby zajištění časových razítek

* Seznam jednotlivých případů zrušení DS, u kterých nebyla splněna garantovaná doba vyřízení s uvedením skutečného času zrušení DS
* Informace Change managementu a Release managementu
* Rozvoj ISDS – rozpis počtu MD vynaložených v daném měsíci a vztažených ke konkrétním změnovým požadavkům Služeb Rozvoje
* Plánované výluky
  + časový plán výluk měsíc dopředu
  + požadavky na součinnost Objednatele
  + naplnění časového plánu výluk za uplynulý měsíc
  + odstranění chyb a problémů z minulého období,
* Bezpečnostní incidenty – přehled a popis
* Provozní statistiky pro Správce a Provozovatele ISDS – podoba statistik bude formou tabulky, která bude upřesněna dohodou mezi Poskytovatelem a Objednatelem
* Systémové požadavky – Podporované operační systémy a prohlížeče, testované prohlížeče

# Požadavky na Dokumentaci

Dokumentací se rozumí dokumentace potřebná pro vybudování, sestavení a zprovoznění ISDS a jeho částí, Migraci dat, instalaci a administraci jednotlivých částí systému a další správu systému. Jedná se mimo jiné o:

* projektovou dokumentaci (včetně harmonogramu, základního dokumentu projektu, registru rizik a další projektové dokumentace související s převzetím a rozvojem ISDS);
* administrátorskou dokumentaci (včetně komplexního popisu všech užitých analytických a monitorovacích nástrojů, provozního deníku aplikace, logické a fyzické architektury aplikace, včetně propojení na externí systémy a popisu komunikace s externími systémy);
* uživatelskou dokumentaci;
* programátorskou dokumentaci (včetně Dokumentace všech zdrojových kódů Licencovaného software, Software vytvořeného Poskytovatelem a seznamu, popisu a verzí Software třetích stran, popisu datových struktur a návrhu databází);
* dokumentaci potřebnou pro sestavení ISDS, požadavky na technickou infrastrukturu;
* příprava testování systému obsahující metodiku testování pro funkční, integrační zátěžové, performance a bezpečnostní testy, testovací scénáře a testovací data;
* bezpečnostní dokumentaci vytvořenou v souladu s požadavky vyhlášky o kybernetické bezpečnosti (včetně komplexního popisu nastavení komunikace, přístupových práv a dalších zabezpečení, včetně zabezpečení dle požadavků ZKB).

Dokumentace musí být zpracována v souladu se ZISVS, a s příslušnými prováděcími předpisy a ZKB.

Povinností Poskytovatele je, aby vytvořil a udržoval projektovou dokumentaci ve struktuře, která je běžně doporučována uznávanými metodikami např. Prince2 respektive PMBOK 5th edition minimálně po podobu, než bude ISDS uveden do Řádného a plného provozu a dále dle požadavků Objednatele. Objednatel dále požaduje, aby Poskytovatel zpřístupnil tuto dokumentaci Objednateli.

Povinností Poskytovatele je při změnách aplikace nebo její konfigurace Dokumentaci aktualizovat.

**Typy Dokumentace:**

**Veřejná dokumentace:**

* Provozní řád
* veřejné formuláře žádostí o zřízení datové schránky

Objednatel zajišťuje potřebné úpravy Provozního řádu, jeho publikaci veřejných formulářů žádostí o zřízení datové schránky na informačním webu <https://www.datoveschranky.info>.

Poskytovatel zajistí nezbytnou součinnost při průběžných úpravách dokumentace v rámci dokumentů Provozního řádu. Předkládá návrhy úprav této dokumentace.

**Neveřejná dokumentace**

* ISDS\_funkcni\_design
* ISDS\_servisni\_modul\_MV
* ISDS\_architektura\_aplikace
* administrátorské příručky
* instalační příručky
* specifikace aplikací
* technická dokumentace k formulářům
* dokumentace webových služeb a komunikačních rozhraní pro předávání dat
* dokumentace a číselníky pro předávání dat hybridní poště
* dokumentace pro komunikaci v případě nestandardních situací
* bezpečnostní dokumentace
* havarijní plány
* další potřebné provozní a ostatní dokumentace dle Smlouvy a legislativou požadované

Poskytovatel zajišťuje průběžnou úpravu kompletní a úplné Dokumentace ISDS a předává ji Objednateli.