



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dodatek č. 1 Detailního návrhu technického řešení informačních systémů e- Sbírka a e-Legislativa

Projekt e-Sbírka a e-Legislativa

Připraveno pro:

Ministerstvo vnitra ČR

16. 6. 2016

Verze 1.0, Finální

Připravil:

MVČR



Změny a schválení

Změny

Datum	Autor	Verze	Popis změn
16. 6. 2016	Tým architekta eSeL	1.0	Finální verze

Revize

Jméno	Schválená verze	Funkce	Datum
Mgr. A. Gola	1.0	Věcný gestor projektu	16. 6. 2016



Obsah

1	Úvod	5
2	Model požadavků	6
2.1	Funkční požadavky	6
2.1.1	e-Legislativa	6
2.1.2	Integrace	7
2.2	Nefunkční požadavky.....	7
2.2.1	Zákon o Kybernetické bezpečnosti	7
2.2.2	Výkon.....	20
2.2.3	Provoz a infrastruktura	22
2.2.4	Dokumentace	23
3	Případy užití	25
3.1	Portál e-Legislativa	25
3.1.1	Prostory připomínek a pozměňovacích návrhů	25
4	Model komponent a implementace.....	28
5	Model nasazení a provozu	29
5.1	Základní architektura řešení v oblasti nasazení a provozu	29
5.1.1	Provozní prostředí a lokality	29
5.1.2	Služby zajišťované CMS a DCeGOV v souladu s ZoKB a VoKB	32
5.1.3	Virtualizovaná serverová infrastruktura	34
5.1.4	Infrastruktura vysoké dostupnosti	34
5.1.5	Koncepce síťové infrastruktury	35
5.1.6	Prostředí pro provoz systému	40
5.1.7	Typy zařízení	46
5.1.8	Provoz informačního systému	48
5.2	Doporučená architektura řešení v oblasti nasazení a provozu	52
6	Přílohy	54
6.1	Příloha č. 1 - Specifikace služeb CMS	54
6.1.1	Služba CMS2 – 02 – Zveřejnění aplikace	54



6.1.2	Služba CMS2 – 03 – Přístup k aplikaci	55
6.1.3	Služba CMS2 – 04 – Umístění aplikace OVM do NDC	56
6.1.4	Služba CMS2 – 05 – Přenos elektronické pošty	56
6.1.5	Služba CMS2 – 06 – DNS hosting.....	57
6.1.6	Služba CMS2 – 07 – Služby sTESTA.....	57
6.1.7	Služba CMS2 – 08 – Přístup do CMS	58
6.1.8	Služba CMS2 – 09 – Přístup do Internetu.....	59
6.1.9	Služba CMS2 – 10 – Přístup k záznamům o provozu	59
6.1.10	Služba CMS2 – 11 – Přístup k účtovacím informacím.....	60
6.1.11	Služba CMS2 – 12 – Virtuální firewall.....	60
6.2	Příloha č. 2 – výňatek přílohy č. 1 k vyhlášce č. 316/2014 Sb.	61
6.2.1	Hodnocení a úrovně důležitosti aktiv	61
6.2.2	Hodnocení rizik	63



1 Úvod

Tento dokument „Dodatek č. 1 k *Detailnímu návrhu technického řešení informačního systému e-Sbírka a e-Legislativa*“ přímo navazuje na dokument „*Detailní návrh technického řešení informačního systému e-Sbírka a e-Legislativa*“, který doplňuje, mění a jinak upravuje.

Tento dokument je změnovým dokumentem a zachycuje vývoj detailního návrhu technického řešení od roku 2013 do data finalizace tohoto dokumentu.

2 Model požadavků

Tato kapitola popisuje další funkční a nefunkční požadavky, které musí systémy e-Sbírka a e-Legislativa pokrýt.

2.1 Funkční požadavky

Funkční požadavky popisují požadované funkce systému, tj. to "co" by měl systém dělat. V následujících kapitolách jsou uvedena doplnění a změny oproti dokumentu „*Detailní návrh technického řešení informačního systému e-Sbírka a e-Legislativa*“.

2.1.1 e-Legislativa

2.1.1.1 Editor e-Šablona pro plusovou osu

2.1.1.1.1 FP2380-Kopie pozměňovacího návrhu

Obsah pozměňovacího návrhu (PN) musí jít zkopírovat z jiného pozměňovacího návrhu. V případě, že zdrojový pozměňovací návrh vychází z jiné vrstvy návrhu, bude vygenerovaný obsah pozměňovacího návrhu proveden způsobem "best effort".

Tato funkčnost musí umožnit jednoduchou přípravu opakovaného pozměňovacího návrhu, který nebyl dříve v rámci schvalovacího procesu přijat, např. opětovné podání PN z Poslanecké sněmovny v Senátu nebo opětovné podání PN z jednání výboru na schůzi Poslanecké sněmovny nebo Senátu.

2.1.1.1.2 FP2381-Podpora pro hlasování o pozměňovacích návrzích

Systém musí umožnit:

- zadat u pozměňovacího návrhu notifikaci, zda byl přijat nebo nikoli, kterou bude možné jednoduše zadat během hlasovací procedury
- zobrazit náhled návrhu předpisu se zapracováním přijatých pozměňovacích návrhů (s případným označením kolizí) umožňující získat přehled o aktuálním stavu návrhu právního předpisu ve znění aktuálně přijatých pozměňovacích návrhů; v průběhu hlasování takový náhled aktualizovat

Tyto mechanismy musí být k dispozici samostatně i pro sady pozměňovacích návrhů (podpora pro hlasování na výborech a komisích).

2.1.2 Integrace

2.1.2.1 RPP

2.1.2.1.1 FP3042- Notifikace změn

Dojde-li v eSbírce k vyhlášení předpisu, na jehož ustanovení je navázán záznam z RPP (dochází tedy k vyhlášení nového ustanovení, jeho změně nebo zrušení), uchová eSbírka informaci o této změně (1 měsíc). Zároveň v rámci veřejného API poskytuje eSbírka dotazovací službu, pomocí které je možné získat seznam takovýchto změn za zadané časové období (např. minulý den). RPP bude pravidelně každý den získávat přes toto API seznam výše uvedených změn v eSbírce za minulý den.

2.2 Nefunkční požadavky

Nefunkční požadavky představují omezující podmínky a obecné vlastnosti vyžadované od informačního systému bez ohledu na jeho dílčí funkčnosti. Jsou to zejména požadavky na výkon, bezpečnost a další provozní charakteristiky. V následujících kapitolách jsou uvedena doplnění a změny oproti dokumentu „*Detailní návrh technického řešení informačního systému e-Sbírka a e-Legislativa*“.

2.2.1 Zákon o Kybernetické bezpečnosti

2.2.1.1 Obecné požadavky

2.2.1.1.1 NP060-Zákon o kybernetické bezpečnosti

Systém musí splňovat požadavky Zákona o kybernetické bezpečnosti č. 181/2014 Sb. (dále jen zákon o kybernetické bezpečnosti nebo ZoKB) ve znění pozdějších předpisů a vyhlášky č. 316/2014 Sb. (dále jen Vyhláška o kybernetické bezpečnosti nebo VoKB) ve znění pozdějších předpisů..

2.2.1.1.2 NP061-Hodnocení systému dle ZoKB

Systém je hodnocen jako významný systém dle §2 ZoKB.

2.2.1.1.3 NP062-Primární aktiva dle VoKB

Primárními aktivy systému jsou:

- IN01 - Zveřejněné platné právo (veřejná část eSbírky)
- IN02 - Platné právo v průběhu digitalizace (neveřejná část eSbírky)
- IN03 - Zveřejněné připravované právo (veřejná část eLegislativy)
- IN04 - Neveřejné připravované právo (neveřejná část eLegislativy)
- IN05 - Externí uživatelé (údaje externích uživatelů)



2.2.1.1.4 NP063-Hodnocení primárních aktiv dle přílohy 1 VoKB

Primární aktiva dle přílohy 1 VoKB jsou hodnocena takto a systém musí umožňovat jejich dodržení v rámci provozu.

Aktivum: IN01 - Zveřejněné platné právo (veřejná část eSbírky)

Důvěrnost: nízká

Integrita: nízká

Dostupnost: vysoká

Aktivum: IN02 - Platné právo v průběhu digitalizace (neveřejná část eSbírky)

Důvěrnost: střední

Integrita: vysoká

Dostupnost: střední

Aktivum: IN03 - Zveřejněné připravované právo (veřejná část eLegislative)

Důvěrnost: nízká

Integrita: nízká

Dostupnost: vysoká

Aktivum: IN04 - Neveřejné připravované právo (neveřejná část eLegislative)

Důvěrnost: střední

Integrita: vysoká

Dostupnost: vysoká

Aktivum: IN05 - Externí uživatelé (údaje externích uživatelů)

Důvěrnost: vysoká

Integrita: střední

Dostupnost: střední

2.2.1.1.5 NP064-Hodnocení rizik dle přílohy 2 VoKB

V rámci implementační analýzy bude provedeno hodnocení rizik dle přílohy 2 VoKB, které bude vstupem pro doplnění a upřesnění bezpečnostních opatření technického i organizačního charakteru.

2.2.1.2 Organizační opatření

2.2.1.2.1 NP065-Systém řízení bezpečnosti informací (VoKB § 3)

odst. 1 b), odst. 2 a):

Je zaveden proces řízení rizik.

odst. 1 c), odst. 2 b):

Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS, zavedena příslušná bezpečnostní opatření.

odst. 2 c):

Prováděna aktualizace zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.

2.2.1.2.2 NP066-Řízení rizik (VoKB § 4)

odst. 1, 2 a):

Stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.

odst. 1, 2 b):

Prováděna identifikace a hodnocení důležitosti aktiv, která patří do rozsahu ISMS, podle § 8 (Řízení aktiv) minimálně v rozsahu přílohy č. 1 k VoKB a výstupy zapracuje do zprávy o hodnocení aktiv a rizik.

odst. 1, 2 c):

Prováděna identifikace rizik, při kterých jsou zohledňovány hrozby a zranitelnosti, posuzovány možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k VoKB. Jsou určena a schválena přijatelná rizika a je zpracována zpráva o hodnocení aktiv a rizik.

odst. 1, 2 d):

Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření.

odst. 1, 2 e):

Je zpracovaný a zavedený plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby odpovědné za prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.

odst. 1, 2 f):

Bez zbytečného odkladu jsou zohledňována reaktivní a ochranná opatření vydaná NBÚ v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, jsou doplněny plány zvládání rizik.

odst. 3:

Řízení rizik je zajištěno jinými způsoby (než jak je stanoveno v odstavci 1 a 2) a orgán a osoba doložil(a), že použítá opatření zajišťují stejnou nebo vyšší úroveň řízení rizik.

Zváženy hrozby, související s/se:

- odst. 4 a) porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany uživatelů a administrátorů.
- odst. 4 b) poškozením nebo selháním technického anebo programového vybavení.
- odst. 4 c) zneužití identity fyzické osoby.
- odst. 4 d) užíváním programového vybavení v rozporu s licenčními podmínkami.
- odst. 4 e) kybernetickým útokem z komunikační sítě.
- odst. 4 f) škodlivým kódem (například viry, spyware, trojské koně).
- odst. 4 g) nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
- odst. 4 h) narušením fyzické bezpečnosti.
- odst. 4 i) přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie.
- odst. 4 j) zneužitím nebo neoprávněnou modifikací údajů.
- odst. 4 k) trvale působícími hrozbami.

- odst. 4 l) odcizením nebo poškozením aktiva.

Zváženy zranitelnosti, související s:

- odst. 5 a) nedostatečnou ochranou vnějšího perimetru.
- odst. 5 b) nedostatečným bezpečnostním povědomím uživatelů a administrátorů.
- odst. 5 c) nedostatečnou údržbou informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
- odst. 5 d) nevhodným nastavením přístupových oprávnění.
- odst. 5 e) nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.
- odst. 5 f) nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování.
- odst. 5 g) nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí.

2.2.1.2.3 NP067-Bezpečnostní politika (VoKB § 5)

Stanovena bezpečnostní politika v oblastech:

- odst. 1 a), odst. 2 a): Systém řízení bezpečnosti informací.
- odst. 1 b), odst. 2 b): Organizační bezpečnost. (viz Organizační bezpečnost (VoKB § 6))
- odst. 2 c): Řízení dodavatelů. (viz Stanovení bezpečnostních požadavků pro dodavatele (VoKB § 7))§ 6))
- odst. 1 d), odst. 2 d): Klasifikace aktiv.
- odst. 1 e), odst. 2 e): Bezpečnost lidských zdrojů.
- odst. 1 f), odst. 2 f): Řízení provozu a komunikací.
- odst. 1 g), odst. 2 g): Řízení přístupu.
- odst. 1 h), odst. 2 h): Bezpečné chování uživatelů.
- odst. 1 i), odst. 2 i): Zálohování a obnova.
- odst. 1 m), odst. 2 j): Poskytování a nabývání licencí programového vybavení a informací.
- odst. 1 o), odst. 2 k): Ochrana osobních údajů.
- odst. 1 r), odst. 2 m): Ochrana před škodlivým kódem.
- odst. 1 s), odst. 2 n): Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.
- odst. 1 u), odst. 2 l): Používání kryptografické ochrany.
- odst. 3: Je pravidelně hodnocena účinnost bezpečnostní politiky. Bezpečnostní politika je pravidelně aktualizována.

2.2.1.2.4 NP068-Organizační bezpečnost (VoKB § 6)

odst. 1:

Zavedena organizace řízení bezpečnosti informací (dále jen „organizační bezpečnost“), v rámci které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury, komunikačním systémem kritické informační infrastruktury nebo významným informačním systémem.

odst. 3:

Bezpečnostní role jsou určeny přiměřeně podle odstavce 2.

odst. 7:

Určen výbor pro řízení kybernetické bezpečnosti.

odst. 8:

Je zajištěno odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle Bezpečnost lidských zdrojů odst. 1 písm. b).

2.2.1.2.5 NP069-Stanovení bezpečnostních požadavků pro dodavatele (VoKB § 7)

odst. 1:

Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS dokumentován písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.

2.2.1.2.6 NP070-Řízení aktiv (VoKB § 8)

odst. 1 a):

Jsou identifikována a evidována primární aktiva.

odst. 1 b):

Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva.

odst. 1 c):

Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k VoKB.

Při hodnocení důležitosti primárních aktiv je posouzeno především:

- odst. 2 a): Rozsah a důležitost osobních údajů nebo obchodního tajemství.
- odst. 2 b): Rozsah dotčených právních povinností nebo jiných závazků.
- odst. 2 c): Rozsah narušení vnitřních řídicích a kontrolních činností.
- odst. 2 d): Poškození veřejných, obchodních nebo ekonomických zájmů.
- odst. 2 e): Možné finanční ztráty.
- odst. 2 f): Rozsah narušení běžných činností orgánu a osoby.
- odst. 2 g): Dopady spojené s narušením důvěrnosti, integrity a dostupnosti.
- odst. 2 h): Dopady na zachování dobrého jména nebo ochranu dobré pověsti.

Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že:

- odst. 4 a) 1.: Jsou určeny způsoby rozlišování jednotlivých úrovní aktiv.
- odst. 4 a) 2.: Jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.
- odst. 4 a) 3.: Jsou stanoveny přípustné způsoby používání aktiv.
- odst. 4 b): Jsou zavedena pravidla ochrany odpovídající úrovni aktiv.
- odst. 4 c): Jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.

2.2.1.2.7 NP071-Bezpečnost lidských zdrojů (VoKB § 9)

odst. 1 a):

Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.

odst. 1 b):

V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.

odst. 1 c):

Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.



odst. 1 d):

Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.

odst. 2:

O školení podle odstavce 1 jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

2.2.1.2.8 NP072-Řízení provozu a komunikací (VoKB § 10)

odst. 1:

Pomocí technických nástrojů uvedených v § 21 až 23 jsou detekovány kybernetické bezpečnostní události, pravidelně vyhodnocovány získané informace a na zjištěné nedostatky reagováno v souladu s: Zvládání kybernetických bezpečnostních událostí a incidentů (VoKB § 13).

odst. 2:

Zajištěn bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem jsou stanoveny provozní pravidla a postupy.

odst. 4:

Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.

2.2.1.2.9 NP073-Řízení přístupu a bezpečné chování uživatelů (VoKB § 11)

odst. 1:

Na základě provozních a bezpečnostních potřeb je řízen přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a každému uživateli je přiřazen jednoznačný identifikátor.

odst. 2:

Jsou přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního



systému podle Nástroj pro ověřování identity uživatelů (VoKB § 18) a Nástroj pro řízení přístupových oprávnění (VoKB § 19), a která brání ve zneužití těchto údajů neoprávněnou osobou.

2.2.1.2.10 NP074-Akvizice, vývoj a údržba (VoKB § 12)

odst. 1:

Jsou stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.

2.2.1.2.11 NP075-Zvládání kybernetických bezpečnostních událostí a incidentů (VoKB § 13)

a):

Jsou přijata nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních jsou vedeny záznamy.

b):

Je připraveno prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VoKB § 21),

Nástroj pro detekci kybernetických bezpečnostních událostí (VoKB § 22), Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (VoKB § 23), je prováděno jejich vyhodnocení a jsou identifikovány kybernetické bezpečnostní incidenty.

c):

Je prováděna klasifikace kybernetických bezpečnostních incidentů, přijímáno opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, prováděno hlášení kybernetického bezpečnostního incidentu podle § 32 a zajištěn sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.

d):

Jsou prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu, vyhodnocena účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení jsou

stanovena nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

e):

Zvládání kybernetických bezpečnostních incidentů je dokumentováno.

2.2.1.2.12 NP076-Řízení kontinuity činností (VoKB § 14)

odst. 1 a):

Jsou stanoveny práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role.

Jsou stanoveny cíle řízení kontinuity činností formou určení:

- odst. 1 b) 1.: Minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
- odst. 1 b) 2.: Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
- odst. 1 b) 3.: Doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.
- odst. 1 c): Je stanovena strategie řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).

2.2.1.2.13 NP077-Kontrola a audit kybernetické bezpečnosti (VoKB § 15)

odst. 1 a):

Je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a VIS a určena opatření pro jeho prosazování.

odst. 1 b):

Jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

2.2.1.3 Technická opatření

2.2.1.3.1 NP078-Fyzická bezpečnost (VoKB § 16)

odst. 1 a):

Jsou přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

odst. 1 b):

Jsou přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

odst. 1 c):

Je předcházeno poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

2.2.1.3.2 NP079-Nástroj pro ochranu integrity komunikačních sítí (VoKB § 17)

Pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, je zavedeno(a):

- odst. 1 a): Řízení bezpečného přístupu mezi vnější a vnitřní sítí.
- odst. 1 b): Segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.
- odst. 1 c): Použití kryptografických prostředků (Kryptografické prostředky (VoKB § 25)) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií.
- odst. 1 d): Opatření pro odstranění nebo blokování přenášených dat, která neodpovídají požadavkům na ochranu integrity komunikační sítě.

2.2.1.3.3 NP080-Nástroj pro ověřování identity uživatelů (VoKB § 18)

odst. 1.:

Jsou používány nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.



Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje:

- odst. 3 a): Minimální délku hesla osm znaků.
- odst. 3 b): Minimální složitost hesla tak, že heslo bude obsahovat alespoň tři z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3.
- odst. 3 c): Maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.
- odst. 5: Nástroj pro ověřování identity uživatelů je zajištěn jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti hesla.

2.2.1.3.4 NP081-Nástroj pro řízení přístupových oprávnění (VoKB § 19)

Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění:

- odst. 1 a): Pro přístup k jednotlivým aplikacím a datům.
- odst. 1 b): Pro čtení dat, pro zápis dat a pro změnu oprávnění.

2.2.1.3.5 NP082-Nástroj pro ochranu před škodlivým kódem (VoKB § 20)

Pro řízení rizik spojených s působením škodlivého kódu je používán nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu:

- odst. 1 b): Serverů a sdílených datových úložišť.
- odst. 1 c): Pracovních stanic. Tato část požadavku může být zajištěna organizačně, např. formulací podmínek užití systému a splnění této povinnosti tak přeneseno na uživatele.

Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.

2.2.1.3.6 NP083-Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VoKB § 21)

Je používán nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajišťuje:



- odst. 1 a): 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.
- odst. 1 b): Ochranu získaných informací před neoprávněným čtením nebo změnou.

Pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému je zaznamenáváno(y):

- odst. 2 b): Činnosti provedené administrátory.
- odst. 2 c): Činnosti vedoucí ke změně přístupových oprávnění.
- odst. 2 d): Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů.
- odst. 2 e): Zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.
- odst. 2 f): Automatická varovná nebo chybová hlášení technických aktiv.
- odst. 2 g): Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností.

odst. 4:

Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

2.2.1.3.7 NP084-Nástroj pro detekci kybernetických bezpečnostních událostí (VoKB § 22)

odst. 1:

Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.

2.2.1.3.8 NP085-Aplikační bezpečnost (VoKB § 24)

odst. 1:

Jsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.



2.2.1.3.9 NP086-Kryptografické prostředky (VoKB § 25)

Pro používání kryptografické ochrany je(jsou) stanovena:

- odst. 1 a) 1.: Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.
- odst. 1 a) 2.: Pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat.
- odst. 1 b): V souladu s bezpečnostními potřebami a výsledky hodnocení rizik jsou používány kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.

2.2.1.3.10 NP087-Nástroj pro zajišťování úrovně dostupnosti (VoKB § 26)

odst. 1:

V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je používán nástroj pro zajišťování úrovně dostupnosti informací.

2.2.2 Výkon

2.2.2.1 NP048- Kapacita

Počty uživatelů, požadavků a uživatelských spojení jsou pro jednotlivé systémy odhadovány následovně.

e-Sbírka - Uživatelé

celkem:

- 7,5 milionu uživatelů

průměrně:

- 3 nové uživatelské spojení za sekundu
- 150 otevřených požadavků
- 3 stránky za vteřinu (denní průměr)

špičkově:

- 60 nových uživatelských spojení za sekundu
- 1500 otevřených požadavků
- 60 stránek za vteřinu (běžná denní špička)

e-Sbírka - Databáze

Špičková hodnota dotazovacích služeb: 60 dotazů/s



e-Legislativa - Uživatelé

celkem:

- 4000 uživatelů

průměrně:

- 2 nové uživatelské spojení za sekundu
- 200 otevřených požadavků

špičkově:

- 20 nových uživatelských spojení za sekundu
- 1000 otevřených požadavků

e-Legislativa - Databáze

Špičková hodnota dotazovacích služeb: 130 dotazů/s

2.2.2.2 NP049- Rezervace výkonu pro dohledové a bezpečnostní nástroje

V každém datovém centru musí být vyhrazeny dva virtuální servery pro provoz dohledových a bezpečnostních nástrojů CMS a DCeGOV, a to nejméně o následující kapacitě a specifikacích:

- vCPU: 4x
- RAM: 32 GB
- Disk 1 (OS): 80 GB
- Disk 2 (Data): 80 GB

Tyto virtuální servery musí být v rámci datového centra provozovány v režimu vysoké dostupnosti na úrovni Virtualizace tak, aby provozovaný hostitelský HW byl alespoň ve formátu N+1 (tedy aby hostitelský HW byl alespoň ze dvou serverů).

Virtualizační technologie pro tyto servery musí být jedna z následujících:

- Redhat
- VMware
- Hyper-V

2.2.3 Provoz a infrastruktura

2.2.3.1 NP043- Klíčové parametry úrovně služeb (SLA)

Systém musí být možné provozovat s nastavením úrovně služeb (SLA) dle níže uvedených parametrů.

RTO = 4 hodiny (včetně obnovy při ztrátě či poškození dat)

RPO = 10 minut s chráněním proti rizikům:

- výpadku či ztrátě jednoho datového centra
- uživatelskému, administrátorskému či aplikačnímu (způsobené SW chybou) poškození či ztrátě databází

Navíc systém musí garantovat nulovou ztrátu dat vyhlášených eLegislativou do eSbírky (vzhledem k výše uvedeným rizikům).

V případě, že dojde k výpadku systému včetně ztráty nebo poškození dat a systém je obnoven se starší verzí dat, musí tlustý klient eŠablony pro plusovou osu nabídnout uživateli k zpracování fragmenty obsahu, které byly do centrálního systému odeslány, avšak obnovou dat byly ztraceny. Tato funkce musí být schopná nabídnout obnovou takových fragmentů minimálně po dobu definovanou parametrem RPO.

2.2.3.2 NP044- Klientské platformy

Části systému běžící na pracovní stanici uživatele (tlustý klient) musí být provozovatelné na následujících OS:

- Windows 7 a novější
- OS X 10.x a novější, který je podporován výrobcem OS

Části systému běžící v internetovém prohlížeči uživatele (tenký klient) musí být provozovatelné v následujících prohlížečích: Internet Explorer, Edge, Firefox, Chrome, Safari či jejich nástupci ve verzích podporovaných výrobcí prohlížečů.

2.2.4 Dokumentace

2.2.4.1 NP090-Dokumentace detailní analýzy

Dokumentace v následujícím rozsahu:

- Analýza a návrh řešení
- Návrh datového modelu
- Návrh uživatelského rozhraní
- Detailní návrh integrace
- Aktualizace procesů dle aktuálního stavu pravidel upravujících legislativní proces
- Detailní metodika digitalizace včetně tezauru CzechVoc a modulu EUR-Lex
- Návrh HW, SW
- Návrh akceptačních scénářů (smluvní)
- Rámcový návrh testovacích scénářů

2.2.4.2 NP091-Architektonická a technická dokumentace

Dokument(y) obsahující skutečnou technickou architekturu systému a jeho komponent, zejména z pohledu:

- Klíčových architektonických a technických principů a postupů použitých v rámci systému
- Komponenty systému
- Integrace
- Síťová úroveň systému
- Fyzický datový model
- Interní API systému
- Externí API systému (ve formátu použitelném pro zveřejnění)

2.2.4.3 NP092-Provozní a instalační dokumentace

Dokument(y) obsahující:

- Způsob nasazení systému do jednotlivých prostředí, použité konfigurační parametry
- Instalační manuály
- Operační a provozní postupy systému, včetně proaktivních a hlavních reaktivních postupů technického provozovatele
- Podklady pro provoz podpory na úrovni 1 a 2
- Školící materiály pro technické správce systému (úroveň 1 a 2)

2.2.4.4 NP093-Uživatelská dokumentace

Dokument(y) popisující funkcionality systému z uživatelského pohledu.

2.2.4.5 NP094-Projektová dokumentace

Dokument(y) zahrnující následující oblasti:

- Kontaktní a komunikační matice projektu
- Detailní časový harmonogram projektu
- Proces řízení rizik s ohledem na Bezpečností dokumentaci
- Plán řízení kvality

Podklady pro interní projektovou dokumentaci:

- Presentace
- Závěrečné vyhodnocení realizace projektu
- Poučení z projektu
- Závěrečné vyhodnocení záměru a vynaložených prostředků

Dále pak periodickou projektovou dokumentaci:

- Záписy z jednotlivých jednání
- Pravidelná zpráva o stavu projektu

2.2.4.6 NP095-Bezpečnostní dokumentace

Dokument(y) zahrnující následující oblasti:

- Bezpečnostní politika
- Strategie řízení kontinuity činností IS
- Bezpečnostní směrnice pro činnost bezpečnostního správce systému
- Hodnocení rizik dle Přílohy č. 2 k vyhlášce č. 316/2014 Sb.

2.2.4.7 NP096-Vývojová dokumentace

Dokumentace zdrojového kódu částí systému, které vznikly vlastním vývojem.

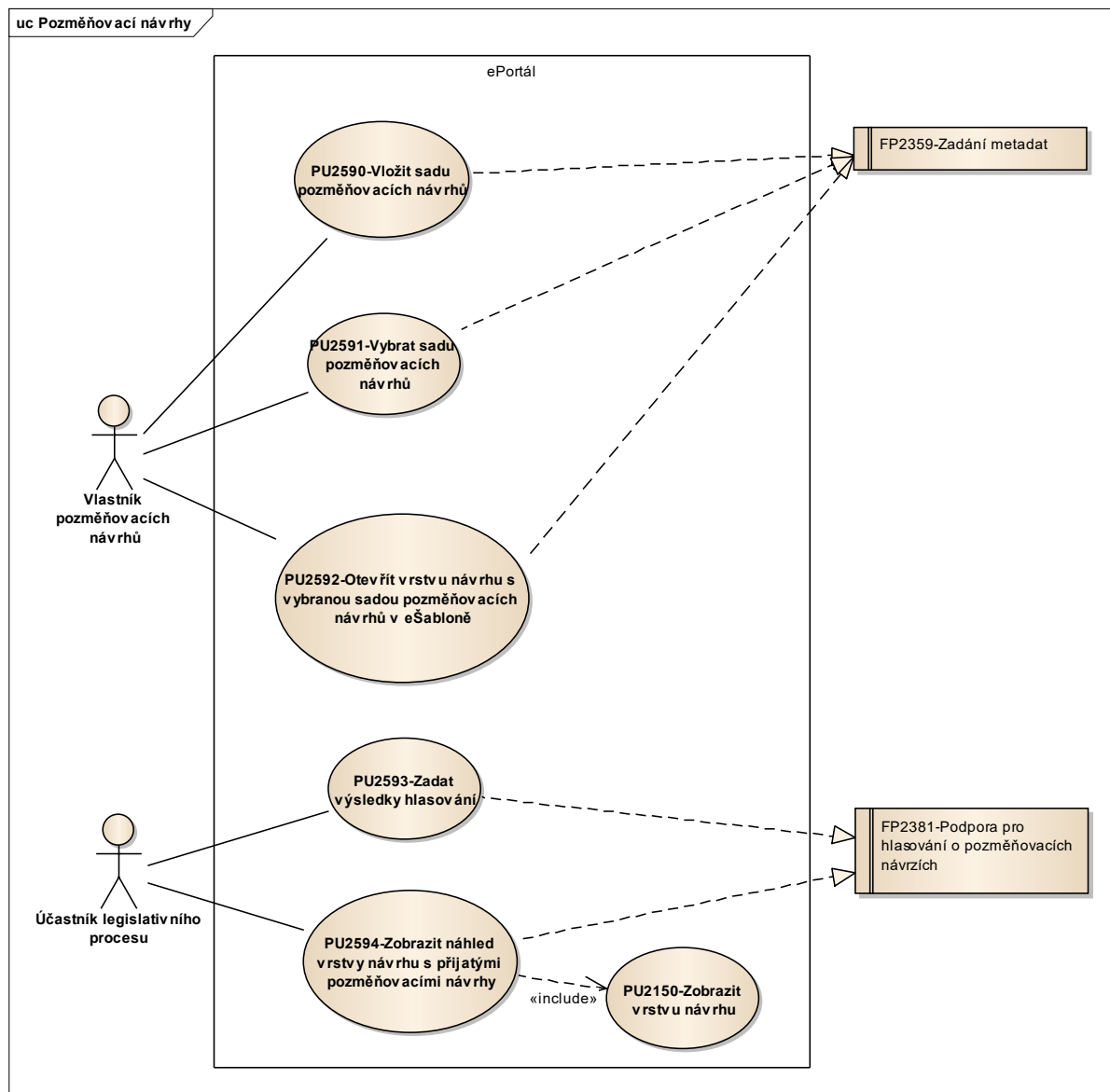
Dokumentace klíčových principů vývoje aplikace, které jsou specifické pro systém.

3 Případy užití

3.1 Portál e-Legislativa

3.1.1 Prostory připomínek a pozměňovacích návrhů

3.1.1.1 Pozměňovací návrhy



POZNÁMKA: Některé případy užití jsou popsány již v hlavním dokumentu Detailní návrh.

3.1.1.1.1 PU2593-Zadat výsledky hlasování

Účel: Uživatel může zadat výsledek hlasování o pozměňovacím návrhu (zda byl přijat), a to v rámci celého prostoru i v rámci sad pozměňovacích návrhů - tak, aby bylo možné odlišit například hlasování na výborech a hlasování na plénu Sněmovny či Senátu.

Realizované požadavky		
FP2381-Podpora pro hlasování o pozměňovacích návrzích		
Předpoklady		
Vybraný prostor pozměňovacích návrhů nebo vybraná sada pozměňovacích návrhů v prostoru pozměňovacích návrhů.		
Scénáře		
Název	Zadat výsledky hlasování	
Typ	Základní scénář	
krok	typ	akce
1	Uživatel	Uživatel v rámci sady pozměňovacích návrhů nebo prostoru zvolí možnost "Zadat výsledky hlasování".
2	Systém	Systém zobrazí pozměňovací návrhy příslušné sady pozměňovacích návrhů nebo prostoru.
3	Uživatel	Uživatel si zvolí pozměňovací návrh a zadá, zda byl přijat (či ne).
4	Systém	Systém zaznamenává pro sadu pozměňovacích návrhů nebo prostor, které pozměňovací návrhy byly přijaty a v jakém pořadí.

3.1.1.1.2 PU2594-Zobrazit náhled vrstvy návrhu s přijatými pozměňovacími návrhy

Účel: Zobrazit aktuální obsah návrhu ve znění přijatých pozměňovacích návrhů v rámci hlasování výborů, komisí a celých schůzí Poslanecké sněmovny a Senátu tak, aby měl uživatel (např. poslanec nebo senátor) přehled o aktuálním obsahu návrhu v pro rozhodování v hlasování o následujících pozměňovacích návrzích.



Realizované požadavky		
FP2381-Podpora pro hlasování o pozměňovacích návrzích		
Předpoklady		
Vybraný prostor pozměňovacích návrhů nebo vybraná sada pozměňovacích návrhů v prostoru pozměňovacích návrhů.		
Stav po ukončení		
Zobrazená vrstva návrhu se zapracovanými pozměňovacími návrhy, které byly přijaty hlasováním v rámci příslušné sady pozměňovacích návrhů nebo prostoru.		
Scénáře		
Název	Zobrazit náhled s přijatými pozměňovacími návrhy	
Typ	Základní scénář	
krok	typ	akce
1	Uživatel	Uživatel v rámci sady pozměňovacích návrhů nebo prostoru zvolí možnost "Zobrazit náhled vrstvy návrhu s přijatými pozměňovacími návrhy".
2	Systém	Systém vygeneruje dočasnou vrstvu návrhu se zapracovanými pozměňovacími návrhy, které byly přijaty hlasováním v rámci příslušné sady pozměňovacích návrhů nebo prostoru. Zapracovávání kolizí systém řeší pomocí variantních fragmentů.
3	Systém	Systém zobrazí vygenerovanou vrstvu návrhu.



4 Model komponent a implementace

Model komponent a implementace není tímto dodatkem měněn.

5 Model nasazení a provozu

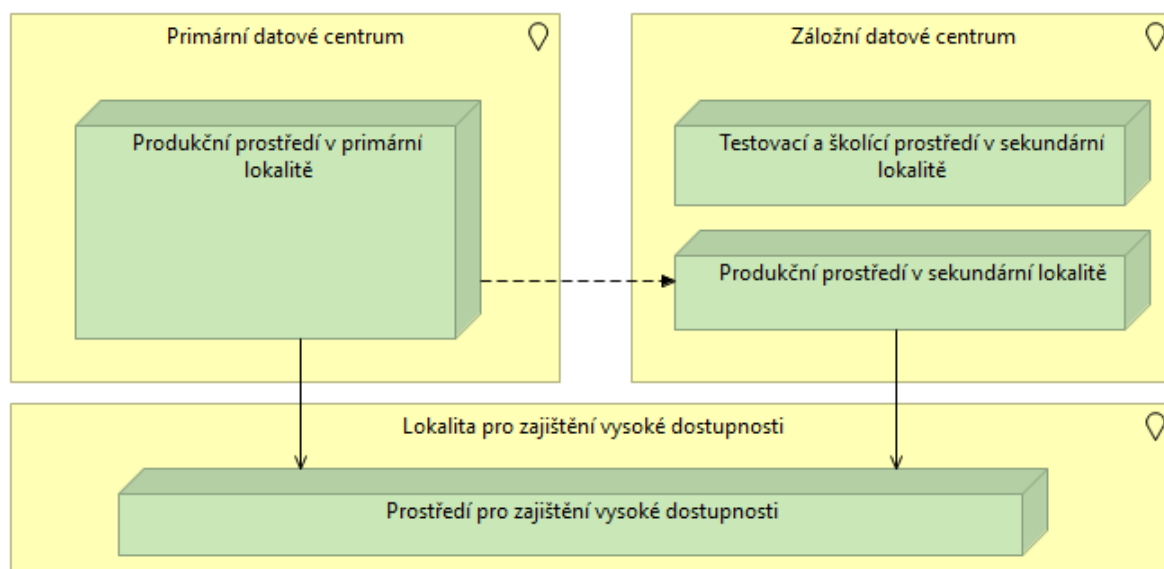
5.1 Základní architektura řešení v oblasti nasazení a provozu

Model nasazení a model provozu systémů e-Sbírka a e-Legislativa. Model nasazení popisuje fyzické nasazení systémů e-Sbírka a e-Legislativa v datových centrech.

Tato kapitola popisuje základní koncepční principy, kterými se bude nasazení a provoz informačního systému řídit, přičemž bude následně na dodavateli informačního systému definovat konkrétní použití ať už HW nebo SW technologie jakož i způsob jejich použití pro dosažení účelu informačního systému za dodržení požadovaných parametrů nebo zákonných předpokladů definovaných zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a zákonem č. 365/2000 Sb. o IS státní správy.

5.1.1 Provozní prostředí a lokality

Umístění systémů e-Sbírka a e-Legislativa do datových center je znázorněno na následujícím obrázku:



Obrázek 1: Provozní prostředí a lokality

Umístění informačních systémů je navrženo ve dvou různých datových centrech (lokality):

- Primární datové centrum
- Záložní (sekundární) datové centrum

Pro potřeby zajištění vysoké dostupnosti se předpokládá použití i třetí lokality (tzv. třetí komunikační lokalita), která bude zajišťovat právě funkci vysoké dostupnosti. Tato infrastruktura bude umístěna v prostředí CMS/DCeGov.

V rámci těchto datových center jsou navrženy 3 prostředí pro nasazení informačních systémů:

- produkční (provozní) prostředí v primární lokalitě,
- záložní produkční (provozní) v sekundární lokalitě,
- testovací (a školicí) prostředí v sekundární lokalitě,

Příčemž je potřeba z důvodů zajištění vysoké dostupnosti systému provozovaných v primárním a záložním datovém centru nasadit i další prostředí v nezávislé lokalitě: prostředí pro zajištění vysoké dostupnosti (třetí komunikační lokalita).

5.1.1.1 Datová centra

V současnosti není rozhodnuto konkrétní umístění jednotlivých prostředí. Možností umístění je několik. Každý z variant umístění však předpokládá konektivitu do CMS (Centrální místo služeb). Popis služeb poskytovaných CMS je uvedený v podkapitole **6.1 Příloha č. 1** - Specifikace služeb CMS.

Návrh počítá se dvěma geograficky oddělenými datovými centry. Mezi primárním a záložním datovým centrem bude dostatečná síťová kapacita pro zajištění realizace scénáře zotavení po havárii tak, aby byly dodrženy požadované parametry RTO a RPO. Podle potřeby bude mezi těmito datovými centry možné zřídit dedikované linky s parametry až 2x10 Gb/s s latencí do 10 ms, jitter/stabilitou do 5 ms, a to ve vysoké dostupnosti s SLA 99,9%, případně linky fibre channel až do 8 Gb/s.

V každém z datových center budou pro infrastrukturu vyhrazeny rackové stojany 19", 42U s garantovaným příkonem 10 kW / rack včetně doporučené kapacity chlazení, v počtu 2-4 RACKy v každém datovém centru.

Hraniční síťové prvky s podporou síťové vrstvy L3 nejsou pro nasazení systémů v datových centrech k dispozici a navrhnout a zajistit je musí dodavatel.

Každá z lokalit má zabezpečenou konektivitu do Centrálního místa služeb (CMS). Primární a sekundární datové centrum bude disponovat konektivitou do CMS s propustností 10 Gb / s.

Datové centrum	Popis
Primární datové centrum	Primární datové centrum bude hostit Produkční prostředí. Primární datové centrum bude hostit také centrum dohledu.

Záložní datové centrum	<p>Záložní datové centrum je geograficky oddělené datové centrum, ve kterém bude provozována infrastruktura záložního produkčního prostředí. Cílem geograficky odděleného záložního prostředí je zajistit vysokou dostupnost řešení a odolnost proti katastrofám.</p> <p>Záložní datové centrum bude také hostit i testovací a školící prostředí, které bude mít stejnou HW a SW architekturu jako produkční prostředí s výjimkou technologií umožňujících přepnutí provozu z produkčního do záložního prostředí.</p>
Lokalita pro zajištění vysoké dostupnosti	<p>Lokalita pro zajištění vysoké dostupnosti bude hostit prostředí pro zajištění vysoké dostupnosti. Jedná se o zabezpečení tzv. Witness pro zjištění nedostupnosti prostředí a umožnění jeho failoveru (řešení situací typu split-brain apod.). Bude zajištěna nezávislá síťová konektivita do primárního i záložního datového centra.</p> <p>Toto prostředí bude nasazeno v CMS centru jakožto nezávislé lokalitě s přístupem do obou prostředí systému eSbírka a eLegislativa.</p>

5.1.1.2 Prostředí

Informační systém je rozvržen do čtyř prostředí. Jedná se primárně o produkční prostředí a záložní produkční prostředí, které jsou nasazeny v geograficky oddělených lokalitách. Následně se jedná o prostředí testovací a školící a třetí komunikační lokalitu pro zajištění vysoké dostupnosti řešení.

Prostředí	Popis
Produkční prostředí	Produkční prostředí je primárním prostředím pro běh informačních systémů e-Sbírka a e-Legislativa. Veškerá komunikace okolního světa do systémů e-Sbírka a e-Legislativa bude primárně směřována do tohoto produkčního prostředí.
Záložní prostředí	Failover prostředí, které zajišťuje vysokou dostupnost řešení a odolnost proti katastrofám. V průběhu normálního provozu informačních systémů bude komunikace mezi aktéry a informačními systémy směřována do primárního produkčního prostředí. V případě jeho výpadku bude tato komunikace přesměrována do záložního produkčního prostředí.
Testovací a školící prostředí	Prostředí nasazené v záložním datovém centru, které bude mít vlastní infrastrukturu, avšak architektonicky shodnou HW infrastrukturu s primárním produkčním prostředím s výjimkou technologií umožňujících přepnutí provozu z produkčního do záložního prostředí.
Třetí komunikační lokalita	Prostředí plní funkci tzv. Witness pro zabezpečení vysoké dostupnosti SW či HW komponent řešení (řešení situací typu split-brain apod.).

5.1.2 Služby zajišťované CMS a DCeGOV v souladu s ZoKB a VoKB

V souladu s ZoKB a VoKB zajišťuje CMS a DCeGOV následující služby, a to včetně zajištění licencí uvedených systémů:

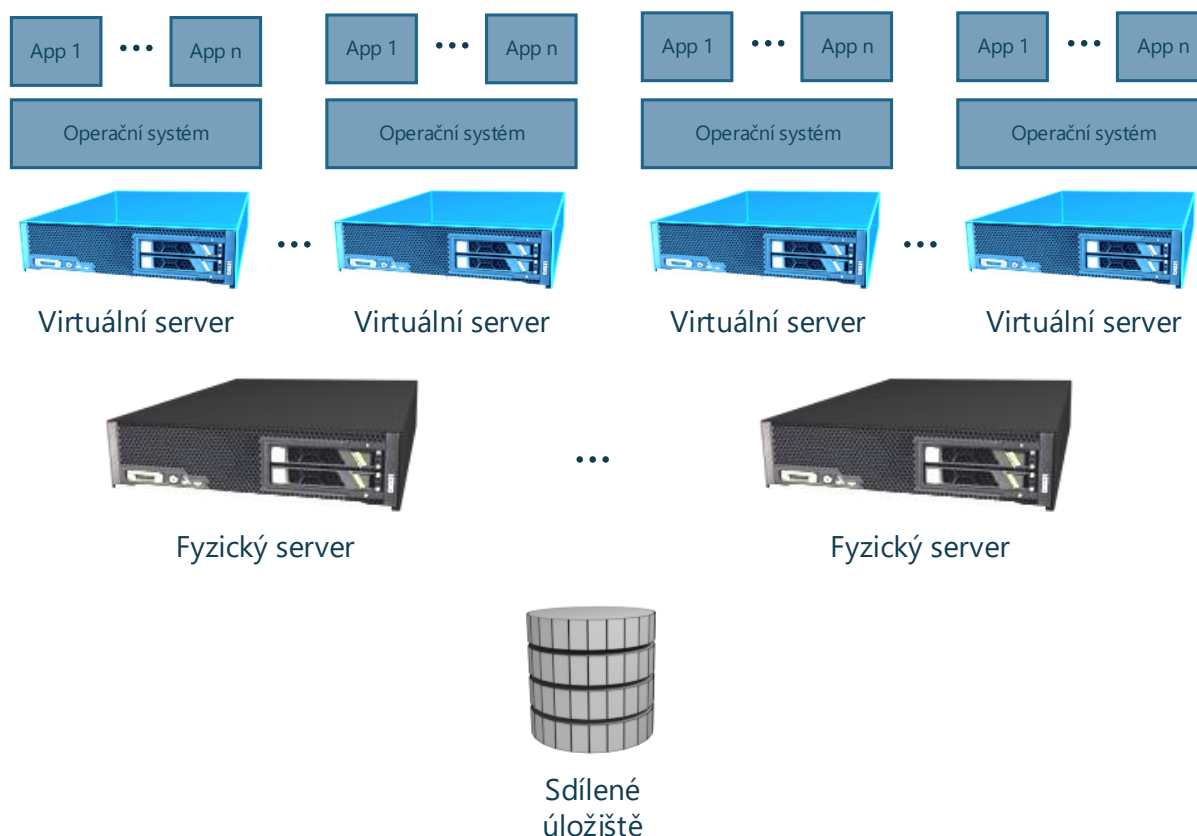
Vyhláška MV č.316/2014 Sb., o kybernetické bezpečnosti		DCeGOV/CMS
§ 17 odst 1, písmeno	a) bezpečný přístup mezi vnější a vnitřní sítí	Netflow - HoneyPot a AntiDDOS - pouze pro 1 perimetr, Vulnerability management - multilicence i pro ostatní projekty, Firewall, IDS/IPS
	b) demilitarizovaná zóna	
	c) používání kryptografických prostředků pro vzdálený přístup	
	d) odstranění a blokování dat	
§ 17 odst. 2	nástroje pro ochranu integrity vnitřní sítě	PIM/PAM 2FA pouze pro CMS 2 a odhad pro ostatní projekty
§ 18 odst. 1	požití nástroje pro uvěření identity	
§ 18 odst. 2	nástroje před zahájením činnosti	
§ 18 odst. 3, písmeno	a) minimální délka hesla 8 znaků	
	b) složitost hesla - V-m - 1 - /	
	c) doba výměny hesla max 100 dní	
§ 18 odst. 4. písmeno	a) nástroj proti opětovnému použití stejného hesla	
	b) nástroj pro ověření identity administrátorů	
§ 18 odst. 5	vyšší bezpečnost a odolnost hesla	Vulnerability management, PIM/PAM 2FA
§ 19 odst 1, písmeno	a) přístup k jednotlivým datům	
	b) pro čtení, zápis a změnu oprávnění	
§ 19 odst 2, písmeno	nástroj pro monitoring a záznam oprávnění	Antivirus
§ 20	a) komunikace mezi vnitřní a vnější sítí	
	b) serverů a sdílených datových úložišť	
	c) pracovních stanic	
§ 21 odst. 1 písmeno	a) sběr provozních a bezpečnostních činností	SIEM
	b) ochrana získaných informací před neoprávněným čtením nebo změnou	
§ 21 odst.2, písmeno	a) přihlášení a odhlášení uživatelů a administrátorů	
	b) činnosti provedené administrátory	
	c) činnosti vedoucí ke změně přístupových práv	
	d) neprovedení činností - nedostatečná práva	



	e) zahájení a ukončení technických aktiv	
	f) automatická varování nebo chybová hlášení	
	g) přístupy k záznamům o činnostech	
	h) mechanismy identifikace přihlašovacích údajů	
§ 21 odst. 3	záznam o činnostech je uchován nejméně 3 měsíce	
§ 21 odst. 4	synchronizace technického času 1 x 24 hodin	
§ 22 odst. 1	použití nástroje pro detekci KBU	
§ 22 odst. 2, písmeno	a) v rámci vnitřní sítě	SIEM, HoneyPot, NetFlow, IPS/IDS - součást CMS 2
	b) serverů patřících mezi kritickou infrastrukturu	
§ 23 odst.1 písmeno	a) integrovaný sběr a vyhodnocení KBU	ArcSight Logger a SIEM
	b) poskytování informací	
	c) nepřetržité vyhodnocování KBU a varování	
§ 23 odst.2, písmeno	a) pravidelná aktualizace pravidel pro vyhodnocování KBU	
	b) využívání informací pro optimální nastavení opatření	
§ 24 odst. 1	provádění bezpečnostních testů zranitelnosti	
§ 24 odst. 2, písmeno	a) trvalá ochrana aplikací a informací dostupných z vnější sítě	částečně Vulnerability scanner, vymezit si povinnosti aplikací dodávat události do předepsaných logů
	b) transakcí před jejich dokončením, duplikací, směrováním atd.	
§ 25 odst. 1, písmeno	a) pro použití se stanoví úroveň ochrany s ohledem na typ a sílu algoritmu, pravidla při přenosu informací nebo uložení na mobilních zařízeních	https/ FTP/smtp
	b) zajištění důvěrnosti a integrity předávaných dat a průkaznou identifikaci osoby za provedení činností	Antispam, PIM PAM
§ 26 odst. 1	použití nástroje dostupnosti informací	
§ 26 odst. 2 písmeno	a) zajistí dostupnost KIS a VIS	Vulnerability management
	b) odolnost vůči kybernetickým útokům	

5.1.3 Virtualizovaná serverová infrastruktura

Informační systémy budou nasazeny na virtualizované serverové infrastruktuře. Virtualizovaná serverová infrastruktura bude existovat v každém datovém centru.



Obrázek 2: Virtualizovaná serverová infrastruktura

K nasazování jednotlivých komponent informačních systémů bude použito toto virtualizované serverové prostředí.

5.1.4 Infrastruktura vysoké dostupnosti

Každá klíčová komponenta v infrastruktuře dodávaných informačních systémů musí být navržena ve vysoké dostupnosti jednak na úrovni lokality jako takové a zároveň i na úrovni mezi datovými centry, z důvodu zajištění odolnosti proti výpadkům datových center. Řešení na HW úrovni neobsahuje jedinečné technické prvky, které by v případě výpadku vedly k nedostupnosti celého řešení (tzv. Single point of failure).

Stejně musí být zajištěna i redundance všech klíčových SW prvků. To znamená, že všechny komponenty řešení jsou redundantní a produkční systém je umístěn duplicitně ve více vzdálených lokalitách.

Primárně bude veškerá komunikace s informačním systémem směřována do primárního datového centra. V případě nedostupnosti informačního systému v primární lokalitě bude tato komunikace přesměrována do sekundárního datového centra.

Primárně se jedná o vysokou dostupnost následujících prvků:

- **Fyzické servery** - každý virtuální server virtualizované serverové infrastruktury musí být provozován v clusteru a nasazený na alespoň 2 fyzických serverech.
- **Síťové komponenty** - všechny navrhované servery musí mít dostatečné množství síťových karet, pro umožnění jejich redundantního připojení do datových sítí. Stejně musí být zajištěna redundance směrovačů a dalších prvků síťové infrastruktury. Souhrnné, všechny navržené a dodané komponenty síťové infrastruktury musí být zdvojené, takže v případě výpadku některé komponenty nedojde k selhání celé síťové infrastruktury.
- **Datová pole** - jádrem datové infrastruktury bude dvojice vysoce dostupných datových polí (doporučuje se propojení přes SAN), do kterých budou přistupovat jednotlivé servery, na kterých bude informační systém provozován.
- **Aplikační servery** - aplikační servery budou implementovány jako virtuální servery tak, aby v případě potřeby mohly být provozovány v clusteru zajišťujícím vysokou dostupnost softwarových komponent na nich provozovaných.
- **Centrální datové úložiště** - bude provozováno jako vysoce dostupné databázové řešení na minimálně dvou fyzicky oddělených serverech. Samotná data tohoto databázového řešení budou uložena na vysoce dostupných datových polích.
- **Replikace mezi datovými centry** - implementace informačních systémů musí umožnit replikaci informačního systému mezi jednotlivými datovými centry. Musí se replikovat zejména všechna data systému včetně dat uložených na diskových polích. Minimální požadavek je asynchronní replikace tak, aby byly splněny požadované hodnoty RPO a RTO. Zároveň je nezbytné plně provozovat produkční systém ze záložní lokality, což může dle zvolené technologie znamenat i nutnost replikace virtuálních serverů.

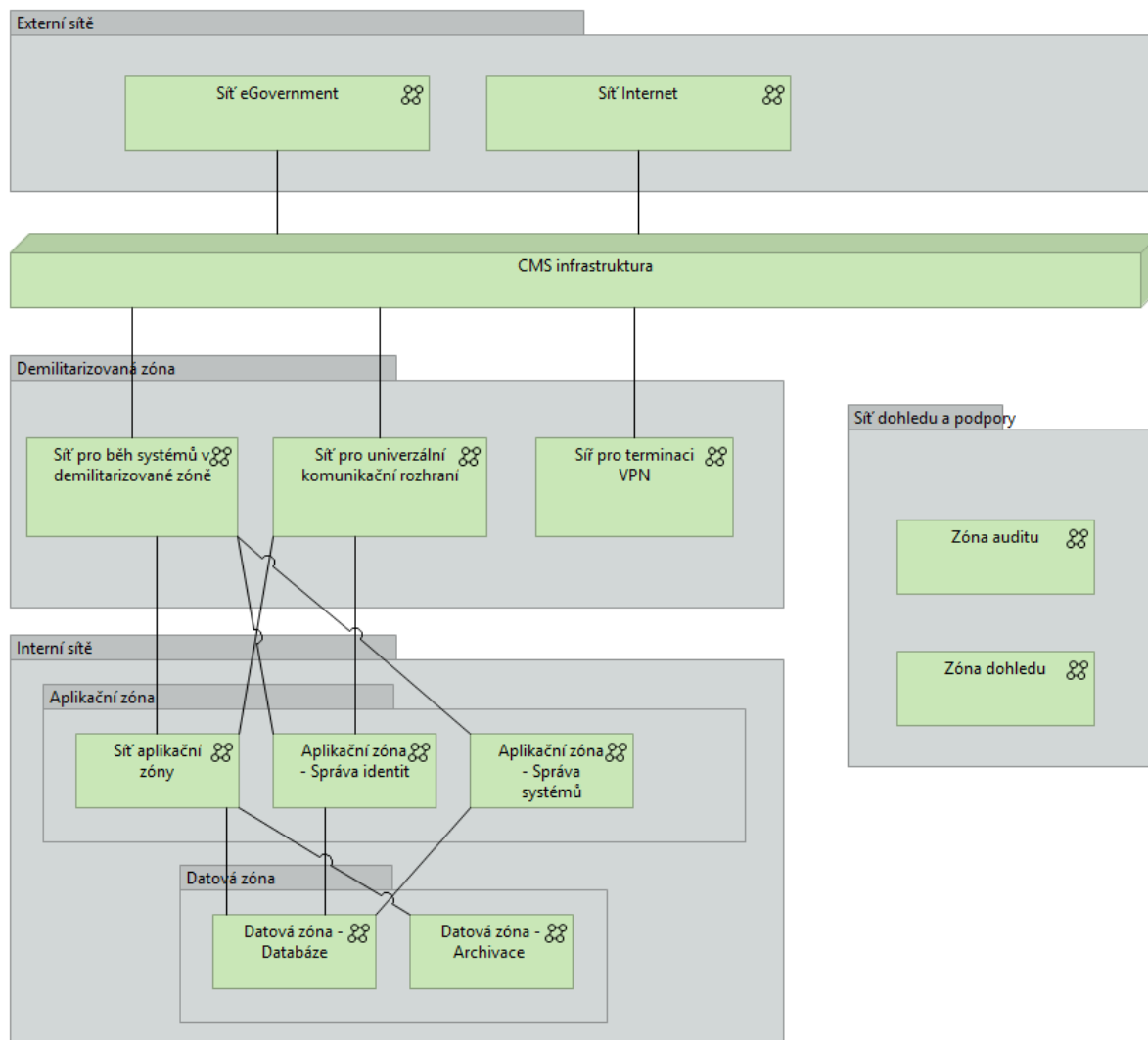
5.1.5 Koncepce síťové infrastruktury

Síťová infrastruktura pro potřeby provozu informačního systému je navržena na logické úrovni. Konkrétní fyzický návrh síťové infrastruktury včetně konkrétních komunikačních prvků se očekává od dodavatele řešení po vyřešení umístění informačního systému se zřetelí na navržené technické řešení

Síťová infrastruktura musí být řešena v souladu s infrastrukturou serverů a musí být zajištěna její vysoká dostupnost. Všechna navrhovaná síťová zařízení musí být zdvojená a nastavená tak, aby i v případě výpadku některého z nich nebyla narušena funkčnost informačního systému.

Princip návrhu síťové infrastruktury je její rozdělení do zón. Taková vícevrstvá síťová architektura umožní jasnou definici umístění komponenty aplikační infrastruktury do odpovídající zóny a jasnou definici pravidel pro komunikaci mezi jednotlivými vrstvami síťové architektury (zónami).

Základní koncepce síťové infrastruktury je na následujícím obrázku:



Obrázek 3: Síťová infrastruktura

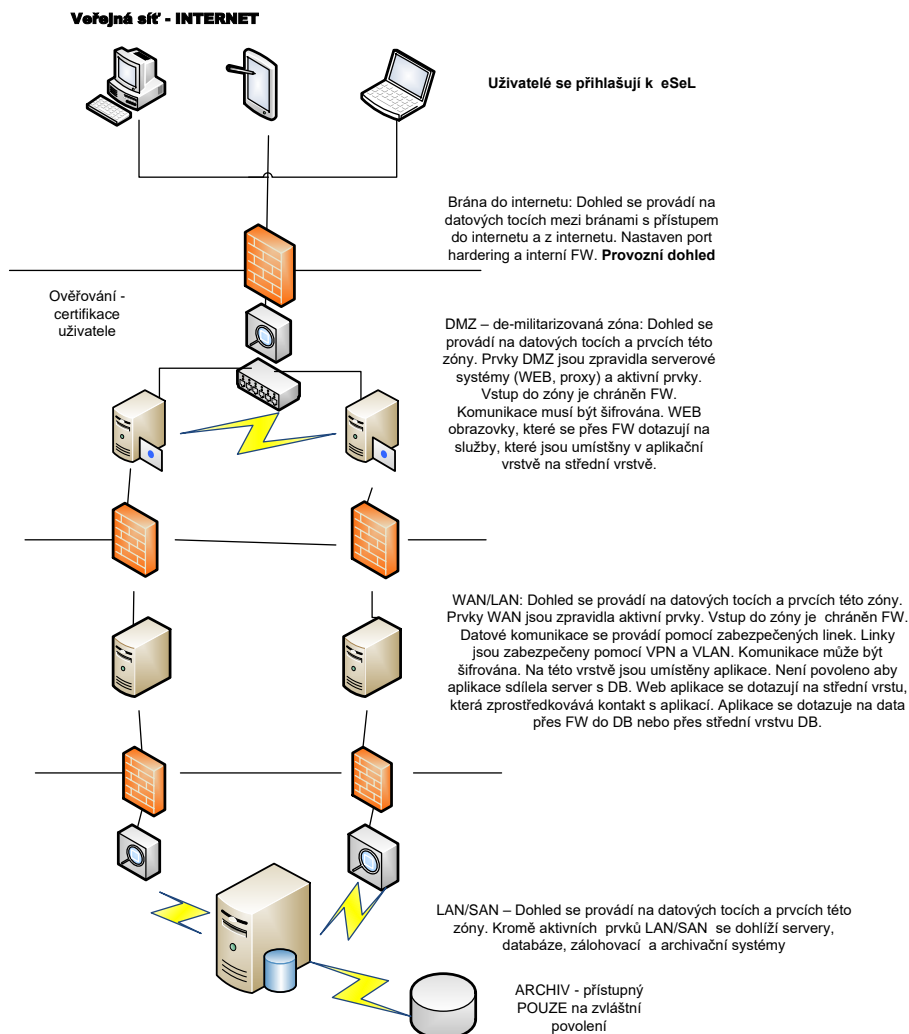
Následující tabulka popisuje jednotlivé zóny:

Zóna	Popis
Externí síť	Jedná se o nechráněné externí síť, které nejsou v gesci provozovatele řešení. Všechny služby vystaveného informačního systému, které jsou viditelné do této zóny, budou striktně dodržovat standardy vycházející s příslušných RFC dokumentů a ostatních standardů.

Externí sítě zahrnují:	
<ul style="list-style-type: none">• Sít' eGovernment• Sít' Internet - všechny ostatní externí sítě	
CMS	Centrální místo služeb. Centrální místo služeb zprostředkovává veškerou komunikaci mezi systémem eSbírka a eLegislativa a okolitým světem. CMS navíc může zabezpečit veškerý monitoring prostředí, jak je uvedeno níže.
Demilitarizovaná zóna	Bezpečnostní překážka mezi vnitřní sítí a okolním světem. Přístup do této zóny je umožněn pouze vybraným protokolem a je chráněn jak z interní tak z externí zóny. Jakákoliv komunikace z externí sítě bude ukončena v této zóně a následně transformována a přesměrována do interní sítě.
Interní sítě	V interních sítích jsou umístěny důvěryhodné prvky informačních systémů. Interní sítě jsou rozděleny do dvou zón – Aplikační zóna a Databázová zóna
Sítě dohledu a podpory	Speciální sít' pro potřeby dohledu a podpory řešení.

5.1.5.1 Sítová architektura s hlediska bezpečnosti a dohledu

Koncepce je znázorněna na následujícím obrázku.



Obrázek 4: Síťová architektura

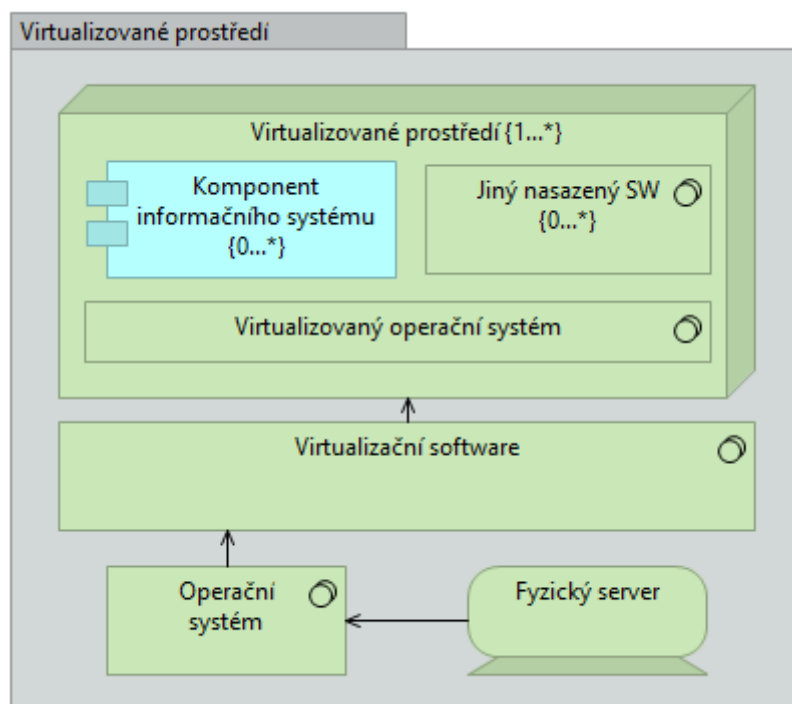
Dohled nad celou infrastrukturou bude implementován v prostředí CMS a následující tabulka ilustruje detaily dohledu:



Vrstva	Router	Ochranná vrstva perimetru	DMZ	Ochranná vrstva perimetru2	Aplikační	Ochranná vrstva perimetru3	Databazová
Prvky	Border router - připojení k ISP	FW (HW a SW)	P	FW		FW	
Režim provozu	24x7	24x7	24x7	24x7	24x7	24x7	24x7
Zálohování	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Archivace	Ne	Ne	Ne	Ne	Ne	Ne	Ne
SLA	Ano	Ano	Ano	Ano	Ano	Ano	Ano
PIM	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Segmenty	N/A	N/A	Veřejný/Interní		Zabezpečení		Silně zabezpečený
Dohled	Brána do internetu: Dohled se provádí na datových tocích mezi bránami s přístupem do internetu a z internetu. Nastaven port hardering a interní FW. Provozní dohled	Ano	DMZ – de-militarizovaná zóna: Dohled se provádí na datových tocích a prvcích této zóny. Prvky DMZ jsou zpravidla serverové systémy (WEB, proxy) a aktivní prvky. Vstup do zóny je chráněn FW. Komunikace musí být šifrována. WEB obrazovky, které se přes FW dotazují na služby, které jsou umístěny v aplikační vrstvě na střední vrstvě.		WAN/LAN: Dohled se provádí na datových tocích a prvcích této zóny. Prvky WAN jsou zpravidla aktivní prvky. Vstup do zóny je chráněn FW. Datové komunikace se provádí pomocí zabezpečených linek. Linky jsou zabezpečeny pomocí VPN a VLAN. Komunikace může být šifrována. Na této vrstvě jsou umístěny aplikace. Není povoleno aby aplikace sdílela server s DB. Web aplikace se dotazují na střední vrstvu, která zprostředkovává kontakt s aplikací. Aplikace se dotazuje na data přes FW do DB nebo přes střední vrstvu DB.		LAN/SAN – Dohled se provádí na datových tocích a prvcích této zóny. Kromě aktivních prvků LAN/SAN se dohlíží servery, databáze, zálohovací a archivační systémy
Nástroje bezpečního dohledu	Logování z: HoneyPot - slouží k identifikaci hackerů AntiDDOS - slouží k ochraně proti DDOS útokům Border router nastaven interní FW IPS/IDS - slouží k identifikaci pokusů o průnik do perimetru	Logování z: FW farmy	IRON Porty - Antimalware, HoneyPot IPS/IDS NetFlow ArcSight Log management		IRON Porty - Antimalware, HoneyPot IPS/IDS NetFlow ArcSight Log management		NetFlow ArcSight Log management
Vyhodnocovací nástroje bezpečnostního dohledu	SIEM, Vulnerability scanner	SIEM, Vulnerability scanner	SIEM, Vulnerability scanner, PIM, 2FA, Certifikáty		SIEM, Vulnerability scanner, PIM, 2FA, Certifikáty		SIEM, Vulnerability scanner, PAM, 2FA, Certifikáty
Nástroje provozního dohledu	SCOM, HP NNMI, HP BSM	SCOM, HP NNMI, HP BSM	SCOM, HP NNMI, HP BSM		SCOM, HP NNMI, HP BSM		SCOM, HP NNMI, HP BSM

5.1.6 Prostředí pro provoz systému

Pro provoz systémů je použita virtualizovaná serverová infrastruktura. Každé navržené prostředí je navrženo pro běh na samostatných virtuálních instancích serverů. V případě potřeby budou jednotlivé prostředí implementovány v režimu vysoké dostupnosti (v clusteru). Schematické znázornění prostředí, včetně virtualizované infrastruktury pro jeho provoz, je na následujícím obrázku.



Obrázek 4: Virtualizované prostředí

5.1.6.1 Šablony prostředí pro provoz systému

Každé prostředí je definováno svou šablonou, která definuje způsob použití prostředí a jeho základní parametry. Pro informační systémy e-Sbírka a e-Legislativa jsou navrženy následující šablony prostředí.

Prostředí	Popis
Prostředí pro provoz aplikací	Virtualizované prostředí, ve kterém budou provozovány aplikační komponenty řešení.
Prostředí pro centrální datové úložiště	Virtualizované prostředí pro provoz řešení pro centrální datové úložiště.

Prostředí pro provoz databázového řešení Virtualizované prostředí pro provoz databázových řešení, které budou zpracovávat údaje které je nevhodné nebo nemožné zpracovávat v rámci centrálního datového úložiště.

Prostředí pro VPN Prostředí pro ukončení připojení VPN. Alternativně může být toto prostředí implementováno odpovídající HW infrastrukturou.

Každé prostředí založené na některé z těchto šablon je navrženo pro provoz na virtualizované serverové infrastruktuře. V případě potřeby budou tato prostředí nasazena redundantně tak, aby byla zajištěna vysoká dostupnost komponenty / prostředí v rámci datového centra.

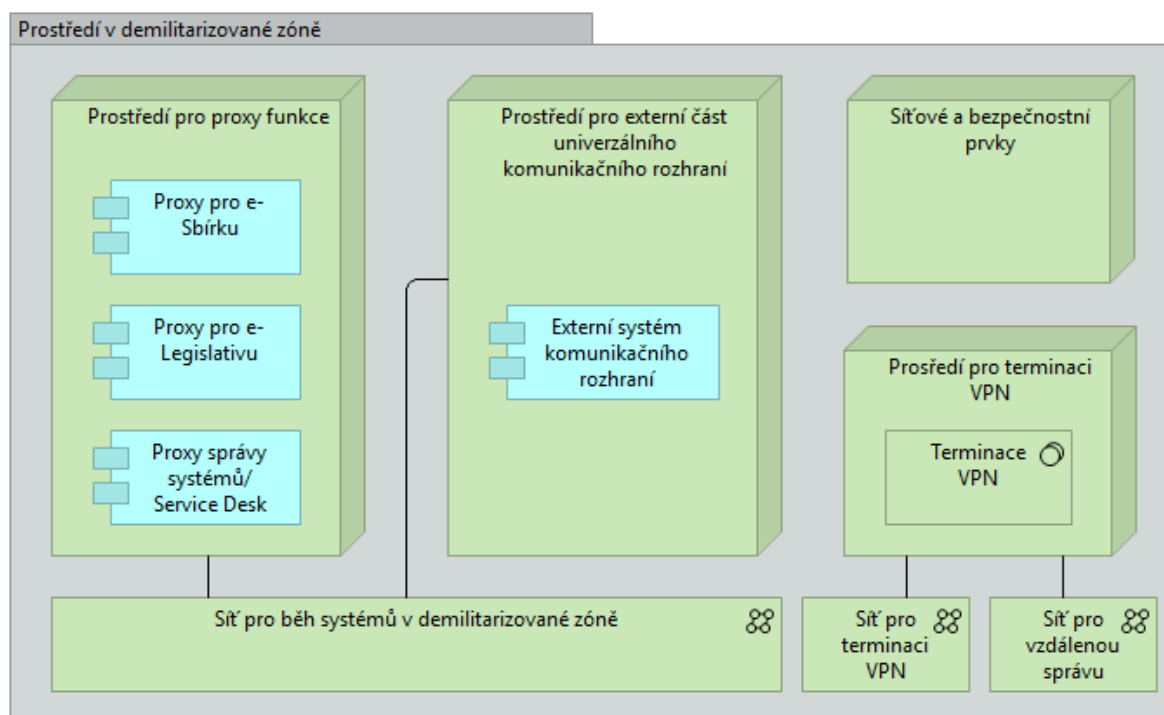
Stejně se v návrhu počítá se zajištěním fail-over řešení mezi jednotlivými datovými centry tak, aby v případě výpadku jednoho datového centra byl provoz přesměrován do záložního datového centra (pouze pro produkční prostředí).

5.1.6.2 Prostředí pro provoz systému v demilitarizované zóně

Demilitarizovaná zóna (DMZ) je zóna v datovém centru, v níž je ukončena komunikace z veřejných sítí. Tato komunikace je ukončena na prostředích v DMZ, následně přeložena a jiným komunikačním kanálem s použitím povolených protokolů odeslána do interní zóny.

V DMZ je navrženo několik prostředí, které jsou jediným bodem interakce mezi nezajištěnými sítěmi a informačním systémem.

Logický pohled na prostředí nasazený v demilitarizované zóně je na následujícím obrázku.



Obrázek 5: Prostředí v demilitarizované zóně

Následující tabulka ukazuje popis jednotlivých prostředí.

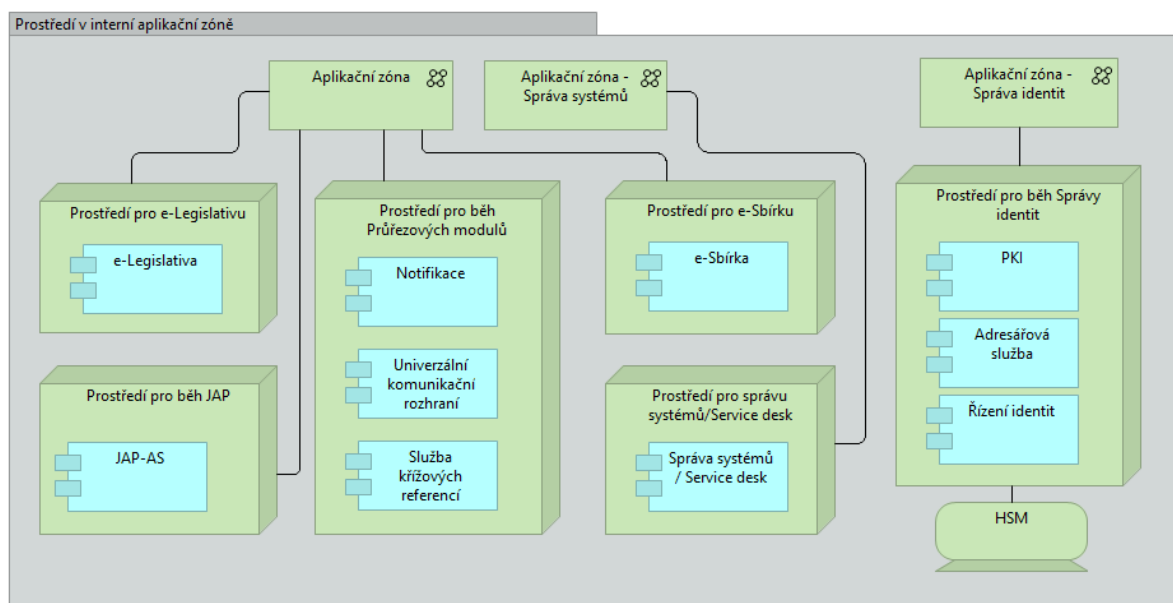
Prostředí	Popis
Prostředí pro proxy funkce	<p>Prostředí odvozené od šablony prostředí pro běh aplikací. Slouží na přeměření dotazů uživatelů systémů e-Sbírka a e-Legislativa. Komunikaci veřejných sítí ukončuje a následně tuto komunikaci přeposílá na zpracování do interní zóny. Prostředí může být zabezpečeno na úrovni síťových a bezpečnostních prvků nasazených v DMZ, které zabezpečí pouze „tunelování“ přicházejícího dotazu z externích sítí do prostředí v aplikační interní zóně. V případě návrhu informačního systému vyžadujícího doplňkovou funkcionalitu v demilitarizované zóně, je možné tuto funkcionalitu implementovat v těchto prostředích avšak při striktním dodržení oddělení aplikační logiky informačního systému od tohoto prostředí.</p> <p>Prostředí je provozováno v síti Síť pro běh systémů v demilitarizované zóně.</p>
Prostředí pro provoz externí části univerzálního komunikačního prostředí	<p>Prostředí založené na šabloně prostředí pro běh aplikací. Ukončuje externí komunikaci směrem k univerzálnímu komunikačnímu rozhraní a zprostředkovává služby komunikačního rozhraní implementovaného v interní zóně.</p> <p>Prostředí je provozováno v síti Síť pro běh systémů v demilitarizované zóně.</p>
Prostředí pro ukončení VPN	<p>Prostředí založené na šabloně prostředí pro terminaci VPN.</p> <p>Prostředí má přístup do sítě Síť pro terminaci VPN a Síť pro vzdálenou správu.</p>
Síťové a bezpečnostní prvky	<p>Prostředí obsahující všechny nezbytné síťové nebo bezpečnostní prvky nasazené v DMZ.</p>

HW zdroje využívané uvedenými prostředími mohou být sdíleny v případě, že i při takovém sdílení bude zajištěna vysoká dostupnost řešení.

5.1.6.3 Prostředí pro provoz systému v interní aplikační zóně

Interní aplikační zóna je bezpečnostní zóna, ve které budou provozovány komponenty portálů, aplikační logiky informačních systémů a komponent správy systémů. Jedná se o zónu, která není přímo přístupná z externích sítí a je považována za bezpečnou. Jakákoliv komunikace směrem do komponent řešení nasazených v interní síti z vnější nezabezpečené sítě je směrována prostřednictvím prostředí umístěných v DMZ.

Logický model nasazení prostředí do interní zóny je znázorněn na následujícím obrázku.



Obrázek 6: Prostředí v interní zóně

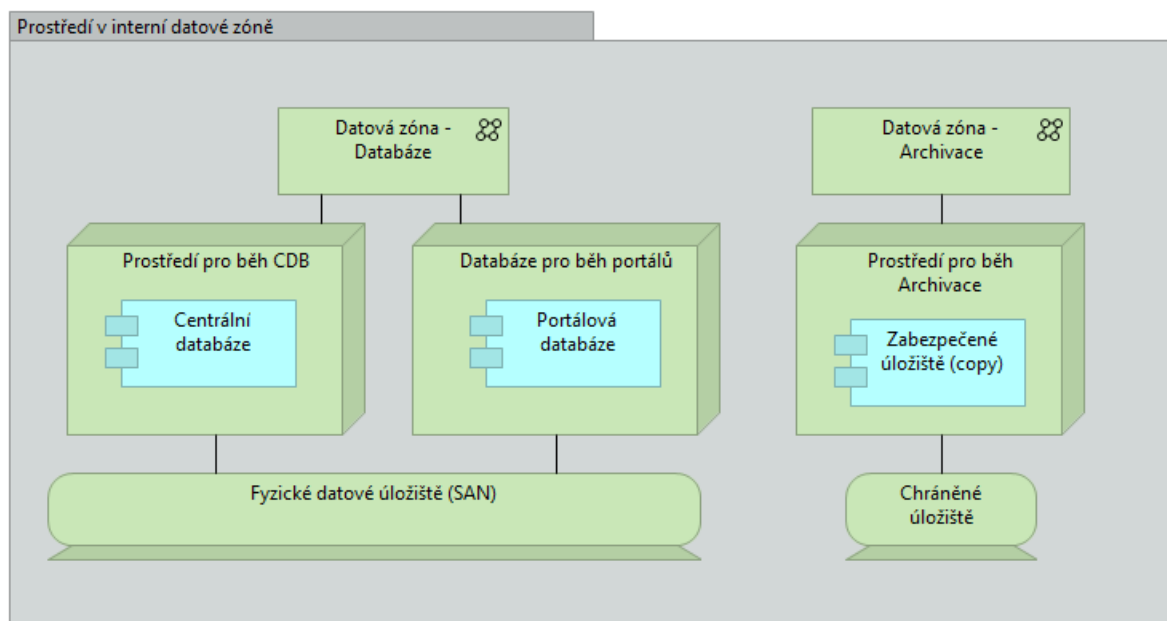
Prostředí	Popis
Prostředí pro e-Legislativu	V prostředí jsou nasazeny portál pro e-Legislativu a aplikační komponenty, které jsou jedinečné pro e-Legislativa. Prostředí má přístup do sítě Aplikační zóna.
Prostředí pro e-Sbírku	Prostředí je určeno k nasazení portálu pro e-Sbírku a aplikačních komponent jedinečných pro e-Sbírku. Prostředí má přístup do sítě Aplikační zóna.
Prostředí pro provoz průřezových modulů	Prostředí je určeno pro nasazení průřezových modulů. Prostředí má přístup do sítě Aplikační zóna.
Prostředí pro provoz JAP	Prostředí je odvozeno od šablony prostředí pro bez aplikací. Jedná se o prostředí, ve kterém běží aplikační komponenty jednotné aplikační platformy. Prostředí má přístup k síti Aplikační zóna.
Prostředí pro správu systému	Prostředí pro nasazení komponentu řešení pro správu systému-Service desk. Prostředí má přístup do sítě Aplikační zóna - Správa systému / Service Desk.
Prostředí pro správu identit	Prostředí je určeno k nasazení aplikačních komponent pro průběh správy identit.

Prostředí	Popis
	Prostředí implementuje Adresářové služby - alternativou může být nasazení specializovaného SW
	Prostředí také implementuje služby PKI - Public Key Infrastructure - alternativou může být nasazení specializovaného SW řešení a publikování k příslušným rozhraní.
	Pro potřeby PKI komponenty prostředí využívá HSM modul.
	Prostředí má přístup k síti - Aplikační zóna - Správa identit.

5.1.6.4 Prostředí pro provoz systému v interní datové zóně

Interní datová zóna je bezpečnostní zóna, ve které budou provozovány komponenty správy dat jako Prostředí pro běh CDB, archivace nebo databáze portálů. Jedná se o zónu, která není přímo přístupná z externích sítí a je považována za bezpečnou. Jakákoliv komunikace směrem do komponent řešení nasazených v interní datové síti z vnější nezabezpečené sítě je směrována prostřednictvím prostředí umístěných v DMZ do interní aplikační zóny a následně komponenta v aplikační zóně komunikuje směrem do datové zóny.

Logický model nasazení prostředí do interní datové zóny je znázorněn na následujícím obrázku.



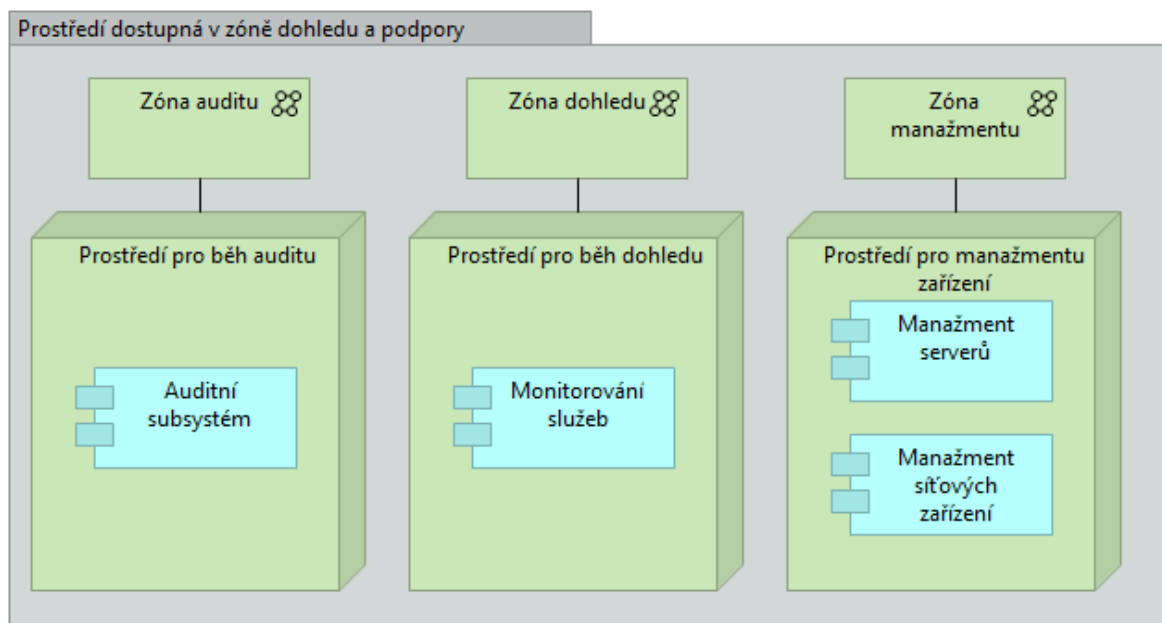
Prostředí	Popis
Databáze pro provoz portálů	Prostředí odvozené od šablony prostředí pro běh databází. Slouží na případný provoz databázových řešení pro používané portálové technologie. Jedná se o uchovávání konfiguračních informací pro portálové technologie nebo jiné údaje, které přímo

Prostředí	Popis
	<p>nesouvisí s údaji zpracovávanými informačním systémem e-Sbírka nebo e-Legislativa.</p> <p>Prostředí je provozováno v Aplikační zóně.</p>
Prostředí pro provoz Centrálního datového úložiště	<p>Prostředí je odvozeno od šablony prostředí pro centrální datové úložiště (CDB). Prostředí hosty SW komponenty zajišťující provoz centrálního datového úložiště. Existuje striktní požadavek na provoz tohoto prostředí napříč tak primárním tak sekundárním datovým centrem v režimu replikace zpracovávaných údajů tak aby bylo možné dosáhnout disaster recovery scénář podle definovaných požadavků. Samotná technologie použitá pro CDB (SW pro databázi) musí být v každém prostředí vysoce dostupných minimálně v režimu Active-Pasive s tím, že přepnutí mezi instancemi SW v případě poruchy primární instance SW bude splňovat požadavky kladené na RTO a RPO.</p> <p>Prostředí má přístup do sítě Datová zóna - databáze.</p>
Prostředí pro archivaci	<p>Prostředí určené pro nasazení komponenty zabezpečené úložiště. Pro potřeby služeb elektronického podpisu využívá HSM modul. Dále používá nezávislé fyzické zařízení Chráněné úložiště, do kterého odkládá všechny zpracovávané údaje. Fyzické zařízení chráněné úložiště je umístěno v archivním datovém centru.</p> <p>Prostředí má přístup do sítě Datová zóna - Archivace.</p>

5.1.6.5 Prostředí dostupná v zóně pro dohledový systém a systém podpory

Uvedená jsou pouze prostředí důležitá z pohledu aplikačních komponent informačního systému. Infrastrukturní prostředí, jako například prostředí pro správu virtualizační technologie, popsána nejsou a předpokládá se, že je popíše dodavatel v kontextu technologie, která bude zvolena.

Prostředí jsou znázorněna na následujícím obrázku.



Obrázek 7: Prostředí v síti dohledu a podpory

Prostředí	Popis
Prostředí pro běh auditu	Aplikační prostředí pro běh systému auditu. Prostředí vyžaduje nasazení komponenty Auditní subsystém. Prostředí má přístup do sítě Zóna auditu.
Prostředí pro běh dohledu	Aplikační prostředí pro běh systému podpory. Prostředí vyžaduje nasazení komponenty Monitorování služeb. Prostředí má přístup do sítě Zóna dohledu.
Prostředí pro management zařízení	Prostředí pro běh systému pro management serverů a management síťových zařízení lokální sítě Prostředí má přístup do sítě Zóna managementu

5.1.7 Typy zařízení

5.1.7.1 Firewall

Firewall bude implementována s využitím bezpečných technologií pro řízení komunikace v sítích. Je požadováno, aby firewall nesloužil pouze na filtraci IP datagramu, ale bude veškerou komunikaci analyzovat na 7. vrstvě (aplikační) modelu ISO / OSI a mezi sítěmi předávat aplikační data vyhovující nastavené bezpečnostní politice.

5.1.7.2 IDS/IPS

IPS tvoří demarkační úlohu, kdy sleduje provoz na vyšších vrstvách ISO/OSI modelu a predikuje a rozpoznává nestandardní či nebezpečné chování. Pokud je zapojena v in-line

režimu, je možné její nasazení za účelem filtrování provozu. Pokud má sonda více portů, je možné monitorovat a kontrolovat více segmentů, například vstupní toky z externích sítí.

Nasazení IPS umožňuje eliminovat velké množství bezpečnostních hrozeb jak na web servery, tak na jakékoliv jiné zdroje publikované na datové síti. V případě web serverů je tak možné omezit/eliminovat útoky jako je například XSS (Cross site scripting), SQL injection, Identity hijacking a podobně. Samozřejmě lze eliminovat i útoky na nižších vrstvách jako je Denial of Service, Distributed Denial of Service, útoky na operační systém nebo na zranitelnosti webového serveru.

Důležitou vlastností IPS zařízení je schopnost reportovat události do nadřazených vyhodnocovacích nástrojů a tímto schopnost provádět globální korelaci událostí mezi různými bezpečnostními zařízeními a servery.

5.1.7.3 Fyzický server

Na úrovni serverů je dostupnost řešení zabezpečena především redundancí serverů ve všech vrstvách aplikace. Předpokladem dosažení vysoké dostupnosti je, že systém nebude nasazený na HW infrastrukturu sdílené s jinými systémy.

Databázové servery budou provozovány v clusteru zajišťujícím vysokou dostupnost databázové vrstvy řešení.

Aplikační servery budou zapojeny jako serverové farmy. Tento návrh umožní, aby v případě výpadku kteréhokoliv serveru mohl přebrat jeho úlohu jiný server ve farmě.

Servery jsou k LAN (Local Area Network) i SAN (Storage Area Network) připojeny minimálně dvěma datovými a jedním management rozhraním.

Pro účely produkční aplikace budou použity shodné typy serverů v primární i záložní lokalitě.

Jednotlivé servery musí samostatně splňovat předpoklady vysoké dostupnosti, tj. musí být řešeny s redundantními prvky, jako je zdvojený zdroj, chlazení, vícenásobné síťové rozhraní atp.

5.1.7.4 Load balancer

Slouží k vyvažování zátěže. Zajišťuje obvykle speciální program, hardwarové zařízení (například switch, který umí přepínat na síťové vrstvě). S ohledem na požadavek vysoké dostupnosti zajistí dosažitelnost duplicitních komponent.

5.1.7.5 Virtuální server

Virtuální server vytvořený v rámci virtuálního prostředí.

5.1.7.6 Centrální úložiště – fyzické zařízení

Vlastní fyzické zařízení splňující požadavky na dlouhodobé ukládání dat a dokumentů.

5.1.7.7 Host Security Modul (HSM)

HSM je kryptografický modul, který slouží serverům k bezpečnému uložení kryptografického materiálu a bezpečnému provádění kryptografických operací. V našem případě se bude jednat o vytváření elektronických značek (tj. specializovaných elektronických podpisů prováděných např. servery dle zákona 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů).

Elektronickou značkou se dle zmíněného zákona míní údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Jelikož elektronické značky budou vytvářeny pomocí HSM, který musí být nasazen dle dikce zákona o elektronickém podpisu „prostředkem pro vytváření elektronických značek“, tak je důležité uvést i požadavky na takové prostředky, které specifikuje § 17a:

- Prostředek pro vytváření elektronických značek musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
 - data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,
 - označující osoba je informována, že zahajuje používání tohoto prostředku.
 - Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí.

Prostředek pro vytváření elektronických značek musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.

Elektronické značky musí také současně splňovat požadavky eIDAS na elektronické pečeti.

5.1.8 Provoz informačního systému

Pro dodržení požadovaných parametrů řešení je nutné zajistit odpovídající parametry údržby a servisu. Hlavními požadavky v této oblasti jsou pak:

Požadavek	Popis
NP035- Provozní doba	<ul style="list-style-type: none">• Systém musí být provozován v režimu 24x7, tj. 24 hodin denně, 7 dní v týdnu

	<ul style="list-style-type: none"> • Přípustná doba plánované odstávky v operační době souhrnně 8 hod měsíčně. • Předpokládaný provoz help desku zajišťujícího uživatelskou podporu je: Po-Pá: 6:00 – 22:00, So-Ne: 8:00 – 20:00
NP036- Dostupnost	<ul style="list-style-type: none"> • Systém musí být možno provozovat v režimu 24x7 s dostupností 99.9%.
NP043- Klíčové parametry úrovně služeb (SLA)	<ul style="list-style-type: none"> • RTO = 4 hodiny (včetně obnovy při ztrátě či poškození dat) • RPO = 10 minut s chráněním proti rizikům: <ul style="list-style-type: none"> ○ výpadku či ztrátě jednoho datového centra ○ uživatelskému, administrátorskému či aplikačnímu (způsobené SW chybou) poškození či ztrátě databází • Navíc systém musí garantovat nulovou ztrátu dat vyhlášených eLegislativou do eSbírky (vzhledem k výše uvedeným rizikům). • V případě, že dojde k výpadku systému včetně ztráty nebo poškození dat a systém je obnoven se starší verzí dat, musí tlustý klient eŠablony pro plusovou osu nabídnout uživateli k zapracování fragmenty obsahu, které byly do centrálního systému odeslány, avšak obnovou dat byly ztraceny. Tato funkce musí být schopná nabídnout obnovou takových fragmentů minimálně po dobou definovanou parametrem RPO.

Pro dodržení těchto parametrů je třeba vybudovat standardní systém podpory založený na několika úrovních podpory. Informační systém obsahuje komponenty Správa systému / Service desk. Realizace podpory předpokládá využití této komponenty ve spolupráci s dalšími podpůrnými komponentami řešení jako Monitoring, Vzdálená správa a podobně.

Komponenta Monitoring umožňuje monitoring infrastruktury a aplikačních komponent a tím pádem umožňuje identifikovat potenciální problémy před tím, než ovlivní provoz informačního systému.

Systém ServiceDesk, bezpečnostní a provozní monitoring, kontaktní centrum a související technologie a implementační práce budou zajištěny zadavatelem a nejsou součástí dodávky. Nejedná se však o aplikační Service Desk popsáný v požadavcích na systém (správa uživatelů a podobně). Předmětem dodávky je zajištění instalace a zprovoznění monitorovacích agentů na veškeré dodávané infrastrukturu (zejména agentů Microsoft SCOM) a dále je dodavatel povinen provést konfiguraci syslogů a síťových zařízení takovým způsobem, aby mohli být dodávané komponenty monitorovány centrálním dohledovým systémem zadavatele (HP NNMI, HP ArchSight).

V případě, že některé komponenty dodávaného řešení není možné monitorovat uvedenými nástroji, je povinností dodavatele zajistit v rámci dodávky nasazení vlastního monitorovacího systému, včetně potřebných SW licencí a HW zdrojů a integrace dodaného řešení do centrálních nástrojů provozovaných zadavatelem.

5.1.8.1 Podpora uživatelů

Systém podpory bude rozdělen do čtyř úrovní (tzv. Levels). Podpora úrovně 1 a 2 budou zajišťovány objednatelem. Podpora úrovně 3 a 4 bude zajištěna dodavatelem.

Úroveň podpory	Popis
Úroveň 1	<p>První úroveň podpory, která odpovídá na základní problémy uživatelů. Úkolem pracovníka podpory 1. úrovně je zaznamenat od uživatele problém, získat informace a pokusit se identifikovat problém. Všechny tyto informace jsou zaznamenány do systému Service Desk.</p> <p>Pracovníci na této úrovni podpory mají základní a obecné znalosti o informačním systému a nemusí mít vždy znalosti dostatečné k vyřešení problému. Nevyřešené problémy jsou následně eskalovány do podpory vyšší úrovně.</p>
Úroveň 2	<p>Další úroveň podpory, při níž jsou pracovníci podpory kompetentní řešit i náročnější problémy technického charakteru.</p> <p>V případě, že pracovník podpory 2. úrovně není schopen problém vyřešit, problém je eskalován do podpory úrovně 3.</p>
Úroveň 3	<p>Nejvyšší přímá podpora informačního systému. Pracovníci podpory úrovně 3. mají hluboké znalosti o informačním systému a měly by být schopni vyřešit i nejvážnější technické problémy uživatelů.</p> <p>Reakční doba pracovníků podpory 3 úrovně je 4 hodiny v rámci běžné pracovní doby.</p>
Úroveň 4	Nejvyšší úroveň podpory jako eskalační mechanismus pro model podpory.

Úroveň podpory 1 a 2 je zabezpečena přímo objednavatelem. V rámci řešení třeba definovat a vybudovat systém propojení mezi úrovní podpory 2 a úrovní podpory 3, která už je realizovaná dodavatelem, resp. v spolupráci s dodavatelem a je pro něj přípustné jiné Service Desk řešení jako to, které je používáné v podpoře úrovně 1 a 2.

5.1.8.2 Organizační zabezpečení systému uživatelské podpory

Podpora uživatelů bude rozdělena do následujících oblastí:

- Podpora pro systém e-Legislativa
Vybudovaný systém podpory bude poskytovat podporu výhradně pro provoz informačního systému e-Legislativa a bude se týkat funkcí a používání tohoto systému.
- Legislativní podpora uživatelů
Zadavatel vybuduje nezávislý helpdesk na legislativní podporu. Poskytování legislativní podpory není předmětem dodávky. Pro účely legislativní podpory pracovník podpory úrovně 1 přesměruje příchozí hovor s požadavkem na legislativní podporu na pracovníka

objednavatele odpovědného za legislativní podporu. Proces přesměrování požadavku také není předmětem dodávky.

Úroveň podpory 1 a 2 je zajištěna přímo objednatel. V rámci řešení třeba definovat a vybudovat systém propojení mezi úrovní podpory 2 a úrovní podpory 3, která již bude realizována dodavatelem resp. ve spolupráci s dodavatelem a je pro ni přijatelné jiné Service Desk řešení než to, které je používáno v podpoře úrovně 1 a 2. Za Service Desk řešení pro úroveň podpory 3 a 4 je zodpovědný dodavatel.

Samotný systém pro HelpDesk poskytne objednatel systému. Objednatel také zajistí pracovníky podpory pro úroveň 1 a 2 podpory. Předběžně se očekává kapacita 5 až 10 pracovníků pro zajištění podpory úrovně 1 a zhruba 10 pracovníků pro zajištění podpory úrovně 2.

Dodavatel musí zaškolit pracovníky objednavatele pro úroveň podpory 1 a 2. Předběžně se očekává kapacita 5 až 10 pracovníků objednavatele pro zajištění podpory úrovně 1 a zhruba 10 pracovníků objednavatele pro zajištění podpory úrovně 2. Při zaškolení pracovníků pro podporu úrovně 2 se očekává se zaškolením zaměřeným i na pokročilejší a složitější funkce e-Legislative.

Uvedená uživatelská podpora se týká zejména funkcí a funkcionalit systému e-Legislative, způsobu jejich používání a řešení případných problémů vzniklých při provozu informačního systému. Samotný provoz infrastruktury informačního systému je řešení zvláště prostřednictvím Podpory provozu informačního systému, který je popsán v následující kapitole.

5.1.8.3 Podpora provozu informačního systému

Samostatnou kapitolou je zajištění podpory provozu informačního systému jako takového. Pro účely tohoto provozu se předpokládá definice procesů, které budou použity při nahlašování problémů řešení, které vyžadují administrátorský nebo implementační zásah dodavatele řešení a netýkají se přímo problémů řešených v rámci podpory uživatelů.

Poskytovatelem této podpory je dodavatel informačního systému a bude využívat prostředky vzdálené správy a prostředky komponentu Monitoring na monitorování nasazeného řešení, identifikaci případných budoucích problémů infrastruktury, práce spojené s prevencí řešení a podobně.

Samotná administrace dodaných informačních systémů a HW infrastruktury je v kompetenci objednavatele. Dodavatel pro tento účel vyškolí dostatečný počet pracovníků objednavatele, kteří budou následně během provozu zajišťovat standardní administrační úkoly vyplývající z provozu informačního systému. V případě vzniku problému, jehož řešení nebude v kompetenci administrátorů objednavatele, bude definována procedura, jejímž prostřednictvím bude

aktivováno řešení vzniklého incidentu prostřednictvím podpory provozu informačního systému zabezpečeného dodavatelem.

5.2 Doporučená architektura řešení v oblasti nasazení a provozu

V následujících bodech jsou popsány doporučení pro architekturu v oblasti nasazení a provozu informačního systému. Uvedené body mají charakter doporučení a nejsou pro finální architekturu závazné a mohou a budou se měnit s ohledem na detailní návrh vypracovaný dodavatelem a na použité ať už HW nebo SW technologie. Doporučení jsou uvedena pouze pro oblasti nasazení nebo provozu, kde dávají nějaký smysl i v rovině technologického abstraktu, v němž se bez konkrétní znalosti použitých technologií pohybujeme.

- Nasazení informačního systému by nemělo zabrat více než 4 RACKy pro každé prostředí (kromě archivního, kde předpokládáme 2 RACKy), ve kterém je informační systém nasazen
- Testovací a školicí prostředí by mělo mít identickou technologickou infrastrukturu jako produkční prostředí, vyjma technologií umožňujících přepnutí na záložní prostředí, čímž se zajistí kvalifikované testování dodávaného řešení případně dodávaných změn na řešení. Pro zajištění dostatečného množství dat doporučujeme zvážit vybudování testovací datové báze anonymizací údajů z produkční databáze.
- Každá HW komponenta řešení by měla být zdvojená, aby se v HW infrastruktuře nenacházel Single Point of Failure, včetně infrastruktury diskových polí v každé lokalitě.
- Každá SW komponenta řešení by měla být na úrovni prostředí zdvojená, aby byla zajištěna vysoká dostupnost řešení na úrovni každého prostředí. Zajištění vysoké dostupnosti SW komponenty vyžaduje, aby každá virtualizovaná SW komponenta byla v rámci Cluster provozována na alespoň dvou různých fyzických serverech.
- Disková pole v obou lokalitách doporučujeme propojit na úrovni SAN a technologie replikace (či současného zápisu do obou lokalit) doporučujeme realizovat na úrovni diskových polí.
- Doporučujeme zvážit využití synchronní replikace mezi diskovými poli (případně současný zápis do obou lokalit) s přihlédnutím ke konkrétním technickým parametrům síťových spojení mezi lokalitami.
- Doporučujeme zvážit provoz lokalit v režimu active-active na všech úrovních (aplikační, databázová apod.)
- Na úrovni lokality by měl být fail-over řešení vykonáván automaticky.
- Mezi jednotlivými lokalitami může být fail - over prováděn manuálně při nastavení procesů zajišťujících včasný monitoring vzniku situace vyžadující fail - over řešení do druhé lokality tak, aby byly dodrženy požadované RTO a RPO.



- Pro technologii centrálního datového úložiště (CDB) je vhodné zajistit okamžitou synchronní replikaci dat v rámci jednoho prostředí.
- CDB by měla všechna data uchovávat na vysoce dostupné SAN infrastruktuře.
- CDB by měla obsahovat infrastrukturu umožňující Administrátorům návrat k stavu datové báze v libovolném čase minimálně jeden týden do minulosti.
- vysoce dostupná infrastruktura SW komponent zajišťujících běh CDB by měla být provozována v režimu Active-Active s případným rozdělováním zátěže mezi jednotlivé instance CDB prostřednictvím load-balancing technik nebo implementováním rozdělení zátěže mezi více instancí CDB na základě označení dotazů jako write/update nebo read-only.
- Z hlediska síťové infrastruktury doporučujeme zvážit rozdělení sítí pro běh systémů na logické sítě rozdílné pro provoz systému eSbírka a eLegislative. Tím pádem bude zajištěno síťové oddělení těchto systémů a bude možné nastavit konkrétní politiky pro jednotlivé systémy.
- Sítě v pásmu dozoru a podpory je vhodné rozdělit na logické sítě zajišťující síťový provoz jednotlivých komponent řešení pro dohled a podporu. Toto může být limitováno způsobem řešení systémů pro dohled a podporu, které provozuje zadavatel.
- Pro účely minimalizace HW zdrojů potřebných na provoz řešení je vhodné agregovat prostředí pro běh systémů na co nejmenší počet fyzických serverů tak, aby však byl stále zajištěn požadavek na rozprostření každé vysoce dostupných SW komponenty přes alespoň dva fyzické servery.

6 Přílohy

6.1 Příloha č. 1 - Specifikace služeb CMS

Pro připojení a zabezpečení infrastruktury bude možné použít standardní služby systému CMS:

6.1.1 Služba CMS2 – 02 – Zveřejnění aplikace

Název parametru	Vysvětlení
Kód služby	CMS2-02
Název služby	Zveřejnění aplikace
Popis služby	<p>Služba vytvoří prostředí pro publikaci aplikační služby informačního systému OVM. Varianty služby se liší podle cílového prostředí. Možné varianty jsou:</p> <ol style="list-style-type: none">1. do sítě Internet2. do sítě CMS3. do sítě sTESTA4. do Extranetu

Aplikační služba může být umístěna v infrastruktuře OVM nebo v infrastruktuře Národního datového centra (NDC). Aplikační služba může být zveřejněna do více prostředí současně. Aplikační služba je zveřejněna na definovaných protokolech a portech.

Při zveřejnění aplikace do sítě Internet jsou aplikaci přiděleny veřejné IP adresy z prostoru CMS. Přístup ke zveřejněné službě může být omezen na definované zdrojové IP adresy.

Při zveřejnění aplikace do sítě CMS jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Službu je možné zveřejnit pro všechny ostatní subjekty připojené do sítě CMS (Veřejná služba) nebo pro definované subjekty (Schvalovaná služba). O přístup ke Schvalované službě musí přistupující subjekty žádat prostřednictvím služby CMS2-03.

Při zveřejnění aplikace do sítě sTESTA jsou aplikaci přiděleny IP adresy z prostoru pro ČR v síti sTESTA. Přístup ke zveřejněné službě je omezen na definované zdrojové IP adresy. Zveřejnění aplikace musí být provozováno v souladu s provozními a bezpečnostními požadavky EU pro síť sTESTA.

Při zveřejnění aplikace do Extranetu jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Aplikační služba je zveřejněna pro všechny subjekty, které mají do daného extranetu přístup.

6.1.2 Služba CMS2 – 03 – Přístup k aplikaci

Název parametru	Vysvětlení
Kód služby	CMS2-03
Název služby	Přístup k aplikaci
Popis služby	<p>Služba umožňuje zřizovat a rušit přístupy k aplikačním službám. Varianty služby se liší podle cílového prostředí. Možné varianty představují přístup:</p> <ol style="list-style-type: none"> 1. k aplikaci v síti CMS 2. k aplikaci v síti sTESTA 3. k aplikaci v síti Internet 4. k aplikacím v Extranetu 5. čtenář eGON Service Bus

Služba umožňuje zřizovat, měnit a rušit přístupy subjektu k cizí aplikační službě. Jednou žádostí lze zřídit přístup právě k jedné aplikační službě. Připojení je povoleno z definovaných IP adres v síti subjektu.

Přístup k aplikaci v síti CMS umožní subjektu připojení k aplikační službě zveřejněné jiným subjektem prostřednictvím služby CMS2-02 v síti CMS. Zřízení přístupu je podmíněno souhlasem vlastníka zveřejněné aplikační služby, které probíhá prostřednictvím portálu CMS.

Přístup k aplikaci v síti sTESTA umožní subjektu připojení k aplikační službě zveřejněné jiným státem Evropské unie v síti sTESTA. Připojení je povoleno na definovaných protokolech a portech. Přístup k aplikaci musí být provozován v souladu s provozními a bezpečnostními požadavky EU pro síť sTESTA.

Přístup k aplikaci v síti Internet umožní subjektu připojení k aplikační službě zveřejněné v síti Internet na definovaných protokolech a portech. Cílovou aplikační službu v síti Internet je nutné definovat konkrétními IP adresami.

Přístup k aplikacím v Extranetu umožní subjektu připojení ze sítě Internet prostřednictvím technologie SSL VPN ke všem aplikačním službám zveřejněným v daném Extranetu. Připojení subjektu k Extranetu musí být schváleno Správcem CMS.

Pro čtenáře eGON Service Bus je nutné zprovoznit přístup z aplikace subjektu k systému eGON Service Bus a zároveň zprovoznit přístup ze systému eGON Service Bus vůči aplikaci žadatele. Logicky se tedy jedná o zřízení obousměrných síťových propustů mezi eGON Service Bus a aplikací žadajícího subjektu.

6.1.3 Služba CMS2 – 04 – Umístění aplikace OVM do NDC

Název parametru	Vysvětlení
Kód služby	CMS2-04
Název služby	Umístění aplikace OVM do NDC
Popis služby	Služba napomáhá OVM jednorázově zajistit podmínky pro umístění infrastruktury do prostředí Národních datových center (NDC) - kontakty na správce NDC, zajištění konektivity mezi NDC

Služba pomáhá OVM zajistit podmínky pro umístění infrastruktury do Národních datových center (NDC). Na žádost OVM jsou poskytovány informace nezbytné pro to, aby byla infrastruktura (resp. informační systém) umístěna do jednoho nebo více NDC.

Na základě žádosti může být pro OVM zprostředkován pronájem konektivity (na úrovni vrstvy L2 nebo L3) s definovanými technickými parametry mezi NDC, ve kterých OVM umístí svoji infrastrukturu.

CMS nezajišťuje vlastní umístění infrastruktury v prostředí NDC, ale umožňuje zpracování požadavků na propojení infrastruktur umístěných v různých NDC.

6.1.4 Služba CMS2 – 05 – Přenos elektronické pošty

Název parametru	Vysvětlení
Kód služby	CMS2-05
Název služby	Přenos elektronické pošty
Popis služby	Služba MTA zajišťuje předávání zpráv elektronické pošty jak mezi jednotlivými subjekty KIVS, tak mezi subjekty KIVS a uživateli sítě Internet. Možné varianty služby představují: 6. Odchozí SMTP provoz 7. Příchozí SMTP provoz

V principu se jedná se o službu Mail Transfer Agent (MTA) – služba zajišťuje předávání zpráv mezi mailovými servery a zároveň plní bezpečnostní funkce antiviru a antispamu. Služba je poskytována ve variantě Odchozí SMTP provoz (odesílání elektronické pošty ze serveru subjektu) a Příchozí SMTP provoz (přijímání elektronické pošty na server subjektu), přičemž je možné objednat obě varianty současně.

Předávání elektronické pošty je možné realizovat v rámci prostředí KIVS nebo do a z prostředí sítě Internet. Služba nezahrnuje poštovní schránky a není též určena k přeposílání zpráv v rámci jednoho subjektu.

6.1.5 Služba CMS2 – 06 – DNS hosting

Název parametru	Vysvětlení
Kód služby	CMS2-06
Název služby	DNS hosting
Popis služby	Služba zajišťuje vedení DNS záznamů na jmenných serverech CMS. Možné varianty jsou: 8. Veřejná registrovaná doména 9. Veřejná doména CMS 10. Neveřejná doména

Služba Veřejná registrovaná doména zajišťuje poskytování jmenných služeb (DNS) do sítě Internet pro domény ve vlastnictví subjektu, veřejně registrované v síti Internet. Subjekt musí zabezpečit nasměrování domény na jmenné servery CMS. Služba nezajišťuje vlastní registraci domény.

Služba Veřejná doména CMS zajišťuje poskytování jmenných služeb (DNS) do sítě Internet pro domény vyššího řádu v doméně „gov.cz“.

Služba Neveřejná doména zajišťuje poskytování jmenných služeb (DNS) do sítě CMS pro záznamy v interní doméně sítě CMS „cms2.cz“.

6.1.6 Služba CMS2 – 07 – Služby sTESTA

Název parametru	Vysvětlení
Kód služby	CMS2-07
Název služby	Služby sTESTA
Popis služby	Služba umožňuje nastavení doplňkových služeb v síti Evropské unie sTESTA.

Služba umožňuje vyžádat nastavení doplňkových služeb v síti sTESTA. Jde se především o správu DNS záznamů v zóně „cz.testa.eu“ či změnu v nastavení směrování elektronické pošty

v rámci sítě sTESTA. Požadavky subjektu jsou zpracovány a následně uplatněny u provozovatele sítě sTESTA. Změna nastavení služeb musí být v souladu s provozními a bezpečnostními požadavky EU pro síť sTESTA.

6.1.7 Služba CMS2 – 08 – Přístup do CMS

Název parametru	Vysvětlení
Kód služby	CMS2-08
Název služby	Přístup do CMS
Popis služby	<p>Služba je určena pro připojení počítačových sítí OVM k síti CMS.</p> <p>Varianty služby se liší podle způsobu připojení. Možné způsoby připojení jsou:</p> <ol style="list-style-type: none"> 1. KIVS VPN 2. IPSec VPN 3. SSL VPN 4. Krajský konektor 5. NDC

Služba zajišťuje připojení počítačových sítí nebo koncových stanic OVM k síti CMS jednou z následujících variant.

1. KIVS VPN – připojení koncové lokality nebo více lokalit prostřednictvím MPLS sítě telekomunikačního operátora. Varianta je určena pro takové lokality, ve kterých sídlí řádově alespoň desítky uživatelů (resp. počítačů připojených k síti).
2. IPSec VPN – připojení koncové lokality pomocí šifrovaného spojení přes síť Internet. K zabezpečení této komunikace mohou být využívány certifikáty vydávané neveřejnou certifikační autoritou CMS. Varianta je vhodná pro lokality, ve kterých sídlí do 25 uživatelů (resp. počítačů připojených k síti).
3. SSL VPN – uživatelské připojení pomocí šifrovaného spojení přes síť Internet. Připojení je realizováno prostřednictvím VPN klienta, instalovaného na každém připojovaném počítači. Varianta je určena pro připojení jednotlivých počítačů.
4. Krajský konektor – připojení lokalit je realizováno přes hraniční prvky CMS, distribuované ve všech krajských městech.
5. NDC – připojení infrastruktury umístěné v Národním datovém centru do sítě CMS. Připojení je realizováno přes hraniční prvky CMS, umístěné v Národních datových centrech.

6.1.8 Služba CMS2 – 09 – Přístup do Internetu

Název parametru	Vysvětlení
Kód služby	CMS2-09
Název služby	Přístup do Internetu
Popis služby	<p>Služba zajistí přístup subjektu do sítě Internet prostřednictvím zřízené přípojky do CMS.</p> <p>Varianty služby se liší podle požadované úrovně zabezpečení přístupu do Internetu. Možné způsoby připojení jsou:</p> <ol style="list-style-type: none"> 11. Přímé připojení 12. Bezpečné připojení <p>Služba neslouží k zajištění přístupu ke službám CMS.</p>

Služba zajistí pro lokality OVM připojené do prostředí CMS přístup do Internetu.

Ve variantě Bezpečného připojení je síťový provoz kontrolován a překládán. Tato varianta umožňuje využít protokoly HTTP, HTTPS, FTP, FTPoHTTP.

Ve variantě přímého připojení není mezi sítí OVM a Internet vkládán jakýkoli bezpečnostní prvek. OVM je přidělen rozsah veřejných IP adres z rozsahu CMS. Přípojku využívanou pro tuto variantu není možné využít v kombinaci s jinými službami CMS.

6.1.9 Služba CMS2 – 10 – Přístup k záznamům o provozu

Název parametru	Vysvětlení
Kód služby	CMS2-10
Název služby	Přístup k záznamům o provozu
Popis služby	Přístup OVM k provozním statistikám jeho služeb včetně údajů o plnění SLA.

Služba zahrnuje přístup OVM k provozním statistikám a záznamům o provozu jím objednaných služeb včetně údajů o plnění SLA a zároveň výsledky monitoringu linek, na kterých jsou provozovány jím objednané služby. Přístup k záznamům o provozu je OVM umožněn přes portál CMS.

6.1.10 Služba CMS2 – 11 – Přístup k účtovacím informacím

Název parametru	Vysvětlení
Kód služby	CMS2-11
Název služby	Přístup k účtovacím informacím
Popis služby	Přístup OVM k účtovacím informacím jeho služeb.

Přístup OVM k vlastním účtovacím informacím přes portál CMS.

6.1.11 Služba CMS2 – 12 – Virtuální firewall

Název parametru	Vysvětlení
Kód služby	CMS2-12
Název služby	Virtuální firewall
Popis služby	<p>Služba zajišťuje zřízení virtuálního firewallu v infrastruktuře CMS. Na virtuálním firewallu jsou zakončeny jednotlivé přípojky a zveřejňovány služby. Bez virtuálního firewallu není možné poskytovat některé další služby CMS.</p> <p>Možné varianty jsou:</p> <ul style="list-style-type: none">13. Virtuální firewall pro OVM14. Virtuální firewall pro Extranet

Virtuální firewall pro OVM zajišťuje zřízení virtuálního firewallu v infrastruktuře CMS pro jednotlivá OVM. Na tomto virtuálním firewallu jsou zakončovány jednotlivé VPN. V rámci zřízení služby je subjektu vyhrazena část rozsahu privátních IP adres CMS (Konsolidovaný adresní rozsah). Jde o překladové IP adresy, pod kterými subjekt přistupuje k ostatním službám v CMS a zároveň tyto IP používá při publikaci svých služeb. Každý subjekt si může zřídit právě jeden virtuální firewall.

Virtuální firewall pro Extranet slouží jako nástroj pro Správce CMS k definici Extranetu. Extranet je skupina aplikačních služeb určených pro stejný okruh OVM. Pomocí této služby definuje Správce CMS složení aplikačních služeb zveřejněných a okruh přistupujících uživatelů v daném Extranetu. Jednotlivé publikující subjekty pak žádají o zveřejnění svých aplikací do tohoto Extranetu prostřednictvím služby CMS2-02. Přístup k aplikacím tohoto Extranetu je vyžádán přistupujícími subjekty prostřednictvím služby CMS2-03.

6.2 Příloha č. 2 – výňatek přílohy č. 1 k vyhlášce č. 316/2014 Sb.

6.2.1 Hodnocení a úrovně důležitosti aktiv

Pro hodnocení důležitosti aktiv jsou použity stupnice o čtyřech úrovních. Orgán nebo osoba uvedená v § 3 písm. c) až e) zákona č. 316/2014 Sb. může používat odlišný počet úrovní pro hodnocení důležitosti aktiv, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jí používaným způsobem hodnocení důležitosti aktiv a stupnicemi a úrovněmi pro hodnocení důležitosti aktiv, které jsou uvedeny v této příloze.

V případě použití tří úrovní hodnocení důležitosti aktiv je přípustné sloučit buď úrovně nízká a střední, nebo úrovně vysoká a kritická.

6.2.1.1 Stupnice pro hodnocení důvěrnosti

Úroveň	Popis	Ochrana
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how orgánu a osoby uvedené v § 3 písm. c) až e) zákona, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítě jsou chráněny pomocí kryptografických prostředků.

Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje).	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
----------	---	--

6.2.1.2 Stupnice pro hodnocení integrity

Úroveň	Popis	Ochrana
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).

6.2.1.3 Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Ochrana
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

6.2.2 Hodnocení rizik

Hodnocení rizik je vyjádřeno jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

Pro hodnocení rizik lze použít zejména tuto funkci

$\text{riziko} = \text{dopad} \times \text{hrozba} \times \text{zranitelnost}$.

Jednoznačné určení funkce pro určení rizika je nezbytnou součástí metodiky pro identifikaci a hodnocení rizika.

Stupnice pro hodnocení dopadů



Úroveň	Popis
Nízký	<p>Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický.</p> <p>Rozsah případných škod nepřesahuje</p> <p>a) 10 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin nebo</p> <p>b) finanční nebo materiální ztráty do 5000000 Kč anebo</p> <p>c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob.</p>
Střední	<p>Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí</p> <p>a) do 10 mrtvých nebo od 11 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin nebo</p> <p>b) finanční nebo materiální ztráty od 5000000 Kč do 50000000 Kč anebo</p> <p>c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2500 osob.</p>
Vysoký	<p>Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí</p> <p>a) od 11 do 100 mrtvých nebo od 101 do 1000 osob s následnou hospitalizací po dobu delší než 24 hodin nebo</p> <p>b) finanční nebo materiální ztráty od 50000000 Kč do 500000000 Kč anebo</p> <p>c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2501 do 25000 osob.</p>
Kritický	<p>Dopad je plošný rozsahem, trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí</p> <p>a) 101 a více mrtvých a 1001 a více osob s následnou hospitalizací po dobu delší než 24 hodin nebo</p> <p>b) finanční nebo materiální ztráty převyšující 500000000 Kč anebo</p> <p>c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25000 osob.</p>
Stupnice pro hodnocení hrozeb	

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.
Stupnice pro hodnocení zranitelností	
Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy o překonání bezpečnostních opatření.
Stupnice pro hodnocení rizik	



Úroveň	Popis
Nízké	Riziko je považováno za přijatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoké	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.

V případě, že orgán nebo osoba uvedená v § 3 písm. c) až e) zákona č. 316/2014 Sb. využívá metodu pro identifikaci a hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení míry hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně postupuje i orgán nebo osoba uvedená v § 3 písm. c) až e) zákona č. 316/2014 Sb., které používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.