1 Struktura výstupů

Výstupem plnění Zhotovitele bude:

1. Realizace komponent systémového prostředí popsaných níže (tzv. **fixní část**).
2. Volné kapacity k využití pro nyní nespecifikovatelné činnosti (tzv. **variabilní část**).
   Důvodem pro *variabilní část* je fakt, že komponenty systémového prostředí, které tvoří *fixní část zakázky*, jsou identifikovány Objednatelem na základě faktů známých v době uzavření Smlouvy, kdy není schválena novela vyhlášky o podrobnostech výkonu spisové služby a národní standard pro elektronické systémy spisové služby, není vytvořena metodika testování spisových služeb a nejsou vytvořeny testovací scénáře pro testování spisových služeb; z tohoto důvodu Objednatel musí předpokládat, že v současné době nezná všechny potřebné komponenty systémového prostředí nebo jejich detailní nastavení a že další budou identifikovány na základě prací na uvedených dokumentech a též na základě reálných výkonových zjištění s hardwarovou infastrukturou pro testování spisových služeb. Předmětem variabilní části jsou například programátorské, konzultační a analytické práce, spoluúčast na jednání s dalšími subjekty jako je Správa základních registrů.

Nyní známá plnění na vytvoření systémového prostředí atestačního střediska, tvořící **fixní část zakázky**, jsou:

1.1 Výstup č. 1: Definice a vytvoření komponent systémového prostředí pro vytvoření, běh a správu virtuálního prostředí pro testování elektronických spisových služeb

*Předmětem plnění je vytvořit technické předpoklady pro běh procesu vyřízení obchodního případu atestace, a to v součinnosti s Objednatelem a na základě schválené metodiky atestací. Činnosti provedené v **rámci fixní části zakázky** jsou uvedeny **v seznamu níže**; jak ale budou postupovat práce, mohou být ze strany Objednatele požadována také plnění v **rámci variabilní části**. Implementace tohoto seznamu, především pak vyladění na produkční kvalitu, bude ale zjevně možné až po realizaci dodávky a zprovoznění hardwarového prostředí (není součástí plnění dle Smlouvy), neboť do té doby není k dispozici hardware, na kterém toto aplikační vybavení má být instalováno. Dodávka hardware zatím není uskutečněna.*
Zhotovitel dodá komponenty systémového prostředí pro vytvoření, běh a správu virtuálního prostředí pro testování elektronických spisových služeb prostředí včetně:

- Popisu způsobu jejich instalace
- Dokumentace (viz bod 1.5)
- Způsobu otestování funkčnosti vytvořených nástrojů (popis vstupů a očekávaných výstupů)

Jednotlivé komponenty jsou:

a. Analýza těch potřeb atestačního střediska ve vztahu k virtualizované hardwarové architektuře, jejichž výkon lze rolím atestačního střediska (především roli vedoucího testera) usnadnit. Jedná se o body tohoto seznamu „b)“ a následující (které tvoří fixní část), avšak plnění může být rozšířeno o body identifikované v této analýze (v rámci variabilní části).

b. Pořízení nebo vytvoření nástrojů pro řízení soustavy virtuálních strojů (a případně dalších elementů systémové infrastruktury, např. síťových prostupů) společně tvořících testovací prostředí pro danou spisovou službu, umožňujících především:
   - vytvoření virtuálního prostředí pro testování dané spisové služby (dále jen „**prostředí**“)
   - zálohování prostředí
   - obnovu prostředí ze zálohy
   - správu více záloh daného prostředí
     kde „zálohou“ se rozumí „odložení“ v jeho současném stavu, včetně logování této akce a zajištění bezespornosti provedení této operace takovým způsobem, aby nemohlo být zpochybněna integrita prostředí ani záznamů o provedení činnosti (tj. fakt, že záloha prostředí byla provedena v daný čas daným pracovníkem)

   takovým způsobem, aby:
   - je mohl využívat i uživatel v roli a se znalostmi pracovní vedoucího testovacího týmu, nikoliv nutně administrátor systému (správce hypervizorů)
   - jejich použití bylo bezpečně a nezpochybnitelně logováno (pozn.: Objednatel disponuje systémem log-managementu), tedy s možností odesílání systémových logů virtuálních počítačů do centrálního log-managementu

   Prostředí pro testování spisové služby je tvořeno soustavou virtuálních strojů (a případně dalších elementů aplikační infrastruktury), kde všechny tyto elementy slouží specificky pro testování jedné konkrétní spisové služby a musí být vytvořeny, zálohovány a ze záloh obnovovány najednou. Zásadní je tedy integrita uchování vazeb mezi elementy prostředí (virtuálními servery, konfigurací síťových prvků apod.) a nezpochybnitelnost této integrity.
   Součást prostředí tvoří nejméně následující virtuální stroje:

   - aplikační server
   - databázový server
   - klientské stanice pro jednotlivé uživatelské role (klientských stanic bude tolik, kolik rolí bude předepsáno testovacími scénáři – toto nyní není přesně známo, neboť testovací scénáře nejsou tvořeny, ale předpoklad je cca mezi 3 a 5 rolemi).

c. Instalace operačních systémů a instalace standardních komponent (např. antivir) na virtuálních strojích dodané hardwarové architektury

d. Nastavení přístupu k virtuálním strojům pro Dodavatele a zpřístupnění těchto přístupů ke sdělení Dodavateli (VPN + VLAN, Dodavatel vidí jen jemu určené virtuální stroje, v žádném případě zbytek infrastruktury nebo ostatní testovací prostředí)

e. Komunikace se správci a provozovateli spolupracujících systémů, se kterými má testovaná eSSL komunikovat podle potřeb testovacích scénářů, nastavení a využití přístupů k těmto systémům

f. Na dodané hyperkonvergované hardwarové architektuře instalace sdílených služeb nutných nebo (z důvodu efektivity) vhodných pro podporu testování a zajištění jejich dostupnosti z testovacích spisových služeb:
   i Prostupy ke spolupracujícím systémům
   ii Validátor SIP balíčků
   iii Systém pro řízení atestací (počítačový program vytvořený za účelem správy jiných dat atestací než jsou virtuální stroje)
   iv Interní emailový server atestačního střediska
   v Interní trezor pro testovací zavirované soubory využívané k testování a nastavení bezpečnostních pravidel a funkčních mechanismů pro práci s nimi.
   vi Interní active directory pro atestační středisko
   vii Klient log serveru
   viii Komponenta pro zajištění služeb vytvářejících důvěru
   ix Podpůrný software odeslání připraveného emailů / datových zpráv cílově do testované eSSL, včetně (pokud tak testovací scénáře předepíší) i řízeně zavirované verze
   x Technické prostředky pro podporu kybernetické bezpečnosti v souladu se zákonnými požadavky a bezpečnostní politikou informací Objednatele
   xi Interní helpdesk pro řízení požadavků (viz bod 1.4)
   xii + další dle budoucí analýzy a v souladu s testovacími scénáři **v rámci variabilní části**

g. Příprava artefaktů užitých v testovacích scénářích, pokud toto budou testovací scénáře vyžadovat
   i konstantní testovací data ve zpřístupněném systému ISZR
   ii datové zprávy ve zpřístupněném systému ISDS
   iii data, která by za účelem testování měly poskytovat spolupracující systémy
   iv výchozí emaily v mail boxu
   v + další dle budoucí analýzy a v souladu s testovacími scénáři **v rámci variabilní části zakázky**

h. Pokud bude součástí řešení také kontinuálně běžící program (služba – service), bude pro něj dodán i způsob monitoringu běhu a log managementu prostředky Objednatele.

i. Definice pracoviště – definice programového vybavení na straně klientských stanic testerů (software, přístupy apod.) týkající se zpřístupnění vytvořeného prostředí

Zhotovitel provede analýzu prostředí Objednatele a navrhne způsob realizace jednotlivých výše uvedených bodů, který před jejich realizací předloží Objednateli ke schválení.

Při realizaci systémového prostředí Zhotovitel dodrží následující zásady:

1. Pokud plnění bude obsahovat komponenty vytvořené (naprogramované) Zhotovitelem a tyto komponenty budou mít grafické uživatelské rozhraní (což je preferovaná varianta), bude toto uživatelské rozhraní realizováno architekturou „tenkého klienta“. Návrh řešení musí preferovat architekturu takovou, aby na straně pracovní stanice uživatele nebylo nutno instalovat žádný pro speciálně vytvořený software (preferovaným klientem je standardní webový prohlížeč).
2. Bude plně oddělen programový kód komponent řešení a konfigurační nebo jinak vzniklá data, tj. v programovém kódu nesmí být například žádné uživatelsky definované konstanty/parametry, odkazy na externí zdroje (např. certifikáty, certifikační autority, firewall ČAS, IP adresu nebo URL na spolupracující systémy). Veškeré možnosti změny

nastavení musí být realizovatelné konfiguračně (s autentizací, autorizací i logováním) bez potřeby zásahu do programového kódu. Stejně tak používané kryptografické prostředky musí být konfigurovatelné bez zásahu do programového kódu. Změna kryptografických algoritmů, funkcí a délek klíčů musí být možná bez nutnosti programování a kompilace.

3. Patch management, release management řešení musí být realizován v časových oknech definovaných Objednatelem.
4. Řešení musí dodržet/naplnit všechna (relevantní) ustanovení platné bezpečnostní politiky informací Objednatele.
5. Řešení nedovolí přístup bez autentizace k jakékoli funkci, která autentizaci má vyžadovat.
6. Řešení musí zajistit veškeré logování své činnosti minimálně v rozsahu stanoveném zákonem 181/2014 Sb. v platném znění, resp. platných navazujících vyhlášek

1.2 Výstup č. 2: Metodika přípravy atestačního prostředí

Zhotovitel vypracuje dokument *Metodika přípravy atestačního prostředí*. Tento dokument bude součástí Provozního řádu atestačního střediska, bude veřejný a určený a závazný pro klienty atestačního střediska; dokument bude popisovat:

- zásady pro chování pracovníků klientů při vzdáleném přístupu k jim vyhražené virtuální infrastruktuře v prostředí Objednatele,
- pravidla a postupy pro instalaci jejich systému eSSL,
- pravidla provozu nainstalované instance eSSL
- pravidla pro instalaci dalších nezbytných aplikačních komponent nutných pro provozování eSSL v atestačním prostředí
- požadavky pro instalaci pracovní stanice pro klientské operace ve virtualizovaném hardwarovém prostředí Atestačního střediska
- pravidla pro vytvoření uživatelských účtů, organizační struktury, testovacích dat a další nastavení testované eSSL
- požadavky na dokumentaci, kterou má klient předat atestačnímu středisku v rámci instalace eSSL, popisující např. přístupové údaje pro jednotlivé vytvořené uživatelské účty eSSL, uživatelskou příručku eSSL, administrátorskou příručku eSSL, návod pro realizaci testovacích scénářů pro provedení atestace
- včetně závazku klienta dodržovat Bezpečnostní politiku atestačního střediska.

Zhotovitel při tvorbě dokumentu vezme v potaz fakt, že jimi instalovaná eSSL komunikuje nejméně s:

- Active directory atestačního střediska
- Interním emailovým serverem atestačního střediska
- Spolupracujícími systémy
- Potenciálně i dalšími systémy identifikovanými v rámci analýzy

Dokument *Metodika přípravy atestačního prostředí* bude obsahovat relevantní popis pro následující možnosti, provádění atestace:

a) ve virtualizovaném hardwarovém prostředí Objednatele (atestačního střediska),

b) na hardware klienta atestačního střediska umístěném v jeho prostředí, přičemž testeři mají k testované eSSL vzdálený přístup

c) v cloudovém prostředí zajištěném klientem atestačního střediska, přičemž testeři mají k testované eSSL vzdálený přístup

Pro případy, uvedené pod písmeny b) a c) bude dokument popisovat i jakým způsobem má Dodavatel eSSL nastavit přístup na spolupracující systémy, jak zajistit přístup k emailovému serveru atestačního střediska (pro testy emailové komunikace, včetně zavirované e-mailové komunikace) a jak zajistit služby active directory. Dokument bude součástí Provozního řádu atestačního střediska, tak jak je popsán v materiálu: „Postup Atestačního střediska pro elektronické systémy spisové služby při provádění atestace elektronického systému spisové služby, podmínky provádění atestace a výše úplaty za provedení atestace“, zveřejněného ve Věstníku ministerstva vnitra. Dokument musí respektovat podmínky, uvedené ve výše uvedeném materiálu.

1.3 Výstup č. 3: Interní podmínky provozu atestačního prostředí

Dokument bude popisovat koncepci, zásady a pravidla pro provoz virtualizovaného atestačního prostředí.

Dokument bude obsahovat také postupy, které bude vedoucí tester aplikovat pro uživatelské scénáře použití (viz bod 1.1), např. založení prostředí pro testování eSSL, vytvoření zálohy, ověření integrity zálohy apod.; tato část bude uvedena ve formě pracovní příručky a bude obsahovat pracovní návody, popis chybových stavů a způsoby jejich řešení.

1.4 Výstup č. 4: Provozní procesy a HelpDesk

Zhotovitel Objednateli navrhne a po jeho schválení dodá aplikaci typu HelpDesk pro použití v rámci atestačního střediska. Help-desk bude sloužit jako knowledge base, poradna pro Dodavatele a pro interní komunikaci testerů.

S využitím systému HelpDesk Zhotovitel navrhne a po schválení ze strany Objednatele implementuje procesy pro podporu svého plnění podle bodu 1.1:

- change managementu,
- incident managementu,
- patch managementu a release managementu,
- procesů zajištění kybernetické bezpečnosti

1.5 Výstup č. 5: Dokumentace systémového prostředí

Dokumentace musí být komplexní a úplná. Dokumentace vytvořená Zhotovitelem musí být v českém jazyce; dokumentace použitých systémů třetích stran je akceptována v anglickém jazyce.

Zhotovitel v rámci implementace dodá nejméně následující dokumentaci:

1.5.1 Instalační příručka

Instalační příručka popisuje instalaci všech provedených komponent, a to v takové kvalitě, aby instalaci byla schopna provést třetí strana s patřičnými technickými znalostmi. Specificky obsahuje:

1. popis instalačního balíku, jednoznačná identifikace, obsah
2. prerekvizity instalace
3. postup instalace, kontrolu logů, chybové stavy, adresářovou strukturu instalace (kde se co po instalaci nachází)
4. popis konfiguračních souborů a významu parametrů včetně požadovaného nastavení
5. konfigurace infrastrukturních prvků (sítě, prostupy ve firewallu, nastavení portů), pokud toto bude relevantní
6. certifikáty a klíče
7. konfigurace monitoringu, pokud bude pro řešení relevantní
8. dokumentace musí být komplexní a úplná a musí umožnit instalaci a konfiguraci systému třetí stranou.

1.5.2 Administrátorská příručka

Podle administrátorské příručky musí být administrátor systému schopen provádět veškeré činnosti, které jsou nutné pro provozování / údržbu řešení. Administrátorská příručka specificky obsahuje popis struktury komponent aplikace a pro každou komponentu:

1. popis výstupních hlášení jednotlivých komponent (např. skriptů), popis log souborů (tam, kde je relevantní) a způsob jejich vyhodnocování
2. popis chybových stavů a jejich nápravy
3. popis případných číselníků a jejich význam
4. dokumentace specifických nastavení jednotlivých komponent (např. nastavení hypervisorů, nastavení firewallu, prostupu na spolupracující systémy)
5. dokumentace veškerých provozních zásahů a úprav do výchozího nastavení operačních systémů
6. způsob otestování funkčnosti jednotlivých scénářů užití (např. založení prostředí pro testování eSSL, vytvoření zálohy, ověření integrity zálohy apod.)
7. popis zajištění aktualizací jednotlivých použitých programových komponent, i pro komponenty třetích stran (kde lze tento požadavek splnit odkazem na relevantní místo v dokumentaci Zhotovitele)
8. dokumentace případných změn v prostředí aplikace a podpůrných systémů

1.5.3 Systémová dokumentace

Systémová dokumentace popisuje koncepci a architekturu řešení. Dokumentace musí vysvětlit sadu problémů, které plnění řeší, alespoň stručně (bodově) popsat zvažované možnosti jejich řešení, jejich výhody, nevýhody a důvody pro výběr vybraného řešení detailně vysvětlit princip a architekturu vybraného řešení.

Systémová dokumentace je vytvořena zejména pro potřeby případného budoucího rozšiřování a případné integrace s jinými aplikacemi a systémy. Musí obsahovat popis architektury fungování jednotlivých komponent systému a popis případných rozhraní, popis toku, protokolů a předpokládaných objemů dat, požadavky na změny a nastavení systémů, které tvoří

bezprostřední okolí plnění, popis rolí a oprávnění, popis způsobu zajištění kybernetické bezpečnosti a licenční podmínky pro všechny komponenty plnění.

1.5.4 Programátorská dokumentace a zdrojové kódy

Součástí plnění je i předání zdrojových kódů pro komponenty vyvinuté Zhotovitelem. Zdrojový kód musí obsahovat komentáře nejméně ke každé použité funkci/proceduře/třídě/komponentě na takové úrovni, která umožní orientaci, porozumění kódu a jeho potenciální budoucí úpravy programátorům, kteří se na vývoji nepodíleli.

Pro případné využité komponenty třetích stran je požadavek na zdrojové kódy nahrazen požadavkem na předání soupisu těchto komponent, jejich licenčních ujednání.

1.5.5 Další dokumentace

Zhotovitel dále dodá:

- Hesla a šifrovací klíče (jsou-li použity)
- Bezpečnostní dokumentaci včetně havarijních plánů a plánů obnovy
- Externí knihovny, resp. kódy třetích stran nezbytné k funkčnímu sestavení aplikace včetně informace o licenčních pravidlech použitých software
- Skripty pro sestavení (jsou-li použity)
- Šablonu provozního deníku

Příloha č. 1: technické parametry výpočetní architektury atestačního střediska

Níže jsou uvedeny jednotlivé komponenty hardwarového řešení:

Servery

3x vSAN Ready Node R750

- R750 Motherboard with Broadcom 5720 Dual Port 1Gb OnBoard LOM
- Intel Xeon Silver 4316 2.3G, 20C/40T
- SAS/SATA/NVMe Capable Backplane
- 2.5" Chassis with up to 24 HDDS (SAS/SATA) including 4 Universal Slots for 1CPU
- PowerEdge 2U Standard Bezel
- Riser Config 8, 2x8 FH, 1x16 LP slots
- Hybrid, VSAN Ready Node
- IDM/Personality Module, VSANRN R750
- 12x 32GB RDIMM
- iDRAC9, Enterprise 15G
- 2x 1.92TB SSD SATA Read Intensive 6Gbps
- 10x 2.4TB 10K RPM SAS 12Gbps
- BOSSS2 controller card + with 2 M.2 240GB (RAID 1)
- Dell HBA355i Controller Front
- Dual, HotPlug,Power Supply Redundant (1+1), 1400W, Mixed Mode
- 2x C13 to C14, 2m, Power Cord
- Trusted Platform Module 2.0 V3
- Broadcom 57504 Quad Port 10/25GbE,SFP28, OCP NIC 3.0

Networking

Dell EMC Networking S5212F

- Dell EMC S5212F-ON Switch, 12x 25GbE SFP28, 3x 100GbE QSFP28 ports, IO to PSU air, 2x PSU
- 2x Jumper Cord - C13/C14, 2M, 250V, 10A (EU, TW, APCC countries except ANZ)
- 3x Dell Networking, Cable, SFP28 to SFP28, 25GbE, Passive Copper Twinax Direct Attach Cable, 5 Meter
- Dell NW Dual Tray, 4-post, S5212F-ON
- OS10 Enterprise, S5212F-ON
- Dell EMC Networking S5212F
- Dell EMC S5212F-ON Switch, 12x 25GbE SFP28, 3x 100GbE QSFP28 ports, IO to PSU air, 2x PSU
- 2x Jumper Cord - C13/C14, 2M, 250V, 10A (EU, TW, APCC countries except ANZ)
- 3x Dell Networking, Cable, SFP28 to SFP28, 25GbE, Passive Copper Twinax Direct Attach Cable, 5 Meter
- OS10 Enterprise, S5212F-ON

Licence virtualizační a SDS vrstvy

- 3x VMware vSphere Standard
  VMware vSphere 7 Standard, 1 CPU (max 32 cores/CPU socket), 1YR VMware SNS
- 3x VMware vSAN Standard
  VMware vSAN 7 Standard, 1 CPU (max 32 cores/CPU socket), 1YR VMware SNS
- VMware vCenter Standard
  VMware vCenter 7 Standard,Per Instance,1YR VMware SNS

Objednatel provedl na uvedeném hardwarovém řešení instalaci a implementaci v následujícím rozsahu:

- instalace dodávaných komponent
- zapojení dodávaného HW do stávající infrastruktury
- konfigurace HCI clusteru
- konfigurace virtualizační vrstvy
- otestování funkčnosti
- zpracování dokumentace, vypořádání připomínek