POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 08-2018

Poskytovatel	AutoCont CZ a.s.
Správce	
Objednatel	ČESKÁ REPUBLIKA - SPRÁVA ZÁKLADNÍCH REGISTRŮ
Smlouva	Č. SZR-374-74/Ř-2015
Název ZP	**Integrace HSM modulů do prostředí ISZR**
Číslo tiketu (ServisDesk)	1-267213900 / 29970
Katalogový list	**ISZR20**
Datum podání	12. 02. 2018
Priorita	Spěchá

1. Identifikace vzniku požadavku

Zadání požadavku emailem.

2. Zadání požadované změny - Integrace HSM modulů do prostředí ISZR

Jedná se tedy o tři témata, která se budou na HSM provozovat:

- Poskytovatel identity eOP, serverový MW
- NIA – úložiště certifikátů
- FAIS – Pečetění, časová razítka.

3. Popis zajištění realizace změny

- Viz vložená Příloha č. 1

4. Celková cena

Činnost	
Analýza: vytvoření dokumentu návrhu využíti sdílené kryptografické služby a jeho prezentace	
Provozní procedury - vytvoření dokumentů provozních procedur	
Školení: Příprava podkladů a vlastní školení (zaškolení, teoretická část a workshop)	
Inicializace kryptografických služeb	
Celkem	

- Cena celkem: **1 530 000,- Kč bez DPH**

5. Návrh harmonogramu změnového požadavku

- Zahájení realizace: do 10 dnů od objednávky.

6. Dopady do provozu / dopady do provozní dokumentace

- Nejpozději 30 pracovních dnů od schválení PnČ budou určeny dopady do provozu. Spolu s dopady do provozu bude připraven případný návrh promítnutí do katalogových listů provozní smlouvy.

7. Návrh testovacího scénáře

- Není relevantní

8. Požadavky na součinnosti

- Viz vložená Příloha č. 1

9. Výstupy změnového požadavku

- HSM moduly integrované do prostředí ISZR

	Schválil (poskytovatel)	Schválil (objednatel)
Jméno	[redacted]	
Datum		
Podpis		

Příloha č. 1 - Integrace HSM do prostředí SZR - popis

Předmět zakázky

Předmětem zakázky je koordinace integrace HSM modulů do prostředí SZR jako sdílené služby využívané jednotlivými komponentami, ze kterých se skládá nebo které využívá systém NIA. Jednotlivé dodávky jsou popsány v následujících kapitolách. V rámci dodávky bude zohledněno napojení subsystémů na HSM.

Základní zaškolení

Způsob dodávky: provedení školení v prostorách SZR a předání školicích materiálů (prezentace)

Rozsah: 1 den školení

Školení účastníky (pracovníci SZR, pracovníci dodavatelů komponent integrujících se na HSM) seznámí se základní filozofií, jakou zařízení z rodiny Thales nShield pracují s kryptografickým materiálem. Sumarizuje možnosti organizace práce s kryptografickým materiálem, možnosti přístupu k HSM z aplikací a z toho vyplývající nutné vlastnosti prostředí.

Analýza

Způsob dodávky: provedení analytických workshopů a jejich zaznamenání formou zápisu a

Rozsah:

- úvodní společný workshop – 1den
- analytický workshop pro každý integrovaný systém – 1 den na každý systém
- validační workshop pro každý systém – 1 den na každý systém
- dokument Analýza požadavků
- závěrečný společný koordinační a validační workshop – 1 den

Dodavatel zorganizuje a uspořádá v prostorách SZR analytické workshopy s technickými řešiteli jednotlivých systémů, které budou využívat HSM infrastruktury. Cílem workshopů bude sběr požadavků, které jednotlivé systému v oblasti kryptografie mají. Bude uspořádán úvodní workshop, pro získání vzájemného všeobecného přehledu. Následovat budou analytické workshopy s jednotlivými dodavateli, zpracování poznatků získaných na analytickém workshopu a jejich následná validace na validačním workshopu. Po validaci vstupů dodavatel zpracuje analytický dokument, který bude shrnovat požadavky na sdílenou kryptografickou infrastrukturu. Analytický dokument bude prezentován a validován na závěrečném koordinačním a validačním workshopu.

Návrh

Způsob dodávky: vytvoření dokumentu návrhu a jeho prezentace

Rozsah:

- dokument návrhu řešení
- workshop prezentující řešení - 1 den

Na základě informací získaných v rámci analýzy dodavatel vypracuje návrh řešení kryptografických služeb, kde bude popsána celková architektura řešení, způsob napojení jednotlivých systémů, procesy správy systému, způsob zabezpečení jednotlivých kryptografických klíčů, způsob zajištění monitoringu, zálohování, HA, DR a bezpečnostního dohledu. V návrhu bude rovněž definováno personální zajištění vyplývající z bezpečnostních požadavků, separace rolí a výčet provozních procedur.

Provozní procedury

Způsob dodávky: vytvoření dokumentů provozních procedur

Rozsah:

- provozní procedury určené v dokumentu návrhu
- workshop prezentující provozní procedury

Na základě schváleného návrhu řešení budou zpracovány provozní procedury pro jednotlivé provozní operace. Východiskem pro zpracování procedur jsou uživatelské manuály Thales, které jsou využity pro definici jednotlivých konkrétních postupů v prostředí SZR.

Školení pracovníků SZR

Způsob dodávky: teoretické školení a praktický workshop pro pracovníky SZR

Rozsah:

- teoretická část školení – 1 den
- praktický workshop – 1 den

Na základě provozních procedur a zvoleného návrhu řešení bude provedeno zaškolení klíčových pracovníků SZR, kteří se budou podílet na provozu kryptografické infrastruktury se zaměřením na problematiku nutnou v rámci provozních procedur.

Inicializace kryptografických služeb

Způsob dodávky: aktivní účast na „klíčové ceremonii“ při inicializaci HSM do prostředí SZR v roli koordinátora

Rozsah:

- zajištění koordinace klíčové ceremonie – 1 den

Procedura inicializace zajistí iniciální nastavení celého kryptografického prostředí. Dodavatel bude vystupovat v roli koordinátora a konzultanta pro řešení případných technických problémů v průběhu klíčové ceremonie.