POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 42-2017

Poskytovatel	AutoCont CZ a.s.
Správce	
Objednatel	ČESKÁ REPUBLIKA - SPRÁVA ZÁKLADNÍCH REGISTRŮ
Smlouva	Č. SZR-374-74/Ř-2015
Název ZP	**Zabezpečení kryptografických prostředků**
Číslo tiketu (ServisDesk)	1-262083824 / 28606
Katalogový list	**ISZR20**
Datum podání	28. 11. 2017
Priorita	-

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServisDesk.

2. Zadání požadované změny

Realizace SW/HW řešení, jehož prostřednictvím bude v rámci systémů ISZR a FAIS zajištěno odpovídající zabezpečení kryptografických prostředků určených pro:

- Autentizaci systémů ISZR, FAIS určených pro vnitřní komunikaci

- Autentizaci systémů ISZR, FAIS určených pro vnější komunikaci s ostatními subsystémy systému ZR a spolupracujícími AIS

- Podepisování/pečetění výpisů ze systému ZR.

3. Popis zajištění realizace změny

Požadovaná změna bude realizována dodáním potřebného HW vybavení. Nedílnou součástí dodávky bude provedení základního oživení HW.

3.1 Dodávka a instalace HW

Specifikace dodávaných kryptografických síťových HSM modulů (HSM Thales nShield Connect 1500+), včetně roční maintenance a fyzické instalace:

Kód položky	Popis položky	Počet
NH2061	nShield Connect 1500+ F3; SEE Ready (no nTokens)	4
EM-STANDARD	Standard Support - 1 year - nShield Connect 1500+ F3	4
nH1991-CL	Additional 'soft' Client Licence - [does not include nToken]	8
EM-STANDARD	Standard Support - 1 year -Additional soft Client Licence	4

FE1637L	Elliptic Curve ['ECC'] Activation	4
EM-STANDARD	Standard Support - 1 year -ECC	4
AC2050	Rail Kit for nShield Connect	4

Dodání a instalace HW proběhne na základě schválení tohoto PnČ.

4. Cenová kalkulace

Předmětem této cenové kalkulace není integrace HW do systémů ISZR a FAIS. Tato integrace bude řešena samostatným PnČ.

Dodávka a instalace HW

Cena HW specifikovaného v bodu 3.1 je **3 190 000 Kč bez DPH**.

Celková cena HW včetně DPH 21% činí 3 859 900 Kč.

Cena HW je včetně instalace.

5. Návrh harmonogramu změnového požadavku

Dodávka a instalace HW proběhne do 18 dnů od schválení PnČ k realizaci.

Předpokládaný termín: Q4/2017.

6. Dopady do provozu / dopady do provozní dokumentace

Nejsou.

7. Návrh testovacího scénáře

Testovací scénáře pro dodání HW a jeho instalaci nejsou relevantní.

Akceptační kritéria jsou uvedena v bodu 9.

8. Požadavky na součinnost

Požadovaná součinnost SZR:

- zajištění služeb datových center (včetně specifikace požadovaného umístění v DC) a konektivity;
- souhlas s rizikovými činnostmi / odstávkami v průběhu instalace HW.

9. Výstupy změnového požadavku

Dodávka a instalace HW

Výstupem bude HW dodaný dle specifikace v bodu 3.1.

Akceptace proběhne na základě Předávacího protokolu.

	Schválil (poskytovatel)	Schválil (objednatel)
Jméno	[redacted]	[redacted]
Datum	29. 11. 2017	29. 11. 2017
Podpis		

Příloha č .1 – podrobná specifikace

Technické parametry pořizovaného zařízení:

- modul pracuje jako síťový, je dostupný bezpečným způsobem pomocí sítě vzdáleně (L2/L3);
- modul poskytuje pro správu a používání klíčů standardní rozhraní (PKCS#11, CryptoAPI);
- modul poskytuje oddělení rolí bezpečnostního správce a běžného uživatele s autentizací jednotlivých rolí PINem;
- modul poskytuje prostřednictvím rozhraní operace
  - generování klíče AES délky 256 bitů uvnitř modulu exportovatelného v zašifrovaném tvaru;
  - import šifrovacího klíče AES délky 256 bitů pro šifrovaný export klíče;
  - operace AES šifrování a dešifrování pomocí klíče AES;
- modul poskytuje úroveň bezpečnosti dle FIPS 140-2 úrovně 3;
- modul umožňuje provoz v HA režimu pomocí více modulů v režimu automatického failover;
- modul umožňuje load-balancing na úrovni ovladačů;
- modul umožňuje sdílení centrální bezpečnostní konfigurace napříč několika moduly;
- modul umožňuje bezpečné zálohování a obnovu centrální bezpečnostní konfigurace včetně klíčů;
- modul podporuje přístup pomocí PKCS#11 z prostředí OS Windows server;
- modul poskytuje možnost monitoringu pomocí SNMPv3, SNMP trap a syslog;
- modul umožňuje redundantní připojení pomocí dvojice ethernetových portů alespoň 2x1Gbit;
- modul umožňuje konfiguraci, kdy je možné bezpečně využívat různé sady klíčů různými aplikacemi tak, aby byly bezpečně odděleny;
- modul poskytuje výkon 50 AES256 šifrování za vteřinu;
- modul poskytuje výkon 1000 RSA 1024 operací za vteřinu;
- modul je možné využívat minimálně ze 4 serverů s možností rozšíření až na 16 serverů;
- modul poskytuje možnost bezpečného vykonávání uživatelského kódu ve vnitřním bezpečném prostředí;
- modul podporuje kryptografii založenou na eliptických křivkách (ECC);