POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 15-2017

Poskytovatel	AutoCont CZ a.s.
Správce	
Objednatel	ČESKÁ REPUBLIKA - SPRÁVA ZÁKLADNÍCH REGISTRŮ
Smlouva	Č. SZR-374-74/Ř-2015
Název ZP	**Změny na Certifikačních autoritách ISZR, navýšení délky klíče – 1. část**
Číslo tiketu (ServisDesk)	1-252280689 / 25640, 25915
Katalogový list	**KL 20**
Datum podání	08. 06. 2017
Priorita	-

1. Identifikace vzniku požadavku

zadání požadavku na ServisDesk

2. Zadání požadované změny

Implementace následujících změn na Certifikačních autoritách ISZR:

1. Změna minimální délky klíče v žádosti pro testovací prostředí z 1024 na 2048 bitů.

2. Změna doby platnosti certifikátů pro testovací prostředí z 1 na 3 roky.

3. V technických žádostech o certifikáty povinně používat hash funkci SHA256. Dosud možno i SHA1. Platí pro obě prostředí.

Opatření 3 bude realizováno v obou prostředích postupně s odstupem v řádu měsíců.

3. Popis zajištění realizace změny

1. Změna minimální délky klíče

   Zabezpečíme nastavení minimální délky klíče akceptovatelné žádosti pro testovací prostředí na 2048 bitů.

Naše řešení se netýká úpravy manuálu „Postup pro generování asymetrického klíčového páru“, to zajistí SZR.

2. Změna doby platnosti certifikátů

   V návaznosti na bod 1. bude s délkou klíče 2048 bitů svázána platnost certifikátu na 3 roky.

   Vytvoření certifikátu s platností 1 rok bude tedy znemožněno.

3. Technické žádosti – hash funkce SHA256

   Certifikáty obsahují sice Thumbprint SHA1, což je ale vlastnost pouze připojená k objektu certifikátu pomocí subsystému CryptoAPI a tato hodnota je vždy SHA1. Thumbprint se používá pouze k nalezení požadovaného certifikátu v databázi. Podpis je součástí digitálního certifikátu a slouží k ověření podpisu certifikátu a ten je SHA256RSA.

   Použití SHA256 je tedy nastavené, proto není třeba nic měnit.

4. Odhad pracnosti

Činnost	
Analýza, návrh řešení, realizace, otestování	
Celkem	

Celková cena: 30 000,- Kč bez DPH

5. Návrh harmonogramu změnového požadavku

S ohledem na rozsah pracnosti není relevantní.

6. Dopady do provozu / dopady do provozní dokumentace

Dopady do provozu neočekáváme.

Změny se promítnou do příslušné provozní dokumentace.

7. Návrh testovacího scénáře

Ověření znemožnění vytvoření certifikátu s délkou klíče 1024 bitů.

Ověření, že je při vytvoření certifikátu nastavena platnost na 3 roky.

8. Požadavky na součinnosti

Nejsou.

9. Výstupy změnového požadavku

	Schválil (AutoCont CZ)	Schválil (zákazník)
Jméno		
Datum	19. 6. 2017	19. 6. 2017
Podpis		