

**POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 42**

<b>Poskytovatel služby</b>	Pasante s.r.o. Hybernská 1007/20, 110 00 Praha 1
<b>Správce IS</b>	Správa základních registrů, 130 00 Praha 3 Na Vápence 14
<b>Objednatel</b>	Správa základních registrů, 130 00 Praha 3 Na Vápence 14
<b>Smlouva</b>	Smlouva o poskytování služeb podpory provozu a rozvoje RAZR, č.: SZR-1658-17/OEM-2017
<b>Číslo RFC SZR</b>	<b>1196</b>
<b>Název RFC SZR</b>	<b>RAZR – Prodloužení RSA klíče a další úpravy pro DIA</b>
<b>Kategorie RFC</b>	<b>Change</b>
<b>Číslo tiketu (Service Desk)</b>	128087
<b>Katalogový list</b>	<b>RAZR10 - objednávka</b>
<b>Typ odstavky</b>	Zero

**1. Identifikace vzniku požadavku**

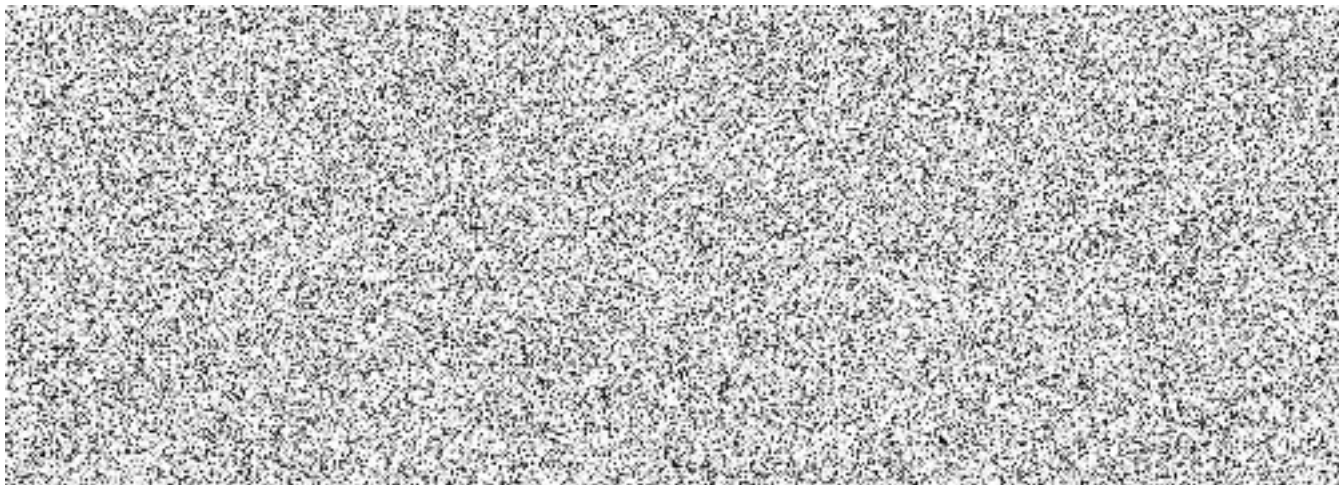
- Pro posílení bezpečnosti PKI SZR/DIA je nutné podporovat bezpečnější kryptografické funkce. Prodloužení RSA klíče na minimálně 3072 bitů je požadavek NÚKIB. Použití hash funkce SHA384 je doporučení NÚKIB.
- K 1.4.2023 přechází SZR pod organizační složku Česká republika – Digitální a informační agentura (DIA). V rámci této transformace je zapotřebí zajistit úpravy RAZR, a to zejména:
  - náhrada odkazů na SZR,
  - změna IČO ve volání služeb základních registrů,
  - výměna certifikátů vydaných pro SZR.

**2. Zadání požadované změny**

- Vyměnit certifikáty pro přístup RAZR do základních registrů. Výměna se týká pouze Interních modulů RAZR-produkce a RAZR-test.
- Ve voláních služeb ISZR uvádět místo dosavadního IČO SZR (72054506) nově IČO DIA (17651921). Změna se týká pouze Interních modulů RAZR-produkce a RAZR-test.
- Nastavit požadovanou minimální délku klíče v technických žádostech o certifikát jako parametr v konfiguraci RAZR.



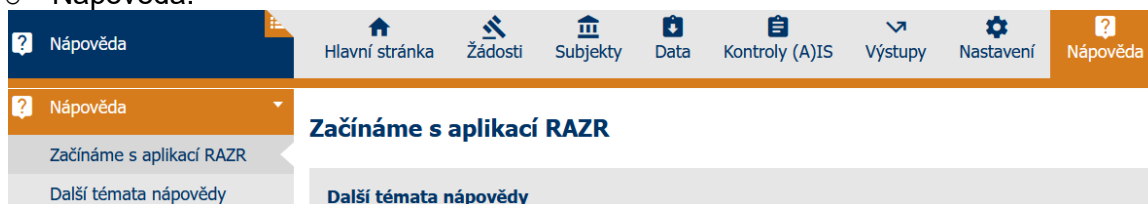
The screenshot shows a web application interface with a navigation bar at the top containing icons for 'Nastavení', 'Hlavní stránka', 'Žadosti', 'Subjekty', 'Data', 'Kontroly (A)IS', 'Výstupy', and 'Nastavení'. Below the navigation bar, there is a sidebar with 'Nastavení žádostí' and 'Nastavení aplikace'. The main content area displays 'Základní nastavení aplikace' with a progress indicator below it.



- Do sekce certifikáty přidat parametr "Minimální délka klíče".
- Počáteční hodnotu nastavit na 2048.
- Přípustné hodnoty jsou násobky čísla 1024 (ne nula).
- Náповěda k parametru:
  - Požadovaná minimální délka klíče v žádostech o certifikáty.
  - Přípustné hodnoty jsou násobky čísla 1024.
- Logem DIA nahradit ve všech modulech logo RAZR:



- Nahradit ve všech modulech RAZR odkazy na SZR odkazy na DIA.
  - Tj. text "Správa základních registrů" nahradit textem "Digitální a informační agentura" a zkratku SZR zkratkou DIA.
  - Změna se netýká DNS domén szrcr.cz a szr.local a AD domény jménem "SZR". Tyto domény se zatím nemění.
  - Požadavek se týká všech odkazů ve všech modulech RAZR s výjimkou následujících textů:
    - Aktuality RAZR ze "Zprávy na hlavní stránce" / Nastavení.
    - Všechny "Nastavení žádostí" (Nastavení žádostí, Textace tisků, Funkce, Texty sdělení) z Nastavení.
    - "Nastavení textu pro web" z Nastavení aplikace / Nastavení.
    - Náповěda:



- Změna přihlašovacích údajů pro WS GINIS:
  - dodá SZR – změna bude v přihlašovacím jménu a url,
  - certifikát zůstává stejný.



### 3. Popis zajištění realizace změny

- Požadované změny jsou na sobě nezávislé a lze je dělat v libovolném pořadí.
- Vydání certifikátů zajistí SZR.
  - SZR předá certifikáty a soukromé klíče firmě Pasante.
  - Pasante nasadí certifikáty a soukromé klíče na příslušné servery.
- Logo DIA zatím existuje prozatímní.
  - Pasante provede další výměnu, a to finální verzi loga.

Prozatímní logo:

**Digitální a informační  
agentura**

### 4. Pracnost

- Analýza
- Zpracování / Implementace:
  - Výměna SSL certifikátů a konfiguračních souborů mimo standartní vypršení platnosti
  - Nové IČO ve volání služeb ISZR – externí funkce a IszrService
  - Minimální délka klíče
  - Nahradit texty a prozatímní logo v RAZR (formuláře, nahlížečící stránky, šablony)
  - Nahradit texty a prozatímní logo na webech [egon.gov.cz](http://egon.gov.cz) a [egon.cms2.cz](http://egon.cms2.cz)
  - Nahradit prozatímní logo konečným logem
- Testování:
  - Texty, loga, šablony
  - Ověření vrácení stejných dat při různých hodnotách IČO (test / produkce)
- Úprava dokumentace
- Release (razr, služby, weby)

**Celková pracnost: 132 437,50 Kč bez DPH,  
tj. 160 249,38 Kč s DPH**

*Poznámka: Článek 5.1.2 Smlouvy „Cena služeb na objednávku“, Katalogový list RAZR10 „Optimalizace parametrů poskytovaných služeb ZR“ – tento KL v rámci tohoto PnČ neslouží k pracím, které vedou k navýšení stávajících funkcionalit, a tedy k technickému zhodnocení IS dle vyhlášky č. 410/2009 Sb., k provedení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů pro vybrané jednotky. V rámci PnČ 2023-42 nebudou prováděny žádné rozvojové činnosti.*

Poskytovatel služby (dále jen „Pasante“) bere na vědomí, že předmět plnění tohoto PnČ č. 42 je spolufinancován z fondů Evropské unie, konkrétně z programu Národní plán obnovy (dále jen „NPO“), v rámci pilíře Digitální transformace, pro projekt, který byl zahrnut do projektu s názvem „Budování referenčního rozhraní propojeného datového fondu“ (dále jen „projekt“) s registračním číslem projektu: CZ.31.1.01/MV/22\_22/0000022. Pasante v této souvislosti bere na vědomí, že je povinen plnit některé další povinnosti vyplývající z podmínek realizace projektu, a to uchovávat veškerou dokumentaci související s realizací poskytnutého plnění dle tohoto PnČ č. 42, včetně všech účetních dokladů, nejméně po dobu 10 let ode dne schválení závěrečné zprávy o projektu, s tím, že o datu jejího schválení bude Pasante ze strany SZR informován po skončení projektu.

Faktura za plnění dle tohoto PnČ č. 42 bude obsahovat údaje o názvu projektu a registrační číslo projektu, viz identifikace výše.

## 5. Harmonogram změnového požadavku

- Úprava systému a testování: do 27.3.2023
- **Nasazení do produkčního prostředí: 31.3.2023**
- Termín dodání: nejpozději do 15.4.2023

Termín dodání může být prodloužen v případě neposkytnutí nezbytné součinnosti dle bodu 9. tohoto PnČ, nebo z dalších důvodů na straně objednatele. Nejzazší termín dodání je však 30.9.2023.

## 6. Testovací scénáře

- Vyzkoušet správné fungování parametru pro zadání minimální délky klíče v žádostech o certifikáty.
- Porovnat data přečtená z testovacího RPP před provedením změn s daty přečtenými z testovacího RPP po provedení změn. Data by měla být stejná.
- Porovnat data přečtená z produkčního RPP před provedením změn s daty přečtenými z produkčního RPP po provedení změn. Data by měla být stejná.

## 7. Výstupy změnového požadavku

- Nová verze RAZR s úpravami uvedenými v tomto dokumentu.
- Upravená dokumentace RAZR.

## 8. Akceptační kritéria, způsob ověření na produkci

- Akceptační kritéria:
  - Úspěšné otestování změn v testovacím prostředí RAZR.
  - Úspěšné otestování změn v produkčním prostředí RAZR.
  - Technická dokumentace RAZR odpovídá skutečnému stavu po implementaci změnového požadavku.
- Způsob ověření na produkci:
  - Kontrola přítomnosti změn v produkčním prostředí RAZR.

## 9. Požadavky na součinnosti

- SZR zajistí vydání nových certifikátů pro RAZR.
- SZR zajistí logo DIA pro RAZR.



## 10. Dopady do provozu / dopady do provozní dokumentace

- Úprava technické a procesní dokumentace - zajistí Pasante.
- Úprava Příručky RAZR pro SZR - zajistí SZR.

Služby definované v čl. 3. „Popis zajištění realizace změny“ tohoto PnČ nebudou generovat další dodatečné finanční prostředky na podporu provozu daného IS.

## 11. Dopady na bezpečnost IS / dopady do bezpečnostní dokumentace

- Posílení bezpečnosti PKI SZR/DIA.
  - Do Základního nastavení konfigurace RAZR doplněn nový parametr pro nastavení minimální délky klíče v technických žádostech o certifikát.
- Bezpečnostní politika bude aktualizovaná – další revize dokumentace RAZR proběhne v dubnu 2023.

