

POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 72-2024

Poskytovatel	Aricoma Systems a.s.
Správce IS	Digitální a informační agentura
Objednatel	Digitální a informační agentura, Na Vápence 915/14, 130 00 Praha 3
Smlouva	SZR- 4231-15/Ř-2020
Číslo RFC	RFC 1514
Název RFC	ISZR_Zajištění pečetění dokumentů časovým razítkem pro PO prostřednictvím služby realizované na FAIS
Kategorie RFC	Change
Číslo tiketu (ServisDesk)	RITM0129953 / 190628
Katalogový list	ISRZ05 - objednávka
Typ odstavky	Bez odstavky

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServisDesk viz tiket RITM0129953 / 190628 ze dne 29.11.2024.

2. Zadání požadované změny

Žádáme o zajištění pečetění dokumentů časovým razítkem pro Portál občana prostřednictvím služby realizované na FAIS.

Cílem je vystavit službu FAIS pro pečetění na rozhraní ISZR tak, aby tuto službu mohly standartním postupem i další projekty DIA.

3. Popis zajištění realizace změny

Na vnějším rozhraní ISZR bude vystavena nová neveřejná eGON služba, který provede pečetění PDF dokumentu.

- *E357 - iszrRrZpracujPecet*

Služba bude dostupná a sdílená pro všechny systémy, které budou potřebovat pečeti a razítkovat na základě oprávnění k přístupu přes RAZR.

ISZR povolí přístup ke službě systémům, kterým bude přiřazen konkrétní bezpečnostní profil. Konkrétní bezpečnostní profil bude nastavitelný v konfiguraci ISZR.

- Pokud nebude mít žadatel přiřazen definovaný BP, bude zpracování ukončeno stavem CHYBA.

Pro razítkování bude použita služba definovaného externího poskytovatele kvalifikovaných časových razítek. V rámci implementace bude provedena a ověřena integrace na jednoho konkrétního poskytovatele kvalifikovaného časového razítka poskytujícího službu pro vydání razítka dle RFC 3161 (I.CA).

Služba E357 bude pro pečetění používat nový definovaný kvalifikovaný certifikát od externí CA, který bude vybrán dle konfigurace ISZR na základě vstupu služby.

ISZR dle vstupu služby a interní konfigurace vybere odpovídající proxy modul zabezpečující pečetění konkrétním kvalifikovaným certifikátem.

Na vstupu služby bude existovat parametr, prostřednictvím kterého bude možné zvolit konkrétní konfiguraci.

- Pokud nebude v žádosti uvedena platná konfigurace, bude zpracování ukončeno stavem CHYBA.

Při zpracování se provede volání proxy modulu, kterému se předá vstupní PDF, na výstup služby bude vráceno pečetěné PDF.

3.1 Technické řešení

3.1.1 Pečetění

- Kvalifikovaný certifikát bude uložen v existujících HSM modulech.
- Komunikaci na HSM moduly realizuje proxy modul zařazený mezi eGON službu a HSM modul.
- Proxy modul je univerzální / konfigurovatelný, pro jeden kvalifikovaný certifikát musí být použita individuální konfigurace proxy modulu.
- Ve stávajícím prostředí ISZR existuje právě jedna konfigurace pro pečeť DIA-FAIS (vydaná NCA).
- Do prostředí bude doplněn další proxy modul s konfigurací pro nový kvalifikovaný certifikát.

3.1.2 Razítkování

- Ve stávajícím prostředí je jako poskytovatel časových razítek využívána služba NCA.
- Ve službě E357 bude implementována možnost konfigurace a napojení na zvoleného dalšího konkrétního poskytovatele kvalifikovaných časových razítek.

3.2 Infrastruktura

Více konfigurací proxy modulu je možné provozovat na jednom serveru. To je podstatné z toho důvodu, že pečetění na HSM modulu je licencováno dle počtu unikátních IP adres, ze kterých pečetění probíhá. Není licenčně povoleno řešení umístěním za NAT IP adresu.

Změny v infrastruktuře v návaznosti na nasazené řešení bez požadavku na navýšení počtu licencí HSM modulů.

3.3 Konfigurace

- Instalace kvalifikovaného certifikátu do stávajících HSM.
- Vytvoření nové instance proxy modulu s konfigurací pro nový certifikát na stávajících serverech.
- Konfigurace eGON služby na nově nakonfigurovaný proxy modul.
- Konfigurace eGON služby na službu poskytující časová razítka.

3.4 Rozsah řešení

V rámci tohoto PnČ je řešena implementace eGON služby a **konfigurace prostředí ISZR pro jednu pečeť a jednoho poskytovatele časových razítek.**

Případná konfigurace pro další kvalifikovanou pečeť nebo poskytovatele kvalifikovaných časových razítek by byla řešena samostatným PnČ.

4. Odhad pracnosti

Činnost	Pracnost MD
---------	-------------

Analytik	
Architekt	
Programátor	
Bezpečnostní architekt	
Bezpečnostní specialista	
Tester	
Projektový manažer	
Celkem	33

Celková cena činí 490 050,00 Kč bez DPH, tj. 592 960,50 Kč včetně DPH.

5. Návrh harmonogramu změnového požadavku

Harmonogram realizace požadavku se bude řídit datem objednání a platným Release kalendářem.

Nasazení aplikace ISZR do testovacího prostředí bude provedeno do 30 pracovních dnů od objednání změny.

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 31.12.2025.

6. Návrh testovacího scénáře

Konfiguraci produkčního prostředí HSM, respektive služby poskytovatele časových razítek bude nutné pro provedení testů zpřístupnit v testovacím prostředí.

- Volání nové služby žadatelem bez oprávnění
 - CHYBA,
- Volání nové služby oprávněným žadatelem s neplatným požadavkem (nenakonfigurovaný kvalifikovaný certifikát),
 - CHYBA
- Volání nové služby oprávněným žadatelem s nedostupným poskytovatelem časových razítek,
 - CHYBA
- Volání nové služby oprávněným žadatelem s platným požadavkem (nakonfigurovaný kvalifikovaný certifikát).
 - Pečetěný PDF dokument opatřený časovým razítkem dle platné konfigurace.

7. Výstupy změnového požadavku

- Nová verze ISZR.

8. Akceptační kritéria, způsob ověření na produkci

8.1 Akceptační kritéria

Cílem je vystavit službu FAIS pro pečetění na rozhraní ISZR tak, aby tuto službu mohly standartním postupem využívat i další projekty DIA.

8.2 Způsob ověření na produkci

- Předání dokumentu pdf do služby, vrácení dokumentu s pečeti.

9. Požadavky na součinnosti

9.1 DIA

- Zajištění kvalifikovaného certifikátu,
- Zajištění služby poskytování kvalifikovaného časového razítka.
- Součinnost při akceptaci.

10. Dopady do provozu / dopady do provozní dokumentace / dopady na finanční prostředky na podporu provozu daného IS

- Bez dopadu.

10.1 Náklady na podporu provozu IS

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

11. Dopady na bezpečnost IS / dopady do bezpečnostní dokumentace

- Bez dopadu.

	Schválil (poskytovatel)	Schválil (objednatel)
Jméno		
Datum		
Podpis		