

POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK

Č. 3

Poskytovatel	Pasante s.r.o.
Správce	SZR
Objednatel	SZR
Smlouva	SMLOUVA O POSKYTOVÁNÍ SLUŽEB PODPORY PROVOZU A ROZVOJE RAZR
Název ZP	Zajištění podpory a vydávání certifikátů pro eGSB
Číslo ticketu (ServisDesk)	36750 , 57585
Katalogový list	RAZR10 - objednávka
Datum podání	29.11.2018
Priorita	normální

1. Identifikace vzniku požadavku

Na základě požadavků od MVČR (pan Tiller) a OVM je třeba zajistit vydávání certifikátů AIS, které podporují specifikaci eGSB. Současně je třeba umožnit vydání dalšího certifikátu pro AIS se zachováním platnosti původního certifikátu (po předem definovanou dobu).

2. Zadání požadované změny

2.1 Pravidla

Každý AIS může mít pouze jeden certifikát pro testovací prostředí a jeden pro produkční prostředí s výjimkou 3 měsíců před uplynutím platnosti certifikátu, kdy mu RAZR umožní získání nového certifikátu. RAZR umožní získání druhého certifikátu pro AIS také v případě, že se správce AIS při žádosti o druhý certifikát zaváže, že požádá o jeho zneplatnění do 3 měsíců od vydání nového certifikátu a potvrdí, že souhlasí s tím, že SZR mu certifikát zneplatní, pokud tak neučiní.

V certifikátech mohou být pouze atributy povolené v profilu certifikátu. Profil je definovaný v Certifikační politice SZR (http://www.szrcr.cz/uploads/Vyvojari/POL008B_2013_Certifikacni_politika_SZR.pdf) v kapitole 7.1. Navíc přibude atribut Subject Alternative Name (SAN).

2.1.1 KIVS modul

Změna údajů
**Certifikáty /
IP Adresy**
Agendy
Rekapitulace

Certifikáty

Platné certifikáty 1 / 1

Zneplatnit	Sériové číslo	Žádost o certifikát	Platnost od	Platnost do	Certifikát
<input type="checkbox"/>	53489850000100002367		06.06.2017	05.06.2020	

Důvod zneplatnění ?

Žádost o vydání / zneplatnění certifikátu

Odesláním žádosti o certifikát správce (A)IS potvrzuje:

- že si je vědom své plné odpovědnosti za jednoznačnou autentizaci a autorizaci všech osob, které budou při výkonu své působnosti v zaregistrované agendě prostřednictvím agendového informačního systému přistupovat ke službám vnějšího rozhraní informačního systému základních registrů, a že tyto osoby budou k dané činnosti oprávněny,
- že se seznámil s dokumentem Certifikační politika SZR, a že se zavazuje certifikační politiku SZR dodržovat,
- že jeho (A)IS splňuje podmínky dokumentu Bezpečnostní požadavky na (A)IS pro připojení k produkčnímu prostředí Základních registrů.

Soubor s žádostí o certifikát ?

Změny:

- Umožnit vydání certifikátu i v případě, že AIS již certifikát má, certifikát bude platný víc jak 3 měsíce a správce AIS nežádá současně o zneplatnění dříve vydaných certifikátů.
- Upravit text:

Odesláním žádosti o certifikát správce AIS potvrzuje:

- že si je vědom své plné odpovědnosti za jednoznačnou autentizaci a autorizaci všech osob, které budou při výkonu své působnosti prostřednictvím AIS používat služby základních registrů, a za to, že tyto osoby budou k takové činnosti oprávněny,
 - že se seznámil s dokumentem [Certifikační politika SZR](#), a že se zavazuje tuto certifikační politiku dodržovat,
 - že AIS splňuje podmínky dokumentu Bezpečnostní požadavky na AIS pro připojení k základním registrům,
 - že požádá do 3 měsíců od vydání certifikátu o zneplatnění všech případně ještě v té době platných dříve vydaných certifikátů pro AIS a že si je vědom toho, že SZR tyto certifikáty zneplatní, pokud tak neučiní,
 - že si je vědom toho, že SZR může žádost o druhý certifikát odmítnout a že tak učiní zejména v případě opakovaných žádostí o druhý certifikát.
- Když uživatel vybere soubor s žádostí o certifikát, RAZR zkontroluje obsah. Úprava kontrol:
 - Povolit pouze atributy definované v profilu. Pokud žádost obsahuje nepovolený atribut, žádost odmítnout a zobrazit zprávu:

Žádost o certifikát obsahuje nepovolený atribut XXXXX. V žádosti je možné uvádět pouze atributy povolené Certifikační politikou v profilu certifikátu.

- K existujícím kontrolám přidat kontrolu atributů CN (Common Name) a SAN. Atributů SAN může být víc. Pokud ani jeden z atributů SAN a ni CN neobsahuje jméno z domény cms2.cz, RAZR zobrazí zprávu:

Certifikát, který bude vydán na základě zadané žádosti, nebude možné použít pro publikaci prostřednictvím eGON Service Bus. Pokud certifikát chcete pro tento účel využívat, musí aspoň jeden z atributů Common Name a Subject Alternative Name obsahovat jméno z domény cms2.cz, např. server.ovm.cms2.cz

Poznámky:

- Podtržený text Certifikační politika SZR je odkaz na http://www.szrcr.cz/uploads/Vyvojari/POL008B_2013_Certifikac_ni_politika_SZR.pdf

2.2 Interní modul

Změny:

1. Umožnit vydání certifikátu i v případě, že AIS již certifikát má, "starý" certifikát bude platný víc jak 3 měsíce a správce AIS nežádá současně o zneplatnění dříve vydaných certifikátů.
2. Umožnit vydání maximálně jednoho certifikátu za podmínek z bodu 1. Tj. AIS může mít maximálně 2 certifikáty.
3. Upozorňovat automaticky na situace, kdy AIS má více platných certifikátů a od vydání posledního uplynuly 3 měsíce a aspoň jeden z ostatních certifikátů má platnost ještě aspoň týden.
4. Evidovat pokusy obcházet pravidlo o jednom certifikátu opakovanými žádostmi o druhý certifikát a upozorňovat na ně. Eviduje se u subjektu, tj. za všechny jeho AIS.
5. Evidovat subjekty, které nedodržují pravidla a nežádají samy včas o zneplatnění "starého" certifikátu. Eviduje se u subjektu, tj. za všechny jeho AIS.

2.3 Algoritmus

- Mám platný certifikát pro AIS ještě víc jak 3 měsíce.
- Zažádám si o další.
- V případě, že nejde o AIS, který má výjimku na počet certifikátů, RAZR zkontroluje, kolikrát jsem za posledních 12 měsíců žádal o druhý certifikát mimo tříměsíční lhůtu před koncem platnosti starého certifikátu pro jakýkoli AIS, jehož jsem správcem. RAZR upozorní interního uživatele, pokud jsem žádal již aspoň jednou a zobrazí mu data takových žádostí za všechny AIS, jejichž jsem správcem, za posledních 12 měsíců a u každého, zda byl certifikát vydán nebo ne.
- Interní uživatel uváží, zda povolí vydání, nebo ho odmítne.
- Dostanu další certifikát na 3 roky s podmínkou, že jeden z platných certifikátů (může to být i ten nový) musí být do 3 měsíců od vydání nového zneplatněn. Tj. 3 měsíce je maximální doba, po kterou můžu mít, pro jeden AIS standardně (tj. pokud AIS nemá výjimku) 2 platné certifikáty.
- Situaci mohu během 3 měsíců od vydání posledního certifikátu vyřešit jedním z následujících způsobů:
 - Požádám o zneplatnění jednoho z certifikátů, buď starého, nebo nového.
 - Požádám v jedné žádosti o zneplatnění obou platných certifikátů a o vydání nového.
- Pokud do 3 měsíců situaci nevyřeším,
 - SZR mi nejstarší platný certifikát pro AIS zneplatní,






- RAZR si u mne poznamená, že nedodržují pravidla,
- SZR pošle Sdělení o zneplatnění certifikátu.


2.4 Kontrola každý den pro všechny AIS:


- Najít AIS, které mají 2 nebo více platné certifikáty a AIS nemá zaškrtnutou výjimku na více certifikátů.
- Má 2:
 - Překryv platnosti certifikátů je maximálně 3 měsíce a jeden týden -> OK
- Má více než 2 platné, nebo se překrývají o více než 3 měsíce a jeden týden:
 - Ponechat pouze nejnovější certifikát, ostatní navrhnout k zneplatnění.
 - Automaticky vytvořit žádost pro AIS a napsat do ní certifikáty k zneplatnění.
 - V automatickém režimu:
 - RAZR pošle vybrané skupině interních uživatelů, že mají zablokovat SN certifikátů v Řídícím pultu ISZR
 - V manuálním režimu:
 - uživatel musí SN zneplatnění certifikátů v žádosti ručně potvrdit
 - uživatel podle uvážení zablokuje nebo nezablokuje certifikát v Řídícím pultu ISZR (na RAZR nemá dopad)
 - Interní modul předá SN certifikátů e-mailem certifikační autoritě.
 - RAZR vygeneruje sdělení o zneplatnění certifikátu.
 - RAZR předá sdělení do KIVS modulu.
 - Interní uživatel předá sdělení do GINIS.

3. Odhad pracnosti

- Analýza – ~~300~~
- Úprava validací csr v ngef.dll - ~~300~~
- Úprava textu ve formuláři žádosti - ~~20~~
- Úprava kontroly obsahu csr v ngef.dll – ~~20~~
- Automatické upozornění na více certifikátů – ~~30~~
 - INTService projde všechny AIS, které nemají výjimku pro více cert a pokud AIS má více jak 1 certifikát a doba od vydání posledního je 3 měsíce a aspoň jeden z ostatních certifikátů má platnost alespoň ještě týden, pak se odešle upozorňovací e-mail na e-mailovou adresu nastavenou v základním nastavení RAZR
 - Vytvoření nového pole v základním nastavení
 - Úprava INTService
- Evidence o druhých certifikátech pro AIS bez výjimky a s mezerou větší než 3 měsíce – ~~30~~
 - Nový vnořený formulář u subjektu – záznam o pokusu o žádosti o cert
 - Při odeslání žádosti na SZR se zkontroluje zda se nežadá o certifikát i přes podmínku, pokud ano zaznamená se tato žádost k subjektu.
 - Úprava skriptu na tlačítku pro odeslání na SZR
- Evidovat subjekty, které nedodržují pravidla a nežadají samy včas o zneplatnění "starého" certifikátu - ~~300~~
 - Nový vnořený formulář u subjektu
 - Při automatickém vytváření žádosti o zneplatnění „starého“ cert se zaeviduje (vytvoří nový záznam) v novém formuláři u subjektu

- Upozornění interního uživatele v žádosti o nedodržování pravidla o jednom cert – 
 - V žádosti pro interního uživatele v sekci certifikátů bude zobrazena tabulka s čísly žádostí a informací o vydání či nevydání certifikátu za posledních 12 měsíců, týkajících se žádostí kdy se žádalo s nedodržením
 - Nová externí funkce, která vypíše html tabulku do žádosti
- Automatická kontrola pro zneplatnění certifikátů navíc – 
 - INTService bude kontrolovat AIS, které nemají výjimku na certifikáty a které mají více certifikátů přes limit 3 měsíce, a pokud najde takový AIS, tak to znamená nedodržení pravidla a INTService vytvoří žádost o zneplatnění nejstaršího certifikátu a zaeviduje k subjektu
 - Úprava INTService
- Testování - 
- Nasazení na test / produkci – 
- Dokumentace – 

Celkem hodin: 112h = 

Celková pracnost  = 91.000,- Kč bez DPH (110.110,- Kč s DPH)

4. Návrh harmonogramu změnového požadavku

T – den schválení požadavku / zahájení prací

- Analýza - již zpracována
- Vývoj T+ 2 týdny
- Nasazení na test a testování T+ 3 týdny
- Nasazení do produkce T+4 týdny

5. Dopady do provozu / dopady do provozní dokumentace

- Dopad na uživatele KIVS modulu – změna validace žádostí
- Aktualizace provozní dokumentace.

6. Návrh testovacího scénáře

Základní testy a kontroly:

- Vložení více žádostí o certifikát
- Testování přesahů platnosti – žádosti / certifikáty s povolenými / nepovolenými přesahy platností
- Chybné žádosti – neúplný obsah žádosti
- Správné žádosti – vše vyplněno podle nové certifikační politiky

7. Požadavky na součinnosti

SZR:

- Změna certifikační politiky, tak aby bylo možné podepsat žádosti vystavené podle nových pravidel.

8. Výstupy změnového požadavku

- Změna pravidel pro podání žádostí.
- Pravidelná denní kontrola platnosti certifikátů podle pravidel nové politiky
 - Návrhy na zneplatnění certifikátů

	Schválil (dodavatel)	Schválil (zákazník)
Jméno		
Datum		
Podpis		