SPRÁVA ZÁKLADNÍCH REGISTRŮ

POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 01-2023

Poskytovatel služby	První certifikační autorita, a. s.
Správce IS	SZR – Správa základních registrů
Objednatel	ČESKÁ REPUBLIKA - SPRÁVA ZÁKLADNÍCH REGISTRŮ
Smlouva	Dílčí Smlouva o poskytování služeb podpory provozu Národní certifikační autority č. 9 k Rámcové dohodě č. II č. SZR – 461 – 159/Ř – 2018
Číslo RFC SZR	**RFC 1204**
Název RFC SZR	**NCA - Zajištění vydávání TWINS certifikátů pro zaměstnance DIA a zahájení činností spojených s přechodem služeb NCA na SSSVD**
Kategorie RFC	**Urgent Change**
Číslo tiketu (Service Desk)	129432
Katalogový list	NCATSA03 objednávka
Typ odstávky	Bez odstávky

1. Identifikace vzniku požadavku

Zadání požadavku prostřednictvím ServiceDesk – viz. tiket č. 129432 ze dne 23.03.2023.

2. Zadání požadované změny

Realizace požadavku souvisí s transformací SZR do DIA. V důsledku této transfomace mj. dále dochází k zániku SZR jako kvalifikovaného poskytovatele služeb vytvářejícího důvěru. Budoucí výkon služeb NCA bude vykonávat nově vytvořená organizace Správa státních služeb vytvářejících důvěru („SSSVD“).

Cílem tohoto RFC je:

1. Zajištění personálních kapacit mobilních registračních autorit NCA obsluhovaných zaměstnanci I.CA pro vydávání certifikátů TWINS v rámci požadovaných dnů.
2. Dodání čipových karet Starcos 3.7 eIDAS C1 a tokenů v počtu: 150 ks čipů a 50 ks tokenů.
3. Zahájení prací souvisejících s první etapou SSSVD týkající se:
   - Aktualizace směrnice „Ukončení činnosti služeb CA, TSA NCA“ a zpracování „Plánu ukončení činnosti SZR jako kvalifikovaného poskytovatele služeb vytvářejících důvěru pro případ právního nástupnictví“, projednání a na pracovní úrovni schválení MVČR ještě před přechodem do DIA.
   - Poskytnutí spolupráce I.CA na obsahu smlouvy mezi DIA a SZR o využití veškerého HW a SW NCA pro budoucí zajištění Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru a vybudování PREPROD a PROD prostředí, především oblasti identifikace nezbytného HW a SW pro zajištění služeb provozu NCA.
   - Aktualizace veškerého SW vybavení - NCA-Core, NCARA, NewCert, SW pro online služby a SW tvořící aplikační prostředí TSA_izol (změna identifikačních prvků SZR na Správu), konfiguračních souborů, implementace případných organizačních změn, pokud budou mít dopad do vzhledu či funkčnosti apod.

3. Popis zajištění realizace změny

Předmětem je dodání personálních kapacit Mobilních registračních autorit NCA obsluhovaných zaměstnanci I.CA pro vydávání certifikátů TWINS, dodání čipových karet Starcos 3.7 eIDAS C1 a tokenů a prací souvisejících s první etapou SSSVD.

3.1 Mobilní registrační autorita

Dle požadavku SZR jsou předpokládané počty zaměstnanců DIA, kterým je nutné vydat nové prvotní certifikáty TWINS:

- Cca 40 osob přecházejících z MVČR
- Cca 70 osob přecházejících ze SZR

Pro zajištění vydávání je nutné ze strany SZR zajistit:

- Stanovit termíny a harmonogram pro vydávání a zajistit účast žadatelů o certifikát
- Operátorům Mobilní registrační autority (dále jen „MRA“) předložit seznam žadatelů, kterým bude vydán certifikát TWINS s naplněním položky O=Digitální a informační agentura podepsaný ředitelem DIA
- Zajistit místnost, ve které proběhne vydávání s přístupem k elektrické síti.

Operátor MRA je schopen vydat certifikát TWINS za cca 15 minut, tj. 4 certifikáty za hodinu.

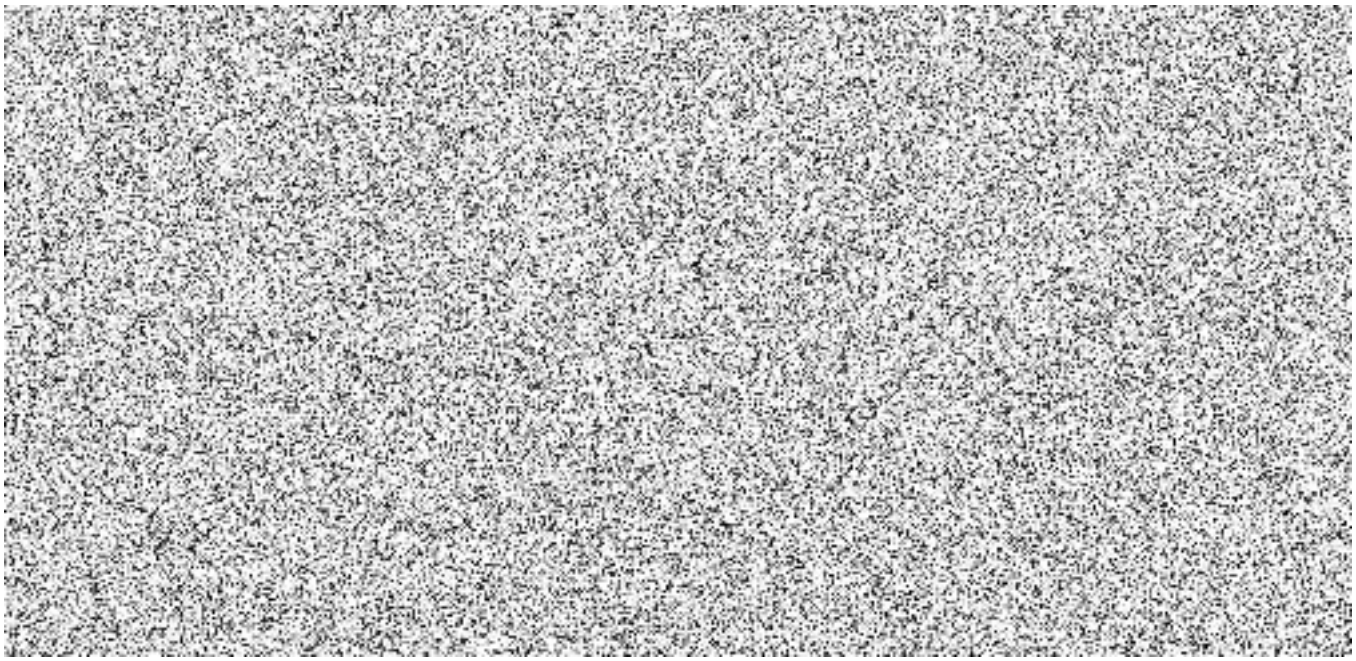
Během pracovní směny tak teoreticky 32 ks, avšak s přihlédnutím k tomu, že ne všichni žadatelé se dostaví v určený čas, a ne vždy se podaří splnit časový limit, je vhodné počítat s průměrným počtem 20 ks certifikátů/8 hodin/1 pracovní den („MD“). Předpokládáme, že vydávání zajistí I.CA dvěma pracovišti MRA, tedy 2 operátory, za den je tedy možné vydat cca 40 ks certifikátů.

Protože se termíny vydávání pro žadatele přecházející z MVČR i SZR překrývají, musí pro první tři dny pracovat druhým tým MRA.

3.2 Čipové karty a tokeny

Pro zajištění nosičů certifikátů předkládá I.CA nabídku čipových karet Starcos 3.7 eIDAS C1 a tokenů (čteček) ACR39T-A5 (USB C rozhraní).

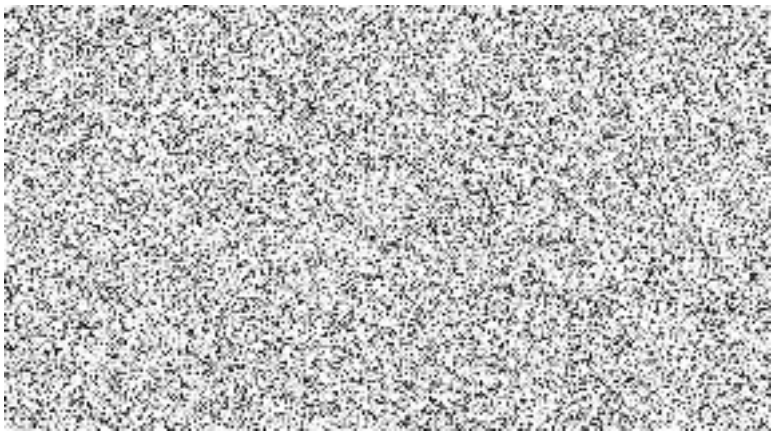
Specifikace kontaktního čipu STARCOS 3.7 eSign Profile



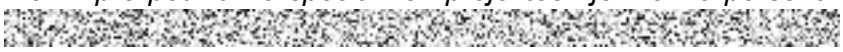
- Podporované standardy: ISO 7815-4/-8/-9, ISO 14443-1/-2/-3/-4
- Podporované protokoly: ISO 7816-3 T=0 a T=1
- Podporované rozhraní: minidriver - MS CSP (Microsoft Base Smart Card Crypto Provider), MS KSP (Microsoft Smart Card Key Storage Provider), PKCS#11
- Standard PKCS#12
- Privátní klíč se generuje přímo v kartě a nikdy neopustí kartu.

Nastavení umožňující zapamatování PINu je řešeno ve správci karty (middleware) SecureStore: uživatel si může v nastavení správce karty navolit vlastní časový úsek, po jaký chce PIN zapamatovat. Nastavení je zvlášť pro podpisové klíče v eSign a zvlášť pro ostatní (šifrovací) klíče.

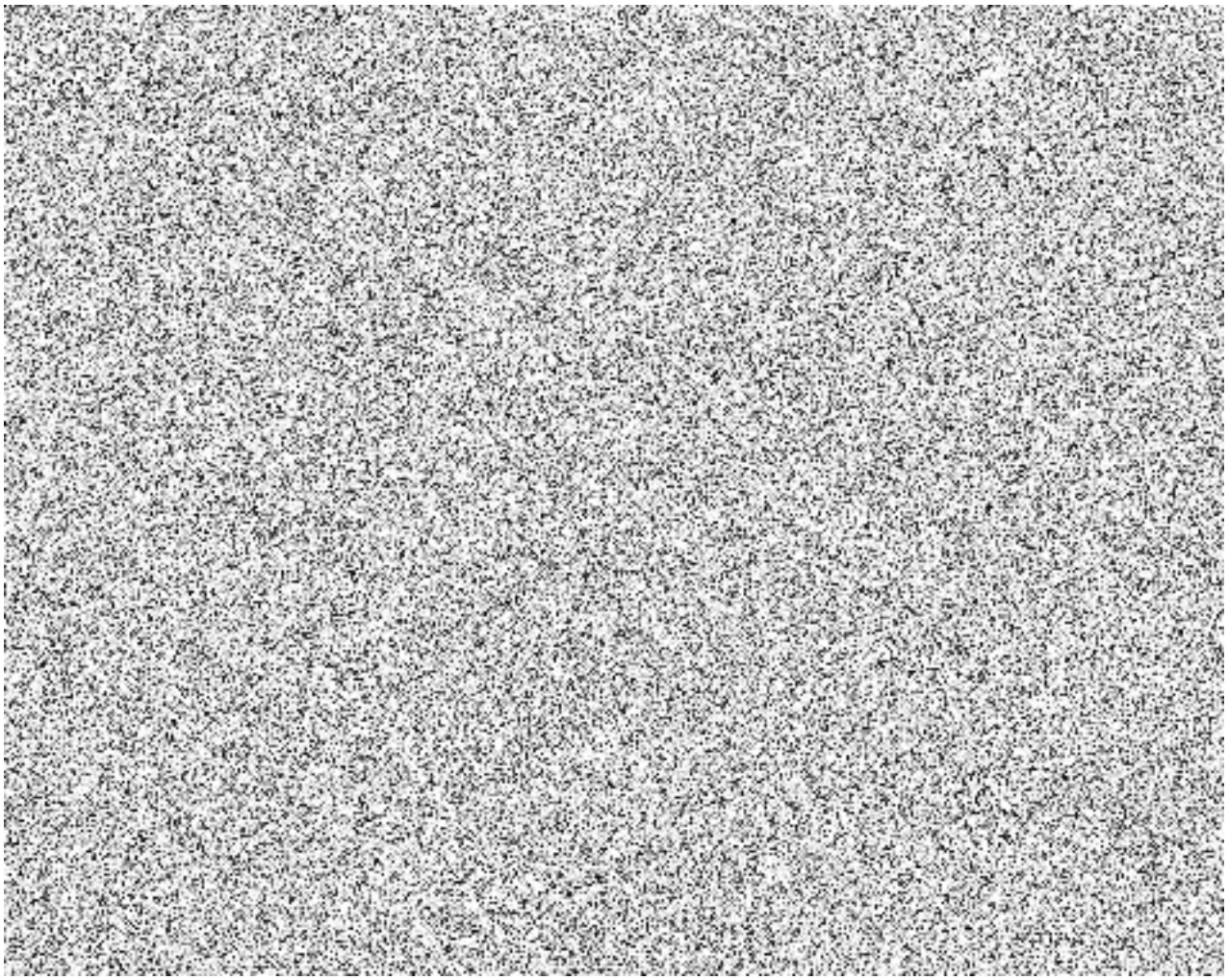
Maximální doba pro podpisové klíče v eSign je 30 minut, pro šifrovací klíče není doba shora omezena. Dále je možné aktivovat potvrzovací dialog, který se zobrazí v době, kdy je PIN zapamatován a je vytvářen podpis klíčem na kartě. V takovém případě se uživateli zobrazí hláška, zda souhlasí s použitím klíče a vytvořením podpisu.



Pozn: pro použití ve speciálních projektech je možné personalizovat čip pro delší počet míst



Použití PUKu: počet použití omezen na 10 úspěšných použití. Odblokování zablokovaného PINu pomocí PUKu u karty Starcos 3.7 neumožňuje nastavení nového PINu, dojde pouze k aktivaci nových 3 pokusů na zadání správného PINu. Funkčnost změny PIN při znalosti aktuálně nastaveného zůstává nezměněna.



3.3 Zajištění SSSVD jako kvalifikovaného poskytovatele

Pro zajištění SSSVD jako kvalifikovaného poskytovatele služeb vytvářejících důvěru byl definován níže uvedený harmonogram, zde uvedený v celém rozsahu, **nicméně předmětem této nabídky jsou činnosti a práce končící 31.5.2023**, tedy body 1 až 3.

Premisy:

- poskytování služeb NCA nesmí být přerušeno, přechod poskytovatele od SZR ke Správě státních služeb vytvářejících důvěru (dále jen „Správa“) musí být zajištěn bez výpadku
- platné certifikáty koncových uživatelů vydané SZR nesmí být zneplatněny a musí být platné do doby jejich expirace (stejně tak certifikáty časových autorit)
- zahájení poskytování služeb vytvářejících důvěru Správou musí nastat nejpozději k 1.1.2024 (čl. XVIII Přechodná ustanovení, odst. 3 zákona č. 471/2022 Sb.), avšak s dostatečnou časovou rezervou, tedy nejpozději od 1. 12. 2023
- rozhodnutí SZR o realizaci musí být učiněno nejpozději do 31.3.2023
- smlouva o realizaci mezi SZR, resp. DIA a I.CA musí být uzavřena do 30.4.2023 s tím, že zahájení prací započne 1.5.2023.

Časový a věcný harmonogram:

1. Aktualizace směrnice „Ukončení činnosti služeb CA, TSA NCA“ a zpracování „Plánu ukončení činnosti SZR jako kvalifikovaného poskytovatele služeb vytvářejících důvěru pro případ právního nástupnictví“, projednání a na pracovní úrovni schválení MVČR ještě před přechodem do DIA

T: 31.3.2023 (schválení premisy nezneplatňování certifikátů je kruciální záležitostí, v opačném případě by byl celý postup i harmonogram zcela jiný)

2. Uzavření smlouvy mezi DIA a SZR o využití veškerého HW a SW NCA pro budoucí zajištění Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru a vybudování PREPROD a PROD prostředí

   T: 30.4.2023

3. Aktualizace veškerého SW vybavení - NCA-Core, NCARA, NewCert, SW pro online služby a SW tvořící aplikační prostředí TSA_izol (změna identifikačních prvků SZR na Správu), konfiguračních souborů, implementace případných organizačních změn, pokud budou mít dopad do vzhledu či funkčnosti apod.

   T: 31.5.2023

4. Vygenerování párových dat, vydání certifikátů veřejných klíčů kořenových a mezilehlých certifikačních autorit (kryptografie RSA i ECC) v PREPROD prostředí

   T: 15.6.2023

5. Vygenerování párových dat, vydání certifikátů veřejných klíčů časových autorit TSU

   T: 15.6.2023 v PREPROD prostředí

6. Vygenerování párových dat, vydání certifikátu pro službu ověřování podpisu v PREPROD prostředí

   T: 15.6.2023

7. Distribuce nových certifikátů na vybranou lokalitu BS a do centra NCA, jejich instalace do PREPROD prostředí

   T: 15.6.2023

8. Aktualizace všech dokumentů pro audit subjektem posouzení shody v PREPROD prostředí

   T: 30.6.2023

9. Zajištění auditu subjektem posouzení shody, spolupráce na auditu centra NCA a vybrané BS

   T: 31.7.2023

10. Zpracování Analýzy rizik NCA, protože NCA je VIS dle ZoKB.

    T: 31.8.2023

11. Vygenerování párových dat, vydání certifikátů veřejných klíčů kořenových a mezilehlých certifikačních autorit (kryptografie RSA i ECC) v PROD prostředí

    T: 31.8.2023

12. Vygenerování párových dat, vydání certifikátu pro službu ověřování podpisu v PROD prostředí

    T: 31.8.2023

13. Oznámení změny v poskytování kvalifikovaných služeb DIA, audit DIA, správní rozhodnutí a zápis certifikátů a poskytovatele do TL

    T: 30.9.2023

14. Vygenerování párových dat, vydání certifikátů veřejných klíčů časových autorit TSU v PROD prostředí

    T: 10.10.2023

15. Zajištění přístupů do chráněných zón BS, instalace root a mezilehlých certifikátů včetně TSU a služby ověřování podpisu na BS a v centru NCA do PROD prostředí

    T: 15.11.2023

16. Zahájení poskytování služeb NCA pod Správou jako kvalifikovaným poskytovatelem služeb vytvářejících důvěru

    T: 30.11.2023

17. Provoz služby o stavech certifikátů vydaných SZR (CRL a OCSP) pro certifikáty koncových uživatelů 3 roky a pro TSU certifikáty 6 let, opatřené původní zaručenou elektronickou pečetí SZR

    T: od 30.11.2023

3.4 Konkrétní činnosti poskytnuté v rámci tohoto RFC

1. Aktualizace směrnice „Ukončení činnosti služeb CA, TSA NCA“ a zpracování „Plánu ukončení činnosti SZR jako kvalifikovaného poskytovatele služeb vytvářejících důvěru pro případ právního nástupnictví“, projednání a na pracovní úrovni schválení MVČR ještě před přechodem do DIA

   T: 31.3.2023

   Poznámka k obsahu: Dokument musí postihnout danou situaci a nastavit postup tak, aby nemuselo dojít k nechtěným krokům, jako je např. zneplatnění většího množství uživatelských certifikátů, certifikátů pro ověřování kvalifikovaných pečetí (za následek by mělo výpadky spisových služeb na úrovni hodin až jednotek dnů), a hlavně certifikátů časových autorit, kde by mohla nastat velmi nepříjemná situace spojená s násilným ukončením platnosti časového razítka bez jeho přerazítkování jiným, platným.

2. Uzavření smlouvy mezi DIA a SZR o využití veškerého HW a SW NCA pro budoucí zajištění Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru a vybudování PREPROD a PROD prostředí

   T: 30.4.2023

   Poznámka k obsahu: Předmětem je poskytnutí spolupráce I.CA na obsahu smluvního dokumentu, především oblasti identifikace nezbytného HW a SW pro zajištění služeb provozu NCA.

3. Aktualizace veškerého SW vybavení - NCA-Core, NCARA, NewCert, SW pro online služby a SW tvořící aplikační prostředí TSA_izol (změna identifikačních prvků SZR na Správu), konfiguračních souborů, implementace případných organizačních změn, pokud budou mít dopad do vzhledu či funkčnosti apod.

   T: 31.5.2023

   Poznámka k obsahu: Vzhledem ke skutečnosti, že z důvodů zajištění nejvyšší míry bezpečnosti aplikací jsou mnohé parametry součástí zdrojových kódů aplikací, a to jak aplikací CA CORE, tak i podpůrných aplikací (NCARA, NewCert, TSA_izol apod.), nelze v žádném případě ztotožňovat výše uvedené a další úpravy parametrů s pouhou změnou konfiguračních souborů. Ve skutečnosti se jedná o úpravy významné části zdrojových textů, včetně úprav souvisejících parametrů v konfiguračních souborech.

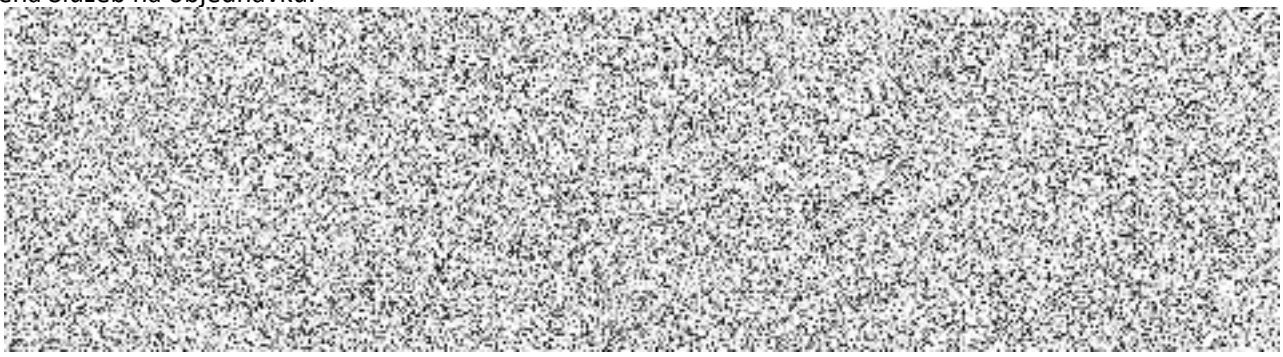
   V daném případě to představuje úpravu vyšších desítek modulů zdrojových kódů, následné otestování, odstranění případných chyb, a nakonec vydání release. K tomu je nutné připočítat ještě testování v PREPROD prostředí.

4. Odhad pracnosti

Níže jsou uvedeny ceny za jednotlivé části. Detailní cenová nabídka je uvedena v přiloženém xlsx souboru.

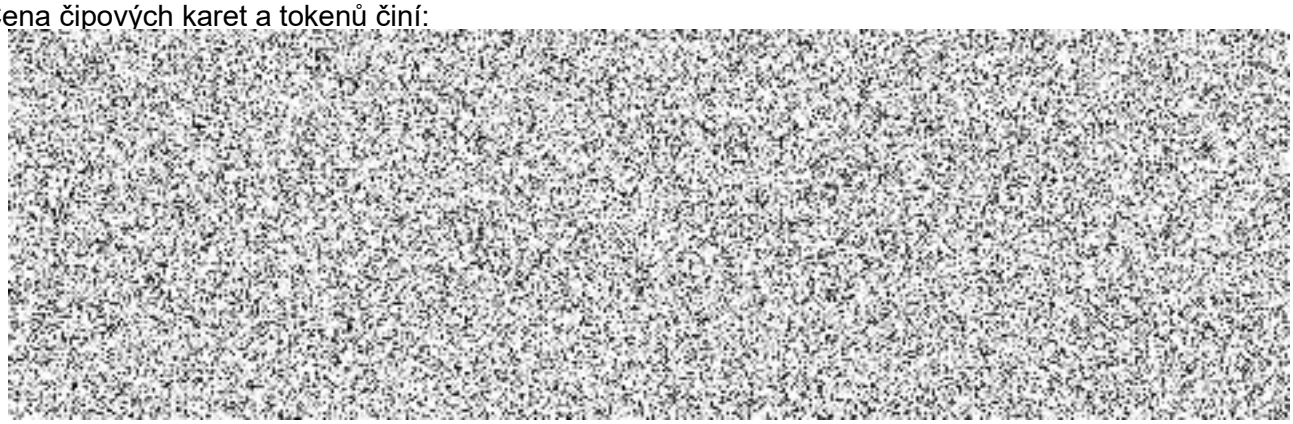
Zajištění vydávání certifikátů bude realizováno podle Katalogových listů bodu NCATSA03-02 Další služby. Cena je stanovena dle bodu 6.1.2 aktuálně platné Dílčí Smlouvy o poskytování služeb podpory provozu Národní certifikační autority č. 9 ze dne 16.12.2022.

Cena Služeb na objednávku:



- Cena vydávání certifikátů činí 154.000,- Kč bez DPH, tj. 186.340,- Kč s DPH.

Cena čipových karet a tokenů činí:



Celková cena činí 991.000,- Kč bez DPH, tj. 1.199.110,- Kč s DPH.

Podrobný rozpad ceny je uveden v přiloženém xlsx souboru.

TWINS certifikáty a čipy a tokeny a 1. etap

5. Návrh harmonogramu změnového požadavku

1. Pro vydávání žadatelům přecházejících z MVČR stanovila SZR termíny:
   - Pondělí 3. dubna
   - Úterý 4. dubna
   - Středa 5. dubna, a to v rozmezí 8:00 – 16:00.

   Lokalitou vydávání bude pravděpodobně budova Centrotex či Nagano III.

2. Pro vydávání žadatelům přecházejících ze SZR stanovila SZR termíny:
   - Pondělí 3. dubna
   - Úterý 4. dubna
   - Středa 5. dubna
   - Čtvrtek 6. dubna, a to v rozmezí 8:00 – 16:00.

   Lokalitou vydávání bude Vápenka.

3. Aktualizace směrnice „Ukončení činnosti služeb CA, TSA NCA“ a zpracování „Plánu ukončení činnosti SZR jako kvalifikovaného poskytovatele služeb vytvářejících důvěru pro případ právního nástupnictví“, projednání a na pracovní úrovni schválení MVČR ještě před přechodem do DIA

   T: 31.3.2023

4. Uzavření smlouvy mezi DIA a SZR o využití veškerého HW a SW NCA pro budoucí zajištění Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru a vybudování PREPROD a PROD prostředí

   T: 30.4.2023

5. Aktualizace veškerého SW vybavení - NCA-Core, NCARA, NewCert, SW pro online služby a SW tvořící aplikační prostředí TSA_izol (změna identifikačních prvků SZR na Správu), konfiguračních souborů, implementace případných organizačních změn, pokud budou mít dopad do vzhledu či funkčnosti apod.

   T: 31.5.2023

   Fakturační milník: 30.6.2023

6. Návrh testovacího scénáře

Není relevantní.

7. Výstupy změnového požadavku

1. Zajištění personálních kapacit mobilních registračních autorit NCA obsluhovaných zaměstnanci I.CA pro vydávání certifikátů TWINS v rámci požadovaných dnů.
2. Dodání čipových karet Starcos 3.7 eIDAS C1 a tokenů v počtu: 150 ks čipů a 50 ks tokenů.
3. Zahájení prací souvisejících s první etapou SSSVD týkající se:
   - Aktualizace směrnice „Ukončení činnosti služeb CA, TSA NCA“ a zpracování „Plánu ukončení činnosti SZR jako kvalifikovaného poskytovatele služeb vytvářejících důvěru pro případ právního nástupnictví“, projednání a na pracovní úrovni schválení MVČR ještě před přechodem do DIA.
   - Poskytnutí spolupráce I.CA na obsahu smlouvy mezi DIA a SZR o využití veškerého HW a SW NCA pro budoucí zajištění Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru a vybudování PREPROD a PROD prostředí, především oblasti identifikace nezbytného HW a SW pro zajištění služeb provozu NCA.
   - Aktualizace veškerého SW vybavení - NCA-Core, NCARA, NewCert, SW pro online služby a SW tvořící aplikační prostředí TSA_izol (změna identifikačních prvků SZR na Správu), konfiguračních souborů, implementace případných organizačních změn, pokud budou mít dopad do vzhledu či funkčnosti apod.

8. Akceptační kritéria, způsob ověření na produkci

8.1 Akceptační kritéria

Číslo milníku	Nejzazší termín pro předání	Název milníku	Výše platby	Akceptační kritéria
1	30.4.2023	Zajištění vydávání TWINS certifikátů. Dodávka čipů a tokenů.	Splnění tohoto milníku zakládá právo dodavatele na fakturaci dle dílčí ceny bodu 5, tj. 210 000 Kč bez DPH, tj. 254 100 Kč s DPH.	1. Operátoři MRA jsou přítomni na určeném místě vydávání certifikátů. 2. V určeném čase vydávají certifikáty na dodaný HW. 3. Po vydání všech certifikátů předložení seznamu držitelů certifikátů.
2	31.5.2023	Vypracování plánu ukončení činnosti, aktualizace směrnice, úpravy SW.	Splnění tohoto milníku zakládá právo dodavatele na fakturaci dle dílčí ceny bodu 5, tj. 781 000 Kč bez DPH, tj. 945 010 Kč s DPH	1. Směrnice a Plán ukončení činnosti jsou schváleny DIA. 2. Je uzavřena smlouva mezi DIA a SZR o využití veškerého HW a SW NCA. 3. Veškeré SW vybavení je aktualizováno.

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

- Upravená Směrnice a Plán ukončení činnosti.
- Veškeré SW vybavení NCA je aktualizováno.

9.1 Náklady na podporu provozu IS

Bez dopadu.

10. Dopady na bezpečnost IS / dopady do bezpečnostní dokumentace

Bez dopadu.