Detailní specifikace Služeb Certifikační autority a podmínek jejich poskytování

Typ certifikační autority

Požadovány jsou služby certifikační autority (dále jen Služby CA), která bude vydávat nekvalifikované podpisové certifikáty pro vzájemnou komunikaci technických zařízení - nejde tedy o kvalifikované certifikáty ve smyslu Zákona o Elektronickém podpisu č. 227/2000 Sb., ve znění pozdějších předpisů (dále jen ZoEP).

Vzhledem k tomu, že Služby CA budou využívány v informačních systémech, které jsou součástí kritické informační infrastruktury resortu ministerstva financí, je požadována vysoká úroveň zabezpečení a bezpečného provozu Služeb CA.

Proces vydávání certifikátů bude implementován prostřednictvím integrace webových stránek Daňového portálu Zadavatele (dále jen DPR) a webových stránek Poskytovatele Služeb CA. DPR zajistí ověření identity žadatele o certifikát, webové stránky Poskytovatele zajistí rozhraní pro generování a příjem žádostí, vydání certifikátů, správu databáze certifikátů, zneplatnění certifikátů.

Funkční specifikace

Požadavky na certifikáty

Certifikáty pro poplatníky

V rámci Služeb CA budou vydávány X.509 certifikáty pro daňové poplatníky (dále „poplatníky“) s přiděleným daňovým identifikačním číslem (DIČ). Poplatník může být fyzická i právnická osoba. DIČ je jediným povinným identifikátorem vlastníka certifikátu, pro každé DIČ je možno vydat libovolný počet certifikátů. Certifikáty jednoho poplatníka se odlišují zejména svým sériovým číslem.

- V certifikátu musí být uvedeno číslo **DIČ** poplatníka jako jedna z položek *distinguishedName* vlastníka certifikátu (Subject DN). DIČ bude jediným obsahem položky DN *commonName* (OID 2.5.4.3).
- DIČ má následující formát jako (regulární výraz nezohledňující logiku kontrolních číslic): ^CZ[0-9]{8,10}$
- Ke každému vydanému certifikátu bude možno v databázi vydaných certifikátů certifikátů (udržována na CA) zadat poznámku, která nebude součástí samotného certifikátu, pro snadnější informaci poplatníka. Poznámka bude u certifikátu poplatníka zobrazena jako dodatečná informace.
- Certifikáty z testovacích prostředí musí být jasně označeny identifikátorem testovacího prostředí v položce Certificate Policies (extension dle RFC3647)

Detailní specifikace náplně položek certifikátů musí být upřesněna Poskytovatelem v detailním návrhu a schválena Zadavatelem.

Certifikáty CA a centrálního systému

Pro potřeby centrálního systému Zadavatele, zejména pro podepisování odpovědí na zprávy poplatníků, je požadován relativně malý počet (desítky) certifikátů.

Registrační proces bude upřesněn v Detailním návrhu, ale předběžně předpokládáme obdobný proces jako u kvalifikovaných nebo komerčních systémových certifikátů. Vydávání těchto certifikátů předpokládáme formou osobní návštěvy registrační autority v pracovních hodinách po předchozí dohodě.

Konkrétní náplň položek vlastních certifikátů CA (kořenová autorita) a certifikátů vydávaných pro potřebu centrálních systémů Zadavatele musí být upřesněna Poskytovatelem v detailním návrhu a schválena Zadavatelem.

Kryptografické parametry a platnost certifikátů

Typ certifikátu	Parametr	Hodnota
Všechny typy	Algoritmus podpisu	RSA2048
Všechny typy	Algoritmus otisku	SHA-256
Certifikát CA	Maximální doba platnosti	6 let
Certifikát CA	Aktivní období certifikátu	3 roky
Certifikát poplatníka	Maximální doba platnosti	3 roky
Certifikát centrálního systému	Maximální doba platnosti	2 roky

Doba uložení neplatných certifikátů v databázi CA po ukončení aktivní platnosti certifikátu je 10 let.

CRL

Součástí Služeb CA musí být vysoce dostupné veřejné rozhraní pro stahování CRL.

Frekvence vydávání CRL musí být určena Poskytovatelem v detailním návrhu a schválena Zadavatelem, maximální možné požadavky jsou:

- pravidelný interval vydávání CRL 15 minut (nextUpdate parametr CRL může být delší)
- vydání nového CRL do 1 minuty od zneplatnění certifikátu

Požadavky na prostředí

Zadavatel bude využívat Služby CA v několika prostředích. V rámci Služeb CA musí Poskytovatel provozovat tři prostředí a integrovat je s prostředími Zadavatele:

- produkční prostředí, ve kterém budou vydávány certifikáty pro skutečné poplatníky v objemech uvedených dále
- testovací prostředí pro testování interními uživateli, ve kterém budou vydávány certifikáty pro relativně malý počet testovacích uživatelů v roli testovacích poplatníků
- testovací prostředí pro testování externími uživateli a vývojáři klientských nástrojů, ve kterém budou vydávány certifikáty pro řádově vyšší stovky až nižší jednotky tisíc testovacích uživatelů v roli testovacích poplatníků

Integrační mechanismus na DPR popsaný dále umožňuje předání identifikace prostředí Zadavatele a integraci jednoho prostředí CA na více prostředí DPR.

Jednotlivá prostředí CA musí být možné odlišit následujícími způsoby

- certifikáty z testovacích prostředí musí být jasně označeny identifikátorem testovacího prostředí Zadavatele v položce Certificate Policies (extension dle RFC3647)
- odlišné certifikáty kořenové CA
- oddělené databáze certifikátů a web rozhraní

Požadavky na Web aplikaci CA

Poskytovatel zajistí web rozhraní pro poplatníky, kterým umožní přístup ke Službám CA (dále jen Web aplikace CA). S Web aplikací CA bude vždy pracovat autentizovaný poplatník, anonymní použití nebude možné. Ověření identity poplatníka (resp. uživatele DPR, který má oprávnění spravovat certifikáty daného poplatníka) zajistí DPR a předá Web aplikaci CA prostřednictvím integračního rozhraní popsaného níže. Web aplikace CA bude přístupná přes HTTPS protokol s použitím SSL certifikátů certifikační autority, jejíž root certifikáty jsou standardně předkonfigurovány ve všech požadovaných podporovaných prohlížečích a operačních systémech.

HTML rozhraní Web aplikace CA musí být buď dostatečně jednoduché nebo responsivní, aby jej bylo možné používat na široké škále zařízení od osobních počítačů po tablety. Web aplikace CA musí podporovat následující klientské platformy ve verzích podporovaných jejich výrobci v k 1.1.2016 a novějších:

- web prohlížeče Chrome, Firefox, Internet Explorer, Safari
- operační systémy a odpovídající standardní web prohlížeče mobilních zařízení: iOS, Android, Windows Phone a Windows 10

Služby Web aplikace CA

Web aplikace CA musí podporovat následující funkce pro poplatníky uživatelsky přívětivou formou (detailní návrh funkcionality musí být rozpracován Poskytovatelem v detailním návrhu a schválen Zadavatelem):

- Ověření předpokladů a potřebné konfigurace prohlížeče a klientských nástrojů – funkce obdobná stránce Kontrola nastavení počítače Daňového portálu (https://adisepo.mfcr.cz/adistc/adis/idpr_pub/dpr/nastaveni_kontrola.faces)
- Podpora generování klíčů na straně poplatníka, vytvoření žádosti o certifikát (CSR - Certificate Signing Request) a instalaci certifikátu *). Web aplikace CA zpřístupní poplatníkovi potřebné klientské nástroje a návody.
- Příjem CSR
- Stažení vydaného certifikátu
- Přehled přijatých CSR, vydaných, zneplatněných a exspirovaných certifikátů poplatníka - podpora stránkování, třídění a vyhledávání
- Možnost uložení nepovinných poznámek k jednotlivým certifikátům a jejich zobrazení v rámci přehledu certifikátů
- Zobrazení údajů o časové platnosti vydaných certifikátů a o blížící se exspiraci
- Zobrazení informace o blížící se exspiraci certifikátu a e-mailová notifikace (pokud žadatel poskytne e-mail adresu jako nepovinný údaj)
- Zneplatnění certifikátu

*) Podpora generování klíčů, vytvoření žádosti a instalace certifikátu je požadována pro všechny uvedené platformy. Podpora může mít formu klientského kódu, který je součástí Web aplikace CA (např. javascript), samostatné klientské aplikace nebo návodu k manuálnímu postupu uživatele, resp.

může jít o kombinaci těchto forem. Nesmí přitom vyžadovat další licence, resp. poplatky nad rámec ceny Služeb CA, od Zadavatele, ani od uživatelů Web aplikace CA. Hlavním cílem je maximalizace uživatelského komfortu uživatele a minimalizace požadavků na technickou podporu (která je rovněž v odpovědnosti Poskytovatele).

Web aplikace CA dále musí podporovat následující hromadné operace:

- Dávkový příjem více CSR jednoho poplatníka (zpracování CSR a vydávání certifikátů bude v případě hromadných operací prováděno vždy asynchronně).
- Stažení všech certifikátů poplatníka (kompletně nebo vydaných v určitém období)
- Stažení seznamů přijatých CSR, vydaných, zneplatněných a exspirovaných certifikátů poplatníka včetně vybraných položek certifikátu (serialNumber, datum vydání, nepovinná pole naplněná poplatníkem) a poznámek ve strojově čitelném formátu (např. CSV)

Součástí Web aplikace CA dále musí být:

- Nápověda a návod k použití Web aplikace CA (dostupné přímo v rámci této aplikace)
- Nápověda a návod Web aplikace CA musí být v českém jazyce

Synchronní a asynchronní mód vydávání certifikátů

Web aplikace CA musí podporovat synchronní i asynchronní mód vydání certifikátu, přičemž

- Formát CSR musí vycházet z široce rozšířeného standardu, aby umožnil snadnou implementaci v software pokladních zařízení nebo administračních nástrojů poplatníků.
- Pokud je možné vydat certifikát do požadovaného času vydání (5 sec), odpověď (certifikát) na CSR musí být uživateli vrácena synchronně v rámci jednoho HTTPS dotazu.
- Pokud to není možné, přejde Web aplikace CA do asynchronního módu – uživatel dostane jako odpověď potvrzení o přijetí žádosti a orientační informaci o času vydání certifikátu. Při další návštěvě Web aplikace CA mu musí být nabídnut seznam nových asynchronně vydaných certifikátů.

Řízení tempa vydávání certifikátů jednoho poplatníka

Web aplikace CA musí podporovat konfigurovatelný mechanismus řízení tempa vydávání certifikátů jednoho poplatníka. Mechanismus řízení tempa vydávání certifikátů bude vycházet z parametru maximálního očekávaného počtu certifikátů poplatníka, kalkulovaného na základě počtu provozoven (který obdrží přes integrační rozhraní od DPR) a konfigurovatelných globálních parametrů. Parametr maximálního očekávaného počtu certifikátů poplatníka musí být možné pro jednotlivé poplatníky manuálně změnit prostřednictvím požadavku na technickou podporu poplatníků. Mechanismus je aktivován při zpracování CSR poplatníka, který má více platných certifikátů vydaných v průběhu jednoho roku zpětně než tento parametr - Web aplikace CA přejde do asynchronního módu a bude zpracovávat CSR tohoto poplatníka a vydávat certifikáty zpomaleným tempem (např. 1 certifikát denně - konfigurovatelný parametr).

API pro vydání dalších certifikátů

Poskytovatel poskytne API pro automatizované vydání certifikátu v odpovědi na CSR podepsanou již vydaným platným certifikátem poplatníka (i certifikátem předchozího poskytovatele). Na rozdíl od standardního způsobu použití Web aplikace CA s předáním identity od DPR v tomto případě poplatník kontaktuje CA přímo a jeho identitu odvodí Poskytovatel z certifikátu, kterým je podepsáno CSR. Před

vydáním certifikátu Poskytovatel zavolá WebService DPR pro ověření platnosti DIČ a získání informace o počtu provozoven poplatníka.

Grafický návrh Web aplikace CA

Grafický návrh Web aplikace CA musí být připraven dle specifikace Zadavatele, vycházející z grafického návrhu DPR.

Integrace DPR a Web aplikace CA

Autentizační služba DPR pro Služby CA

Předání řízení z DPR na CA bude probíhat následujícím algoritmem:

1. Následující akce na DPR může provést pouze uživatel, který se úspěšně přihlásil a má právo spravovat certifikáty poplatníka s určitým DIČ.
2. Pokud uživatel zvolí akci „Správa certifikátů“, provede aplikace DPR následující kroky:
    a. Vytvoří náhodný unikátní identifikátor daného požadavku – dále jen *authToken*
    b. Poznamená si čas vytvoření tohoto požadavku – dále jen *authTime*
    c. Uloží si do interní evidence *authToken*, *authTime*, a DIČ poplatníka, se kterým uživatel pracoval
    d. Pomocí HTTP kódu 302 provede DPR předání řízení na dohodnutou URL adresu Web aplikace CA, kde jako HTTP GET parametr předá *authToken*
3. Web aplikace CA převezme řízení.
4. Web aplikace CA vyvolá WebService službu poskytovanou DPR, a v dohodnuté XML struktuře předá *authToken*.
5. DPR odpoví na požadavek Web aplikace CA dle následujícího algoritmu:
    a. Pokud *authToken* není aplikaci DPR znám, vrátí chybovou zprávu,
    b. Pokud *authToken* je znám, ale od času *authTime* uplynula delší než nastavená doba životnosti *authToken*, nebo byl *authToken* zneplatněn, vrátí chybovou zprávu.
    c. Pokud *authToken* je znám a platný, tak je nejprve pro další operace zneplatněn. Následně DPR vrátí v XML datech následující informace:
        i. authTime
        ii. authToken
        iii. authValidity (časová platnost autentizační informace)
        iv. aktuální čas vyřízení požadavku
        v. DIČ poplatníka
        vi. počet provozoven poplatníka
        vii. Informace o platnosti DIČ[1]
        viii. Identifikaci uživatele, který se přihlásil k DPR
        ix. Volitelně: kontaktní údaje uživatele (mobilní číslo, email)
6. Pokud Web aplikace CA obdržela v kroku 5 chybnou odpověď, musí o tom stručně informovat uživatele a musí mu nabídnout možnost předání řízení na DPR (pomocí dohodnuté URL adresy).
7. Pokud Web aplikace CA obdržela v kroku 5 pozitivní odpověď obsahující DIČ, může v rámci této web session poskytnout Služby CA pro dané DIČ.

[1] Uvažuje se o situaci, kdy poplatník přestal být registrován, tedy by mu neměly být vydávány nové certifikáty – nicméně může mít stále přístup do DPR i Web aplikace CA, např. kvůli zneplatnění certifikátů.

8. Poskytovatel Služeb CA je odpovědný za bezpečné zacházení s výsledkem autentizační služby, zejména za časové omezení platnosti takto autorizované web session, vyloučení možnosti záměn web session při opakovaném použití tohoto integračního mechanismu apod.
9. Web aplikace CA umožní uživateli předat řízení na DPR, pomocí dohodnuté URL.

authToken bude obsahovat následující informace:

- identifikátor prostředí, kde byl token vytvořen (použito k odvození adresy WebService na ověření authToken a URL adresy pro zpětné předání řízení na DPR)
- číslo unikátně identifikující token (při generování na straně DPR bude zahrnuta i náhodná složka, aby nebylo možné odhadovat následující tokeny)
- další případnou identifikaci zařízení, které *authToken* vytvořilo, kvůli určení logu při řešení chybových stavů

Veškerá komunikace mezi DPR, uživatelem a Web aplikací CA musí probíhat zabezpečeným protokolem HTTPS. Pro zabezpečení vzájemné komunikace formou WebService musí obě strany používat komerční serverové certifikáty vydané akreditovaným poskytovatelem certifikačních služeb a kontrolu IP adres.

Podpora migrace na jiné řešení Služeb CA

Poskytovatel musí podporovat převzetí služeb od jiného předchozího poskytovatele a předání služeb jinému následnému poskytovateli.

Převzetí služeb od jiného předchozího poskytovatele

Poskytovatel musí podporovat import databáze certifikátů předchozího poskytovatele a jejich zobrazování uživatelům ve Web aplikaci CA spolu s nově vydanými certifikáty. Web aplikace CA musí podporovat požadavky na zneplatnění certifikátů předchozího poskytovatele formou volání WebService předchozího poskytovatele. Pro zabezpečení vzájemné komunikace formou WebService musí obě strany používat HTTS protokol, komerční serverové certifikáty vydané akreditovaným poskytovatelem certifikačních služeb a kontrolu IP adres. Stav importovaných certifikátů musí být pravidelně aktualizován na základě CRL předchozího poskytovatele.

Předání služeb jinému následnému poskytovateli

Poskytovatel musí podporovat export databáze certifikátů.

Poskytovatel musí poskytovat web rozhraní pro zneplatňování platných certifikátů a publikovat CRL po celou dobu platnosti posledního certifikátu. Poskytovatel musí dále v tomto období poskytovat samostatnou WebService pro následného poskytovatele pro zneplatnění jednoho certifikátu. Pro zabezpečení vzájemné komunikace formou WebService musí obě strany používat HTTS protokol, komerční serverové certifikáty vydané akreditovaným poskytovatelem certifikačních služeb a kontrolu IP adresu.

Požadavky na služby CA poskytované pracovníkům Zadavatele

Součástí Služeb CA jsou následující služby poskytované pracovníkům Zadavatele:

- WebService pro stažení seznamu všech vydaných certifikátů jednoho nebo všech poplatníků dle zadaných parametrů (minimálně: DIČ a/nebo uzavřený či otevřený časový interval vydání certifikátu) včetně vybraných položek certifikátu (serialNumber, datum vydání, nepovinná pole naplněná poplatníkem) a poznámek

- WebService pro stažení všech vydaných certifikátů jednoho poplatníka dle zadaných parametrů (minimálně: DIČ a/nebo uzavřený či otevřený časový interval vydání certifikátu).
- Kompletní export databáze certifikátů na vyžádání
- Pravidelný export databáze zpracovaných dotazů a odpovědí technické podpory

Služby typu WebService budou využívány formou B2B kanálu používajícího HTTPS protokol, komerční serverové certifikáty vydané akreditovaným poskytovatelem certifikačních služeb a kontrolu IP adres.

Ostatní služby budou využívány zabezpečenými kanály definovanou skupinou administrátorů Zadavatele, s použitím certifikátů vydaných akreditovaným poskytovatelem certifikačních služeb.

Požadavky na technickou podporu poplatníků

Součástí Služeb CA je technická podpora pro poplatníky ve věcech týkajících se použití Web aplikace CA, generování klíčů a CSR - formou písemných dotazů, předávaných Poskytovateli prostřednictvím pracovníků uživatelské podpory Zadavatele.

Dále je v pracovní době (po-pá 9:00-17:00) požadována telefonická podpora pro vybrané pracovníky uživatelské podpory Zadavatele.

Dotazy poplatníků a odpovědi musí být zaznamenávány a kontinuálně zapracovávány do nápovědy a návodu Web aplikace CA.

Veškerá komunikace s poplatníky a pracovníky Zadavatele musí být v českém jazyce.

Bezpečnostní požadavky

Bezpečnostní a provozní standardy Služeb CA

Služby CA budou využívány v informačních systémech, které jsou součástí kritické informační infrastruktury resortu ministerstva financí, a to jak formou využití vydaných certifikátů pro zajištění autentizace, integrity a nepopiratelnosti dat na aplikační úrovni těchto informačních systémů, tak formou spolupráce a předávání řízení uživatelského sezení mezi web portály těchto IS a CA. Bezpečnost těchto informačních systémů nebo integrita jejich dat bude záviset na bezpečnosti a důvěryhodnosti Služeb CA. Kompromitace certifikátů nebo dokonce kompromitace celé CA může způsobit vážné ohrožení integrity dat informačních systémů resortu ministerstva financí, které jsou prvky kritické informační infrastruktury státu, a ohrožení výkonu zákonných povinností Finanční správy České republiky. Z těchto důvodů je požadována vysoká úroveň zabezpečení a bezpečného provozu Služeb CA.

Služby CA musí být provozovány na technické provozní platformě, která svým technickým řešením a režimem provozu odpovídá normám a standardům uvedeným v následujícím seznamu (s vyloučením požadavků, které jsou v rozporu se specifickým zadáním Služeb CA v této příloze, např. požadavky na ověření identity osob pro vydávání osobních certifikátů). Odkazy na normy a standardy znamenají vždy buď aktuálně platnou verzi uvedené normy, nebo normu/standard, které je aktuálně nahrazují.

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411 (Part 1, Part 2) - Electronic Signatures and Infrastructures (ESI); Policy and security Requirements for Trust Service Providers issuing certificates
- ETSI EN 319 412 (Part 1-5) Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI TS 102 042 - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
- CEN TS 419 261 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures) nebo profil ochrany definovaný dle ISO/IEC 15408 (Common Criteria)
- privátní klíče CA musí být generovány a uloženy v HSM splňujícím požadavky na důvěryhodný systém s úrovní minimálně EAL 4 dle standardu ISO/IEC 15408, nebo uvedené ve standardech ISO/IEC 19790, nebo FIPS PUB 140-2 level 3

Poskytovatel dále musí alespoň jednou ročně umožnit Zadavateli provést bezpečnostní audit služeb CA a jejich provozní platformy, jehož cílem je ověření výše uvedených požadavků. Audit Zadavatele může být částečně nahrazen předložením auditní zprávy externí auditní organizace schválené Zadavatelem.

Certifikační politika

Certifikační politika musí vycházet z požadavků Zadavatele. V oblasti bezpečnostních a provozních procesů na straně Poskytovatele Služeb CA musí vyhovovat uvedeným bezpečnostním a provozním standardům. Identifikace poplatníků je zprostředkována DPR výše popsaným způsobem. Privátní klíče musí být generovány na straně poplatníka. Certifikační politika nebude předepisovat žádná povinná konkrétní pravidla pro zacházení s privátními klíči a certifikáty na straně poplatníků, pouze obecné ustanovení odpovědnosti za bezpečnost privátních klíčů a akce/operace jimi podepsané.

Certifikační politika pro neprodukční prostředí může být podle požadavků Zadavatele dále uvolněna, např. v oblasti identifikace poplatníka.

Změna root certifikátů

Poskytovatel v dokumentaci zpracuje a odsouhlasí s Poskytovatelem pravidla změny root certifikátů CA a postupy při takové změně.

Bezpečnostní testy

Součástí akceptace přípravy Služeb CA bude penetrační bezpečnostní test, provedený organizací pověřenou Zadavatelem. Penetrační test bude proveden minimálně v rozsahu dle OWASP 4.

V rámci bezpečnostních testů bude dále provedena kontrola souladu technického řešení a režimu provozu technické provozní platformy Služeb CA s uvedenými bezpečnostními požadavky, normami a standardy. Kontrolován bude soulad dokumentace s uvedenými normami a soulad reality s dokumentací.

Auditní logování

Poskytovatel musí mít implementován systém auditního logování platformy CA, Web aplikace CA a integračního rozhraní na DPR, který zaznamenává všechny operace s certifikáty a všechny přístupy a operace Web aplikace CA. Poskytovatel musí na vyžádání auditní logy předat nebo zpřístupnit Zadavateli.

Řešení bezpečnostních incidentů

Poskytovatel musí mít implementován systém detekce a řízení bezpečnostních incidentů. Vzhledem k využití Služeb CA v rámci kritické informační infrastruktury resortu ministerstva financí, podléhající Zákonu o kybernetické bezpečnosti (dále jen ZKB), musí Poskytovatel hlásit předem definované bezpečnostní incidenty Zadavateli a poskytnout další informace o řešení těchto bezpečnostních incidentů tak, aby umožnil Zadavateli naplnění požadavků ZKB.

Dokumentace

V rámci přípravy Služeb CA Poskytovatel zhotoví a v průběhu provozu služeb musí udržovat následující dokumentaci:

- Detailní návrh Služeb CA
- Certifikační politika
- Dokumentace prokazující soulad s požadavky na uvedené bezpečnostní a provozní standardy

Fáze přípravy Služeb CA

Fáze přípravy Služeb CA probíhá mezi podpisem smlouvy a zahájením poskytování Služeb CA na produkčním prostředí.

Harmonogram

Hlavní milníky Služeb CA, zejména termíny zahájení poskytování služeb jsou uvedeny ve smlouvě. Harmonogram přípravy Služeb CA musí naplnit následující požadavky:

- Detailní návrh Služeb CA – dva týdny po podpisu smlouvy
- Zahájení integračního testování – 1 měsíc po podpisu smlouvy.
- Integrační testování – do zahájení poskytování Služeb CA na produkčním prostředí dle Smlouvy
- Předání dokumentace – dva týdny před zahájením poskytování Služeb CA na produkčním prostředí dle Smlouvy
- Migrace databáze certifikátů předchozího poskytovatele – k momentu zahájení poskytování Služeb CA na produkčním prostředí (detailní plán bude určen v Detailním návrhu)

Integrační testování

Integrační testování obsahuje následující části

- Funkční testy Služeb CA – navržené Poskytovatelem v Detailním návrhu, prováděné Poskytovatelem pod kontrolou Zadavatele.
- Integrační testy – prováděné Zadavatelem, zahrnuje testy Služeb CA v rámci end-2-end testů DPR.
- Zátěžový test Služeb CA - navržený Poskytovatelem v Detailním návrhu, prováděný Poskytovatelem pod kontrolou Zadavatele.
- Bezpečnostní test Služeb CA – prováděný Zadavatelem

V rámci Detailního návrhu je možné (po odsouhlasení Zadavatele) rozdělit fázi testování na menší úseky a určit kritické a nekritické prvky funkcionality pro jednotlivé úseky testování. Hlavním kritériem pro schvalování plánu testování bude dostatečný časový prostor pro všechny typy testů a zajištění spolupráce třetích stran. Časově nejkritičtějšími prvky funkcionality jsou integrace DPR a Web aplikace CA, vydávání certifikátů a související funkcionality Web aplikace CA. Implementace všech funkcí a všechny fáze testování ale musí skončit před zahájením Etapy vydávání certifikátů.

Poskytovatel je povinen poskytovat nezbytnou součinnost a bezodkladně řešit problémy pro všechny části testování.

Integrační testy budou probíhat primárně na testovacím prostředí. Zátěžové a bezpečnostní testy mohou probíhat na testovacím nebo na produkčním prostředí, před jeho spuštěním pro veřejnost.

Akceptované výstupy

Předmětem akceptace přípravy Služeb CA jsou

- Akceptace Detailního návrhu Služeb CA
- Akceptace dokumentace
- Akceptace zpráv o průběhu a výsledku testování

Řízení přípravy služeb

Poskytovatel zajistí po dobu přípravy Služeb CA roli odpovědného projektového manažera pro praktické projektové řízení. Projektový manažer Poskytovatele se bude účastnit jednání příslušných projektových týmů Zadavatele.

Smluvní záležitosti a projektové eskalace budou řízeny na úrovni odpovědných osob určených ve smlouvě.

Fáze provozu Služeb CA

Etapy provozu

Fáze produkčního provozu Služeb CA se rozděluje do dvou etap:

Etapa vydávání certifikátů – 60 měsíců– ve které jsou poskytovány následující služby

- Vydávání certifikátů
- Zneplatňování certifikátů a publikace CRL
- Kompletní funkcionalita Web aplikace CA a integrace s DPR
- Služby CA související s převzetím služeb od jiného předchozího poskytovatele
- Služby CA poskytované pracovníkům Zadavatele
- Technická podpora poplatníků

Etapa podpory vydaných certifikátů – 3 roky po ukončení etapy vydávání certifikátů – ve které jsou poskytovány následující služby

- Zneplatňování vydaných certifikátů
- Část Web aplikace CA – rozhraní pro zneplatňování certifikátů
- WebService pro následného poskytovatele pro zneplatňování certifikátů
- Publikace CRL
- Technická podpora poplatníků v rozsahu výše uvedených služeb Etapy podpory vydaných certifikátů

SLA řešení provozních incidentů a dostupnosti (v rozsahu funkcionality poskytované v aktuální Etapě) budou uplatňovány na celou Fázi provozu Služeb CA.

Řízení provozu

Poskytovatel musí zajistit řízení provozu Služeb CA v souladu s ISO 20000 (ITIL). Po celou dobu provozu Služeb CA zajistí Poskytovatel roli odpovědného Service Delivery Managera pro komunikaci s určenými osobami Zadavatele.

Smluvní záležitosti a provozní eskalace budou řízeny na úrovni odpovědných osob určených ve smlouvě.

Rozsah a kvalita Služeb CA bude akceptována na základě měsíční zprávy o rozsahu a kvalitě služeb, předkládané Poskytovatelem. Šablona měsíční zprávy musí být schválena v rámci detailního návrhu Služeb CA.

Řešení provozních incidentů

Poskytovatel musí mít implementován systém detekce a řízení provozních incidentů. Poskytovatel musí přijímat, řešit a ve svém systému řízení incidentů evidovat incidenty hlášené osobami pověřenými Zadavatelem. Poskytovatel musí zpřístupnit nebo poskytovat podklady o incidentech relevantních pro Služby CA a jejich řešení tak, aby umožnil řešení integračních problémů a kontrolu kvality Služeb CA.

Provozním incidentem se rozumí nahlášená odchylka chování Služeb CA od jejich popisu ve Smlouvě a v dokumentaci. Provozní incident může mít charakter vady (odchylka implementované

funkcionality od popisu ve Smlouvě a dokumentaci), nebo provozního problému. Provozní incidenty a vady budou klasifikovány Poskytovatelem do následujících kategorií. Zadavatel si vyhrazuje právo vyžádat změnu kategorie incidentu.

- Kategorie A - Kritické incidenty a vady s nejvyšší prioritou, které znemožňují užívání Služeb CA nebo jejich významné části nebo způsobují kritické provozní problémy.
- Kategorie B - Vážné incidenty a vady, které způsobují částečnou nefunkčnost nebo vážné omezení užívání Služeb CA nebo jejich významné části nebo způsobují vážné provozní problémy.
- Kategorie C - Ostatní incidenty a vady

SLA

Provozní doba 7x24

Dostupnost služeb 99,8%, definovaná jako poměrná část provozní doby, kdy není aktivní žádný incident kategorie A. Kalkulováno souhrnně na roční bázi.

Doba řešení (Odstranění vady) je čas od vzniku incidentu do jeho vyřešení (případně poskytnutí náhradního řešení a snížení kategorie incidentu)

- **Kategorie A: 4 hodiny**
- **Kategorie B: 8 hodin**
- **Kategorie C: 10 dnů**

Kapacitní a výkonnostní požadavky

Garantovaný výkon vydávání certifikátů 6 certifikátů za sekundu.

Maximální doba vydání certifikátu – 5 sec, za předpokladu zátěže nižší než garantovaný výkon vydávání certifikátů. Maximální doba vydání certifikátu se nevztahuje na CSR, pro které byl aktivován mechanismus řízení tempa vydávání certifikátů jednoho poplatníka.

Očekávaný počet vydávaných certifikátů je 2,3/6,9 miliónu certifikátů za celou Etapu vydávání certifikátů. **Horní limit počtu vydaných certifikátů** není určen a může být i vyšší.