Příloha č. 1

Specifikace předmětu plnění

Certifikační služby a časové služby pro resort Ministerstva financí

Pořízení a výdej certifikátů

I. Kvalifikovaný Poskytovatel služeb vytvářejících důvěru zajistí dle nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, příslušných prováděcích předpisů a prováděcích rozhodnutí EK v souladu s potřebami, záměry a provozovanými systémy resortu Ministerstva financí vydávání následujících certifikátů a s tím souvisejících služby:

1) Osobní - zaměstnanecké certifikáty, prvotní i následné
   A. Pár kvalifikovaného a komerčního certifikátu vydané na jednu žádost

2) Systémové, serverové nebo aplikační certifikáty, prvotní i následné
   B. Kvalifikované certifikáty pro elektronickou pečeť
   C. SSL DV a OV certifikáty
   D. Komerční serverové certifikáty

3) Osobní i serverové komerční autentizační certifikáty pro zajištění služeb spojených s poskytováním kvalifikovaných elektronických časových razítek

   E. Kvalifikovaná elektronická časová razítka

4) Ověřování platnosti elektronických uznávaných elektronických podpisů (zaručených elektronických podpisů založených na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaných elektronických podpisů), elektronických pečetí a časových razítek, českých i zahraničních, na příchozích dokumentech evidovaných
   F. Ověřování elektronických podpisů, elektronických pečetí a časových razítek

5) Výdej všech typů certifikátů v místě Objednatele
   G. Klientská registrační autorita

II. Další požadavky spojené s výdejem certifikátů

1) Vydávání certifikátů:
   a) bude prováděno pomocí klientských registračních autorit dostupných v Objednatelem stanovených lokalitách a provozovaných Pověřenými osobami Objednatele
   b) bude zajištěno minimálně v pracovní dny a v době od 7:00 – 19:00
   c) bude realizováno max. do 15 minut od zahájení procesu vydávání příslušnému zaměstnanci bez nutnosti jakékoli předchozí registrace
   d) všechny typy certifikátů (prvotní i následné) budou vydávány bezpapírovou formou

      To konkrétně znamená:

      - všechny dokumenty potřebné pro vydání prvotního certifikátu budou existovat v elektronické podobě,
      - všechny výše uvedené dokumenty budou uloženy v interním úložišti provozovaném Poskytovatelem, budou dostupné držiteli certifikátu po autentizaci komerčním certifikátem z páru kvalifikovaného a komerčního certifikátu vydaného na jednu žádost,
      - součástí procesu vydání certifikátu bude zaslání dvou e-mailů držiteli certifikátu: první bude obsahovat vydaný certifikát s funkčností jeho registrace do operačního systému se stažením nadřízených a kořenových certifikátů, druhý bude obsahovat odkaz do úložiště dokumentů; Poskytovatel je povinen zajistit, že se držitel certifikátu dostane v úložišti pouze ke svým dokumentům uloženým k jeho vydanému certifikátu,
      - Poskytovatel je povinen zajistit Pověřeným osobám Objednatele přístup do úložiště dokumentů ke všem dokumentům k vydaným certifikátům,
   e) úložiště dokumentů bude dostupné pro Pověřené osoby Objednatele on-line,
   f) generování klíčových párů u osobních certifikátů bude probíhat vždy na čipové kartě u Objednatele,
   g) je stanovena dostupnost služby (SLA) k bodům b), c) a g)
      - celková nedostupnost za rok – 3,65 dne,
      - maximální jednorázová garantovaná doba nepřetržité nedostupnosti – 4 hodiny,
   h) jakékoli plánované odstávky systému na straně Poskytovatele budou prováděny mimo pracovní dny.

2) Další požadavky:
   a) Poskytovatel umožní naplnění položek kvalifikovaných a komerčních certifikátů (osobní zaměstnanecké certifikáty) podle požadavků Objednatele sdělených Poskytovateli před podpisem Smlouvy, včetně integrace do prostředí Objednatele pro automatické načítání dostupných informací,
   b) Poskytovatel dodá řešení pro uložení osobních zaměstnaneckých certifikátů (včetně následných) na zařízení, která má certifikována,
   c) Poskytovatel zajistí ověření, zda je soukromý klíč ke konkrétnímu kvalifikovanému certifikátu pro elektronický podpis vygenerován na kvalifikovaném prostředku pro vytváření elektronických podpisů, a v případě, že ano, zajistí vložení položky QCStatements s naplněním id-tsi-qcs-QcSSCD (OID 0.4.0.1862.1.4) do rozšiřujících položek certifikátu,
   d) Poskytovatel zajistí interface pro vedení přehledu o vydaných certifikátech v prostředí Objednatele,
   e) Poskytovatel zajistí zasílání reportů o vydaných certifikátech na vyžádání,
   f) Poskytovatel umožní automatického stahování CRL,
   g) Poskytovatel zajistí možnost zneplatnění certifikátů Pověřenými osobami Objednatele,

h) Poskytovatel umožní spolupráci vybraných zaměstnanců Objednatele na přípravě a zpracování návodů a postupů směřujících k vydání a instalaci certifikátů,
i) Poskytovatel zajití vytvoření testovacího prostředí, testování bude možné rovněž v provozním prostředí,
j) Poskytovatel umožní vytvářet statistiky odběru služeb za jednotlivé Objednatele.

Klientská registrační autorita

Služba bude zajišťovat výdej všech typů certifikátů v místě Objednatele a bude realizována Pověřenými osobami Objednatele, které budou proškoleny Poskytovatelem.
Služba na základě dat dodaných Objednatelem umožní vygenerování žádosti o příslušný certifikát a zajistí jeho vydání příslušným kvalifikovaným Poskytovatelem služeb vytvářejících důvěru a nahrání na příslušný nosič. V případě osobních certifikátů se bude generovat a ukládat vždy na čipovou kartu uživatele.
Operátoru služby klientské registrační autority bude umožněno provést revokaci certifikátů i bez vědomí, souhlasu či spolupráce osoby (např. sdělení hesla pro zneplatnění), jíž byl certifikát vydán. Z bezpečnostního hlediska bude autentizace operátora služby klientské registrační autority vůči kvalifikovanému poskytovateli služeb vytvářejících důvěru prováděna výhradně příslušnými k tomu určenými certifikáty operátora služby registrační autority, umístěnými na kvalifikovaném HW prostředku, dodaném Poskytovatelem. Autentizace pouze uživatelským jménem a heslem nebude přípustná.

1) Zřízení a provoz služby klientské registrační autority
   a) Poskytovatel zajistí funkčnost a dostupnost služby pro Objednatele podle reálné potřeby.
   b) Služba klientské registrační autority bude provozována ve stanovených lokalitách, musí však být zajištěna jejich funkčnost pro operativní výjezdy do jiných lokalit.
   c) Služba klientské registrační autority bude umožňovat výdej potřebného certifikátu pro libovolného uživatele z resortu MF.
   d) Součástí zřízení služby bude prvotní vyškolení dvou operátorů, a zajištění následných školení při změnách nebo doplnění operátorů.

Kvalifikovaná elektronická časová razítka

1) Kvalifikovaný Poskytovatel služeb vytvářejících důvěru zajistí poskytování kvalifikovaných elektronických časových razítek podle nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS).
2) Pro vydávání časových razítek v režimu 365 x 24 je stanovena dostupnost služby (SLA) takto:
   a) celková nedostupnost za rok – 1,825 dne,
   b) maximální garantovaná doba nepřetržité nedostupnosti – 4 hodiny.
   Do této doby nejsou započítány plánované odstávky nahlášené minimálně 7 dní předem.
3) Z bezpečnostního hlediska bude autentizace žadatele o kvalifikované elektronické časové razítko u serveru TSA prováděna výhradně komerčními osobními nebo serverovými certifikáty, autentizace pouze uživatelským jménem a heslem nebude přípustná.
4) Garantovaná minimální propustnost poskytování časových razítek tj. počet ks razítek za 1 vteřinu je 10 ks.
5) Poskytovatel zajistí důvěryhodnost dokumentů (v souladu s požadavky zákona č. 297/2016 Sb.) opatřených kvalifikovaným elektronickým časovým razítkem; Poskytovatel zajistí pravidelné přerazítkování (tzv. archivaci) vydaných kvalifikovaných elektronických časových razítek pro Objednatele tak, aby každé razítko vydané po datu uzavření Smlouvy bylo plně ověřitelné po dobu 10 let od jeho vydání (např. pokud platnost elektronické značky/pečetě kvalifikovaného poskytovatele služeb vytvářejících důvěru, kterým je razítko podepsáno, činí 5 let, zajistí Poskytovatel ověřitelnost dokumentu vydáním prvotního a dalších následných zřetězených razítek tak, aby razítko bylo plně ověřitelné). Všechna vydaná kvalifikovaná elektronická časová razítka (prvotní i zřetězená) ukládá a spravuje Poskytovatel ve svých interních systémech, bez nutnosti interakce Objednatele.

6) Poskytovatel zpřístupní webovou aplikaci pro ověření stavu razítka (platné, bylo/nebylo přerazítkováno, stažení razítka i všech dalších zřetězených razítek).
7) Poskytovatel
   bude zasílat Objednateli statistiky odběru razítek.
8) Poskytovatel zpřístupní Objednateli testovací prostředí, testování umožní rovněž v provozním prostředí.
9) Jakékoli plánované odstávky systému budou realizovány mimo pracovní dny.

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů, elektronických pečetí a kvalifikovaných elektronických časových razítek

1) Kvalifikovaný poskytovatel služeb vytvářejících důvěru zajistí poskytování Kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů, pečetí a razítek (dále společně „podpisu“) podle nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), konkrétně článků 32, 33 a 40.

2) Vzhledem k tomu, že zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce zavedl 2-leté přechodné období, během kterého může být ze strany veřejnoprávního podepisujícího použit při podepisování dokumentu, kterým právně jedná, místo kvalifikovaného elektronického podpisu uznávaný elektronický podpis (zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis) a současně (bez přechodného období) může být při úkonu, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu použit uznávaný elektronický podpis nebo kvalifikovaný elektronický podpis, zajistí kvalifikovaný poskytovatel i ověřování platnosti uznávaného elektronického podpisu.

3) Služba je koncipována jako komponenta pro ověření platnosti podpisů instalovaná v prostředí Objednatele a volaná spisovou službou/DMS systémem. Služba ověření bude ověřovat dokumenty ve formátech PAdES a CAdES B-B a B-T (CAdES v interní i externí verzi) a XAdES B-B a B-T podle Prováděcího rozhodnutí Komise (EU) č. 2015/1506. Výstupem bude stav ověření (platný/neplatný podpis, nelze ověřit, důvod, proč nelze ověřit nebo proč je podpis neplatný), čas, ke kterému se ověřovalo, zdroj času (čas obdržení požadavku, časové razítko, parametr zadaný uživatelem, data, na základě kterých bylo ověření provedeno, legislativní typ podpisu, zda je certifikát na QESCD). Ověření bude mít charakter elektronicky podepsaného PDF/A verze 1b protokolu s připojeným kvalifikovaným elektronickým časovým razítkem a on-line zasílané elektronicky podepsané XML odpovědi v definované struktuře.

4) Ověřována bude platnost podpisu či podpisů v daném dokumentu. PDF protokol i XML data budou obsahovat tabulkovou strukturu vážící se k jednomu podpisu a struktur bude tolik, kolik bude v dokumentu podpisů (PDF/XML protokol je vždy jeden pro jeden dokument).

5) Budou ověřovány podpisy založené na certifikátech vydaných kvalifikovanými poskytovateli služeb vytvářejících důvěru uvedených na EUTL, resp. kvalifikovaných certifikátů pro elektronický podpis. V případě, že některý poskytovatel sice je uveden na EUTL, ale není možné dohledat validační data, bude podpis ověřen jako „nelze rozhodnout“.

6) Ověřovány budou i podpisy založené na již expirovaných certifikátech, a to i tehdy, pokud je v dokumentu již expirované časové razítko. To znamená, že ověření takového podpisu nebude odmítnuto, ale ověření proběhne s výsledkem, že podpis je neplatný a bude standardně vystaven protokol o ověření.

7) Kvalifikovaná elektronická časová razítka budou vydávána časovou autoritou Poskytovatele.

8) Pro službu ověřování platnosti podpisů v režimu 365 x 24 je stanovena min. dostupnost služby (SLA) 99,5 %, tj. celková nedostupnost služby činí 1 den 19 hod 48 min./rok. Do této doby nebudou započítány plánované odstávky nahlášené minimálně 7 dní předem. Maximální garantovaná doba nepřetržité nedostupnosti činí 30 min. Jakékoli plánované odstávky systému budou realizovány mimo pracovní dny.