

## Příloha č. 4 – Technická specifikace

### Popis současného stavu:

Pověření uživatelé jsou vybaveni tokenem a pomocí aplikace SECOM od společnosti 1.CA elektronicky podepisují a opatřují časovými razítky jednotlivé dokumenty. Spisová služba je provozována pomocí systému is-USYS.net. V něm se nachází většina dokumentů, které budou elektronicky pečetěny a razítkovány.

### Základní popis prostředí ČRo

Pracovní stanice: Desktopy a Notebooky se systémem Windows 7 nebo Windows 10 s poslední aktualizací, Antivir TrendMicro – Enterprise Security for Endpoints Light, Damage Cleanup Services, MS Office 2013.

Servery: Microsoft Windows Server 2008, 2012, 2016, Standard/Datacenter, Linux RedHat, CentOS, Debian, IBM AIX 7.X, Oracle Solaris 11.3

Virtualizace: VMware 5.5, 6.0, 6.X, AIX 7.X

### Popis cílového stavu:

Očekáváme kompletní dodávku řešení služby kvalifikovaného elektronického podepisování, pečetení, razítkování a ověřování elektronických certifikátů (tzn. zejména podpisů, razítek a pečeti a ověřování dokumentů). Uživatelé budou schopni jednotlivě nebo hromadně podepisovat dokumenty kvalifikovaným elektronickým podpisem a připojovat kvalifikovaná časová razítka v prostředí pracovních stanic. ČRo bude schopen přidávat k dokumentům kvalifikované pečeti s časovými razítky, samostatná razítka a ověřovat došlé dokumenty. Dodavatel bude zajišťovat službu správy certifikátů, sledování jejich platnosti a realizování včasné výměny.

### Podmínky dodávky:

1. Dodavatel musí mít status kvalifikovaného poskytovatele služeb vytvářejících důvěru 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 (dále též „eIDAS“), musí být na seznamu „kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru“ zveřejněným na stránkách Ministerstva vnitra ČR. <https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx>
2. Dodavatel dodá řešení služby **pečetení dokumentů** kvalifikovaným certifikátem pro elektronickou pečeť a kvalifikovaným prostředkem formou služby vzdáleného pečetení (se správou kvalifikovaného prostředku ve vlastnictví dodavatele, v jeho prostředí) ve smyslu článku 38 nařízení eIDAS. Předpokládaný objem dokumentů je cca 60 000 ks za rok.
3. Dodavatel dodá řešení služby kvalifikovaného **ověřování** platnosti kvalifikovaných elektronických podpisů a pečeti ve smyslu článku 33 nařízení eIDAS. Předpokládaný objem dokumentů je cca 70 000 ks za rok.

4. Dodavatel dodá řešení služby připojování kvalifikovaných elektronických **časových razítek** k dokumentům ve smyslu článku 42 nařízení eIDAS. Předpokládaný objem dokumentů je cca 530 000 ks za rok.
5. Dodavatel dodá řešení služby jednotlivého a hromadného elektronického podepisování dokumentů prostřednictvím kvalifikovaného certifikátu ve smyslu článku 28 nařízení eIDAS pro přibližně 300 uživatelů.
6. Dodavatelem dodané externí kvalifikované prostředky (úložiště privátního klíče kvalifikovaného certifikátu pro elektronický podpis) budou vždy s rozhraním USB.
7. Pro pečetění bude dodáno SW řešení, bez nutnosti investic do HW komponent.
8. Certifikáty budou vydávány Dodavatelem dle průběžných potřeb ČRo s ohledem na platnost již vydaných a potřebu nově zřizovaných a to ve formě nových i následných certifikátů. Dodavatel hlídá platnost již vydaných certifikátů a v případě nutnosti úkonů ze strany ČRo zašle v dostatečném předstihu informační emaily na všechny zainteresované osoby k zajištění plynulého provozu služby. Certifikáty musí být vydávány v souladu s požadavky nařízení eIDAS, zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů a v souladu s platnými certifikačními politikami Dodavatele jako kvalifikovaného poskytovatele služeb vytvářejících důvěru pro elektronické transakce.
9. K veškerým svým službám Dodavatel dodá uživatelský manuál v českém jazyce a navrhne způsob proškolení uživatelů, u kterých to bude v průběhu doby nutné.
10. Minimální úroveň SLA na všechny služby je 98 % v režimu 7/24/365.
11. Dodavatel musí být schopen obnovit službu po neplánovaném výpadku svých softwarových nebo hardwarových komponent nejpozději do 24 hodin.
12. Dodavatel musí zaslat písemnou informaci o jakýchkoli plánovaných odstávkách svých služeb a to nejpozději 3 pracovní dny předem. Tyto odstávky nesmí být delší než 24 hodin.
13. V případě nutnosti jakékoli změny Software nebo Hardware prostředků sloužících k realizování poskytovaných služeb, oznámí Dodavatel tuto skutečnost písemně a to nejpozději 3 pracovní dny předem.
14. Dodavatel se zavazuje dodat kontaktní email a telefonní číslo pro potřeby technických konzultací případně nestandardních situací. Po zadání dotazu ze strany ČRo bude Dodavatel reagovat nejpozději do následujícího pracovního dne.
15. Dodavatel dodá veškerou technickou dokumentaci, potřebnou pro provozování služby.
16. V případě neplánovaného výpadku, oznámí Dodavatel pověřené osobě na straně ČRo začátek i konec výpadku a to ihned po zjištění změny stavu, nejpozději však do 60 minut od začátku této změny. Písemný report pošle dodatečně, viz. bod 17.
17. Dodavatel bude v měsíční periodě zasílat reporting o čerpání služeb a s tím souvisejícími náklady na určené kontakty v ČRo. Součástí reportingu bude statistika nedostupnosti služeb s uvedením rozsahu a důvodu této nedostupnosti.
18. Dodavatel již v rámci zadávacího řízení přesně vyspecifikuje podmínky fyzické bezpečnosti, pokud nějaké budou.

19. Dodavatel zajistí možnost otestování poskytovaných služeb ještě před zahájením provozu a také kdykoli vznikne ze strany ČRo potřeba.
20. Zpracovávané dokumenty neopustí prostředí IT infrastruktury ČRo.
21. Elektronické podpisy a elektronické pečeti budou realizované pomocí kvalifikovaných prostředků, které jsou uvedené na seznamu vedeném evropskou komisí „Compilation of Member States notification on SSCDs and QSCDs”.
22. Služba ověřování elektronických podpisů a pečetí bude poskytována online i pro již zneplatněné, nebo propadlé certifikáty a to až 10 let zpětně.
23. Dodavatel zodpovídá za právní a technickou aktuálnost všech komponent nutných k poskytování požadovaných služeb s relevantností k právním a technickým předpisům a normám v návaznosti na eIDAS.
24. Dodávané čipové karty musí být plně kompatibilní s USB čtečkami ve formě tokenů MiniLector S-EVO, kterými jsou již zaměstnanci ČRo v současné době vybaveni.

### **Požadavky na kvalifikovaný prostředek pro vytváření elektronických podpisů:**

1. Nosič splňuje požadavky na kvalifikované prostředky pro vytváření elektronických podpisů definované nařízením Evropského parlamentu a Rady EU č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS); uchazeč je povinen tuto skutečnost doložit předložením jednoho z následujících dokladů (buď dle bodu a) nebo dle bodu b)):
  - a) Doklad (certifikát) o provedeném hodnocení kvalifikovaného prostředku pro vytváření elektronických podpisů podle standardu CWA 14169 – Secure signature-creation device na úroveň EAL 4+, a to licencovanou zkušební laboratoří na shodu s jedním z těchto profilů:
    - Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05 (BSI-PP-0004-2002)
    - Protection Profile - Secure Signature-Creation Device Type 2, Version 1.04 (BSI-PP-0005-2002)
    - Protection Profile - Secure Signature-Creation Device Type 3, Version 1.05 (BSI-PP-0006-2002).
  - b) Doklad (certifikát) o provedeném hodnocení kvalifikovaného prostředku pro vytváření elektronických podpisů podle standardu EN 419 211-1 – Protection profiles for secure signature creation device na úroveň EAL4 augmented with AVA\_VAN.5 licencovanou zkušební laboratoří na shodu s jedním z těchto profilů:
    - EN 419 211-2 (BSI-CC-PP-0059-2009)
    - EN 419 211-3 (BSI-CC-PP-0075-2012)
    - EN 419 211-4 (BSI-CC-PP-0071-2012)
    - EN 419 211-5 (BSI-CC-PP-0072-2012)
    - EN 419 211-6 (BSI-CC-PP-0076-2013).
2. Uchazeč zajistí ověření, zda je soukromý klíč ke konkrétnímu kvalifikovanému certifikátu pro elektronický podpis vygenerován na dodaném 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.
3. Data pro vytváření elektronických podpisů jsou generována kvalifikovaným prostředkem bez možnosti exportu.
4. Operace s daty pro vytváření elektronických podpisů vyžadují zadání PIN kódu.