

## Příloha č.4

### Technická specifikace veřejné zakázky „Sokolov – zajištění správy elektronických certifikátů vzdálenou formou – vzdálené podepisování a pečetění“

Poskytovatel je kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Poskytuje služby vzdáleného podepisování a pečetění pro vytváření kvalifikovaných podpisů a kvalifikovaných pečeti se souhlasem Ministerstva vnitra jakožto orgánu dohledu. Pro tyto služby poskytuje aplikační rozhraní pro integraci služeb podepisování a pečetění do aplikací a informačních systémů zadavatele, tak i pro použití na koncových stanicích uživatele.

Poskytuje, nebo zprostředkovává služby kvalifikovaného časového razítka. Zajišťuje dodávky kvalifikovaných certifikátů pro podpis a pečeť.

Poskytuje, nebo zprostředkovává služby vytváření komerčních elektronických podpisů na dálku jménem podepisující osoby. Zajišťuje dodávky komerčních certifikátů pro elektronické podpisy pro zaměstnance zadavatele vzdáleným způsobem.

#### Požadované služby

Nabízené řešení musí obsahovat minimálně všechny níže popsané služby a splňovat minimálně všechny níže popsané požadavky:

##### 1) Vzdálené podepisování

a) Služba zajišťuje vytváření kvalifikovaného elektronického podpisu využívající certifikované HSM (Hardware Security Module) zařízení umístěné u Poskytovatele a pod správou kvalifikovaného poskytovatele služeb, na kterém jsou uloženy příslušné klíče a související kvalifikované certifikáty pro vytváření kvalifikovaných elektronických podpisů prostřednictvím certifikované serverové aplikace.

b) Služba zajišťuje vytváření komerčního elektronického podpisu, prostřednictvím něhož se uživatelé přihlašují do JIP-KAAS (jednotného identitního prostoru-katalogu autorizačních a autentizačních služeb) a zabezpečující elektronické podepisování a šifrování e-mailové korespondence.

c) Uživatelé se musí před podpisem autentizovat, a potvrdit vlastní operaci podepsání např. zadáním PIN aby bylo zaručeno, že je toto prostředí používáno pod výhradní kontrolou podepisující osoby.

d) Automatická propagace certifikátů pro podepisování ze vzdáleného úložiště HSM do systémového úložiště certifikátů Windows, což umožní transparentní použití pro aplikace podporující podepisování certifikáty v systémovém úložišti Windows.

##### 2) Vzdálené pečetění

a) Služba zajišťuje vytváření kvalifikované elektronické pečeti využívající certifikované HSM (Hardware Security Module) zařízení umístěné u Poskytovatele a pod správou kvalifikovaného poskytovatele služeb, na kterém jsou uloženy příslušné klíče a související kvalifikované certifikáty pro vytváření kvalifikovaných elektronických pečeti prostřednictvím certifikované serverové aplikace.

b) Webové služby včetně dokumentace pro přístup aplikací objednatele ke službě vzdáleného pečetění (např. spisová služba ELISA).

##### 3) Poskytování časových razítek

a) Služba představuje poskytování kvalifikovaných časových razítek Poskytovatelem v rámci předmětných služeb bez nutnosti dalších smluv a požadavků na integraci.

b) Je možné je čerpat též z libovolných aplikací, které podporují standardní protokol dle RFC3161.

##### 4) Ověřování validity elektronicky podepsaných dokumentů

a) Služba zajistí pro systémy zadavatele úplné a správné ověření platnosti dokumentů opatřených elektronickým podpisem, elektronickou pečetí a časovým razítkem.

b) Je realizována v souladu s evropskou legislativou a respektováním českého právního prostředí (Nařízení EU č. 910/2014 a zákon č. 297/2016 Sb.).

c) Poskytuje jednoznačné výsledky ověření platnosti elektronických podpisů, pečeti a razítek poskytované formou strukturovaných XML dat, PDF dokumentu či HTML doložky.

d) Služba ověřuje podpisy ve formátech PAdES, CAdES, XAdES a ASiC v souladu s požadavky technických norem ETSI, na které je odkazováno z Nařízení (EU) eIDAS.

- 5) Uchovávání platnosti a ověřitelnosti elektronických podpisů, pečeti a časových razítek
- Služba zajišťuje uchovávání kvalifikovaných a zaručených elektronických podpisů či pečeti a elektronických časových razítek dle specifikací definovaných v Nařízení eIDAS přímo v původní aplikaci, kde jsou spravovány dokumenty.
  - Předpokládá se využití dokumentovými úložišti archivu, spisové služby a dalších informačních systémů zadavatele, které mají plný přístup k uchovávaným dokumentům a dle požadavků na jejich uchování řeší logiku pro prodloužení ověřitelnosti dokumentu. Zadavatel využívá informační systém GINIS, se kterým bude poskytovaná služba kompatibilní.
  - Cílem je zajištění dlouhodobé ověřitelnosti elektronických podpisů, pečeti a razítek.
- 6) Služba ověřování správnosti formátu PDF, konverzi dokumentů do PDF/A
- Služba zajišťuje vznik PDF dokumentu v archivním formátu PDF/A-1, PDF/A-2, PDF/A-3, případně novější verzi a zároveň jej opatří kvalifikovanou elektronickou pečeti a časovým razítkem ve formátu PAdES pro zachování jeho dlouhodobé ověřitelnosti a průkaznosti v souladu s § 5 odst. 2 zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.
  - Umožňuje provést konverzi libovolného souboru do formátu PDF, či PDF/A podle definovaných požadavků. Je možné nastavit úroveň souladu se specifikací PDF/A, podepsání dokumentu elektronickou pečeti, opatření kvalifikovaným časovým razítkem, opatření vodotiskem a další.
- 7) Administrace
- Centrální správa pověřenými zaměstnanci zadavatele s vysokým zabezpečením a možnost integrace do webových aplikací bez nutnosti vydávat osobní kvalifikované prostředky (karty, tokeny).
  - Přehled o vydaných certifikátech a provedených operacích s certifikátem.
  - Kontrola nad použitím a rychlá revokace certifikátu.
  - Obnova certifikátů před vypršením jejich platnosti.
  - Synchronizace uživatelů z adresářových služeb LDAP (MS Active Directory, OpenLDAP) Objednatele.
- 8) Další požadavky
- Podepisovat lze z jakéhokoliv počítače.
  - Podepisovat lze na jakémkoliv zařízení – PC, tablet.
  - Nezávislost na platformě a operačním systému.
  - Neomezený počet kvalifikovaných certifikátů pro zaměstnance zadavatele.
  - Neomezený počet kvalifikovaných elektronických podpisů.
  - Neomezený počet kvalifikovaných pečeti včetně certifikátů.
  - Neomezený počet kvalifikovaných časových razítek.
  - Neomezená spotřeba kvalifikované služby ověření certifikátů.
  - Neomezená spotřeba kvalifikované služby uchovávání certifikátů.
  - Zajištění servisní podpory a rozvoje, školení a konzultace uživatelům a administrátorům, metodické pomoci a uživatelské podpory.
  - o Poskytování poradenství k odstranění problémů, havárií příp. nefunkčnosti formou hot-line či helpdesku.
- 9) Zajištění aktualizací a implementací nových verzí v souladu s vývojem a legislativními změnami vždy nejpozději k datu, kdy případná legislativní změna vstoupí v platnost.
- 10) Implementace software včetně uvedení do provozu a zaškolení pověřených osob zadavatele
- 11) je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady 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“) a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
- 12) Bezobslužná instalace klientského SW na PC (Windows 10 a 11)