Příloha č. 1 – Technická specifikace

1. Požadavky na poskytovatele:

Poskytovatel garantuje, že poskytované služby budou v souladu s Nařízením EU 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a s další platnou legislativou EU a ČR.

Poskytovatel musí být uveden v Seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru vedeném národní autoritou (DIA).

Poskytovatel musí poskytovat minimálně:
- Kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů a pečetí,
- Kvalifikovanou službu uchování kvalifikovaných elektronických podpisů a pečetí.

Poskytovatel pro objednatele bude dále poskytovat, nebo zprostředkovávat služby:
- vzdáleného podepisování prostřednictvím kvalifikovaných certifikátů pro elektronické podpisy
- vzdáleného pečetění prostřednictvím kvalifikovaných elektronických pečetí
- vzdáleného kvalifikovaného časového razítka

Pro využití těchto služeb zajistí poskytovatel pro objednatele dodávky kvalifikovaných a komerčních certifikátů.

Poskytovatel zajistí pro kvalifikované služby vydávání kvalifikovaných certifikátů pro elektronické podpisy a vydávání kvalifikovaných certifikátů pro elektronické pečetě kvalifikovaného poskytovatele uvedeného v Seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru vedeného národní autoritou (DIA).

Poskytovatel pro zajištění služby vzdáleného podepisování a pečetění poskytne aplikační rozhraní pro integraci služeb podepisování a pečetění informačními systémy objednatele.

2. Rozsah implementace:

Požadované výstupy a služby
Implementace softwaru a služeb vytvářejících důvěru dle evropského nařízení eIDAS a souvisejících právních předpisů České republiky, a to:

- vzdálené elektronické podepisování dokumentů prostřednictvím kvalifikovaných a komerčních certifikátů z desktop (windows, macOS) i mobilních zařízení (iOS, android),
- vzdálené kvalifikované elektronické pečetění dokumentů,
- poskytování kvalifikovaných časových razítek,
- ověřování platnosti elektronických podpisů, pečetí a časových razítek,
- správa a ukládání klíčů a certifikátů používaných pro vytváření kvalifikovaných elektronických podpisů a pečetí,
- integrace se systémy Ginis společnosti Gordic a.s.,
- integrace na systémy formulářových řešení společnosti Software602 a.s. (FormFlow Server, FormAps server, FormFiller),
- Integrace s cloudovou platformu pro digitální podepisování dokumentů,
- integrace s Entra ID (Azure AD) objednatele,
- zpracování provozně technické dokumentace (PTD) řešení,
- zpracování implementačního projektu (návrh řešení) před zahájením implementace
- poskytování technické podpory.

Požadavky

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

1. Vzdálené podepisování a pečetění:
   1.1. Služba zajišťuje vytváření kvalifikovaného elektronického podpisu a kvalifikované pečetění, a to prostřednictvím vzdáleného přístupu k certifikátům.
   1.2. Služba využívá certifikované HSM (Hardware Security Module) zařízení umístěné u Poskytovatele a pod správou kvalifikovaného poskytovatele služeb – tj. provoz typu SaaS (Software as a Service). Na tomto HSM zařízení jsou uložené příslušné klíče a související kvalifikované a komerční certifikáty pro vytváření elektronických podpisů a pečetí prostřednictvím certifikované serverové aplikace.
   1.3. Uživatelé se musí před podpisem autentizovat, a potvrdit vlastní operaci podepsání, aby bylo zaručeno, že je toto prostředí používáno pod výhradní kontrolou podepisující osoby. Objednatel požaduje dvou faktorovou autentizaci. Možnost potvrzení pomocí PIN nebo aplikace v mobilu.
   1.4. 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 jednotlivých OS (např: Windows.,MACOS,…)
   1.5. Webové služby včetně dokumentace pro přístup aplikací objednatele ke službě vzdáleného pečetění

2. Poskytování časových razítek:
   2.1. Služba představuje poskytování kvalifikovaných časových razítek Poskytovatelem v rámci předmětných služeb bez nutnosti dalších smluv a požadavků na integraci.
   2.2. Je možné je čerpat též z libovolných aplikací, které podporují standardní protokol dle RFC3161.
   2.3. Služba zahrnuje i možnost čerpání časových razítek zřizovaným a zakládaným organizacím kraje

3. Ověřování validity elektronicky podepsaných dokumentů:
   3.1. Služba zajistí pro systémy objednatele úplné a správné ověření platnosti dokumentů opatřených elektronickým podpisem, elektronickou pečetí a/nebo časovým razítkem.
   3.2. Je realizována v souladu s evropskou legislativou a respektováním českého právního prostředí (Nařízení EU 910/2014 a zákon 297/2016 Sb.).
   3.3. Poskytuje jednoznačné výsledky ověření platnosti elektronických podpisů pečetí a razítek poskytované formou strukturovaných XML dat, PDF dokumentu či HTML doložky.
   3.4. Služba ověřuje podpisy v souladu s požadavky nařízení (EU) eIDAS.
   3.5. Služba zajišťuje dlouhodobou ověřitelnost elektronických podpisů, pečetí a časových razítek dle specifikací definovaných v Nařízení eIDAS.
   3.6. Služba uchovává auditní stopu každého úkonu minimálně s informacemi identifikující identitu podepisujícího, podepisovaný dokument a soukromý klíč kterým se podepisuje, případně další auditní data např čas

4. Služba ověřování správnosti formátu PDF, konverzi dokumentů do PDF/A:
   4.1. Služba zajišťuje vznik PDF dokumentu v archivním formátu PDF/A-1, PDF/A-2, PDF/A-3 a zároveň jej opatří kvalifikovanou elektronickou pečetí ve formátu PAdES pro zachování jeho dlouhodobé ověřitelnosti a průkaznosti.
   4.2. 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 pečetí, opatření kvalifikovaným časovým razítkem, opatření vodotiskem a další.

5. Integrace systému
   5.1. Objednatel provozuje Entra ID (Azure AD, AAD) provázanou v hybridním režimu s lokálním AD. Služba zajistí synchronizaci uživatelů systému vzdáleného podepisování s Azure AD objednatele. Všechny nezbytné identifikační údaje uživatele – jméno, příjmení, e-mail, osobní

číslo, guid, příp. další – budou automaticky načteny do systému z Azure AD objednatele. K synchronizaci systému vzdáleného podepisování s Azure AD objednatele budou využity funkce a rozhraní, které standardně Azure AD, případně služba Microsoft 365, nabízí, bez potřeby jejich dokupování.

5.2. Při administraci uživatelských účtů se správci systému vzdáleného podepisování nabídne seznam uživatelů z Azure AD objednatele, ze kterého si (ergonomicky, např. pomocí „našeptávače“) vybere.

5.3. Systém pečetění, vzdáleného podepisování a ověřování musí být dodán tak, aby byl integrován minimálně se dvěma aplikacemi systému Ginis společnosti Gordic spol. s r.o. A to Ginis SSL (spisová služba) a Ginis EPK (elektronická podpisová kniha). Systém vzdáleného podepisování bude umístěn na samostatný server, tj. nebudou se mísit na jednom serveru aplikační části vzdáleného podepisování a aplikace třetích stran. V rámci integrace s multiserverovým prostředím Ginis je tedy požadavkem objednatele nezasahovat do stávajícího systému a ponechat služby systému Ginis na stávajících serverech. Vlastní integrace spočívá v následujícím: Obě aplikace systému Ginis umožňují podepisování dokumentu. Služba vzdáleného podepisování musí dodat potřebné moduly IS Ginis tak, aby umožnily podpis prostřednictvím kvalifikovaných i komerčních certifikátů umístěných na HSM modulu včetně časového razítka, resp. odpovídající certifikáty (osobní kvalifikovaný a komerční certifikáty daného uživatele, případně el. pečeť, pokud má uživatel právo jí použít) musí být uživatelům systému Ginis nabídnuty k realizaci podpisu. Vzdálené podepisování musí fungovat jak z desktop operačních systémů, tak z přenosných i mobilních zařízení. Podepisování z mobilních OS musí být uživatelsky přívětivé a nesmí uživatele nutit ukládat soubory do mobilních zařízení a podepisovat soubory v jiné aplikaci. Musí být využito principu Single Sign On, aby se uživatel nemusel znovu přihlašovat, pokud je již přihlášen v IS Ginis.

5.4. prostřednictvím vzdáleného podpisovaní podepsat formuláře společnosti Software602 a.s. - objednatel využívá pro správu a řízení workflow formulářů systém FormFlow server, uživatelé formuláře vyplňují ve webovém rozhraní na aplikačním serveru FormApp nebo v klientské aplikaci FormFiller.

5.5. Bezobslužná hromadná instalace klientského SW na PC (Windows 10 a 11)

6. Administrace:

6.1. Centrální správa pověřenými zaměstnanci Objednatele s vysokým zabezpečením a možnost integrace do webových aplikací bez nutnosti vydávat osobní kvalifikované prostředky (karty, tokeny).

6.2. Přehled o vydaných certifikátech a provedených operacích s certifikátem

6.3. Kontrola nad použitím a rychlá revokace certifikátu

6.4. Obnova certifikátů před vypršením jejich platnosti

6.5. Synchronizace uživatelů z adresářových služeb LDAP (MS Active Directory,EntraID, OpenLDAP) Objednatele.

6.6. Ověřování uživatelů účty v síti Objednatele prostřednictvím protokolu SAML 2.0.

7. Součástí dodávky musí být „Provozně technická dokumentace“ (PTD) řešení. Všechna schémata budou předána ve zdrojovém tvaru (ArchiMate nebo Visio), umožňující aktualizaci objednatelem. Minimální požadavky na obsah jsou následující:

7.1. systémová příručka, uživatelská příručka, administrátorská příručka, bezpečnostní dokumentace

7.2. Popis infrastruktury – jednotlivé HW a SW komponenty (servery, zařízení, aplikace …) jejich komunikační matice (schéma jednotlivých komponent a jejich vazeb, co s čím komunikuje), nastavení HW a SW komponent, včetně nastavení operačních systémů,

7.3. Popis infrastruktury – jednotlivé HW a SW komponenty (servery, zařízení, aplikace …) jejich komunikační matice (schéma jednotlivých komponent a jejich vazeb, co s čím komunikuje), nastavení HW a SW komponent, včetně nastavení operačních systémů,

7.4. Popis integrace na AAD,

7.5. Popis správy certifikátů HSM,

7.6. Nastavení služeb na použitých serverech,

7.7. Popis integrace se systémem Ginis společnosti Gordic a.s., nastavení v systému Ginis (účty, funkční místa, parametry),

7.8. Popis integrace se systémy formulářových řešení společnosti Software602 a.s.,
7.9. Popis integrace s cloudovou platformu pro digitální podepisování dokumentů
7.10. Nastavení jednotlivých stanic a zařízení (klíčenka),
7.11. Nastavení VPN pro počítače a zařízení,
7.12. Postup, jak uživatel podepíše z počítače a zařízení (odkaz v mailu, odkaz na portále, aplikační prostředí uživatele …),
7.13. Popis komunikace HSM – AAD. Vazba (synchronizace) AAD,
7.14. Popis rozhraní API systému vzdáleného podepisování, aby bylo možné napojení dalších systémů a využít podepisování, pečetění, razítkování aplikacemi třetích stran, ukázka použití v PHP,
7.15. popis funkčních a technických vlastností, a to včetně organizačně technických opatření, která zajišťují zachování těchto vlastností,
7.16. Popis zálohování a postupy obnovy (plán kontinuity), co se zálohuje a kam, jak a kdo zálohy provádí (poskytovatel, objednatel),
7.17. Popis bezpečnostních opatření, která se uplatňují při zajišťování bezpečnosti systému VP,
7.18. Popis procesu spuštění a vypnutí aplikací pro VP,
7.19. Provádění aktualizací VP,
7.20. Monitoring systémů VP, co a jak se monitoruje,
7.21. Popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v IS, a návod na použití těchto funkcí.

8. Další požadavky:
8.1. Neomezený počet kvalifikovaných certifikátů pro zaměstnance objednatele v hlavním pracovním poměru, vedlejším pracovním poměru a zastupitelů v AAD
8.2. Neomezený počet kvalifikovaných elektronických podpisů
8.3. Neomezený počet kvalifikovaných pečetí včetně certifikátů
8.4. Neomezený počet kvalifikovaných časových razítek
8.5. Neomezená spotřeba kvalifikované služby ověření certifikátů
8.6. Neomezená spotřeba kvalifikované služby uchovávání certifikátů
8.7. Vysoká dostupnost řešení Služby dle bodů výše jsou dostupné v režimu 24x7 s garancí dostupnosti min. 99 %, propustnost min. 20 transakcí provedených za 1 minutu.
8.8. Aktualizace poskytované služby po celou dobu trvání této smlouvy, instalace oprav a bezpečnostních aktualizací