č.j. 7355/SFDI/331032/16370/2020

 CES SFDI 33/2020

**SMLOUVA O POSKYTOVÁNÍ SLUŽBY VYTVÁŘENÍ KVALIFIKOVANÝCH ELEKTRONICKÝCH PEČETÍ NA DÁLKU**

uzavřená podle § 1746 odst. 2 a násl. OZ mezi Stranami, kterými jsou:

|  |  |
| --- | --- |
| **OBJEDNATEL:** | **Státní fond dopravní infrastruktury** |
| Sídlo: | Sokolovská 1955/278, 190 00 Praha 9 |
| IČO: | 70856508 |
| DIČ: | CZ70856508 |
| Osoba oprávněná k podpisu Smlouvy | Ing. Zbyněk Hořelica, ředitel |
| Bankovní spojení: | xxx |
| Číslo účtu: | xxx |
| ID datové schránky: | e5qaihb |
| email: | podatelna@sfdi.cz |
| Kontaktní osoba Objednatele: | Ing. Miroslav Balík, tel. xxx e-mail: miroslav.balik@sfdi.cz  |
| Kontaktní osoba CENDIS:(dále jen „Objednatel“) | xxx, tel. xxx, e-mail: xxx  |
| a |  |
| **POSKYTOVATEL:** | **společnost eIDAS Solutions** |
| Sídlo:Bankovní spojení:Číslo účtu: | Hornokrčská 15, 140 00 Praha 4Česká spořitelna, a.s.976652 / 0800 |
|  |  |
| Vzniklá na základě Smlouvy o společnosti uzavřené podle § 2716 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, dne 15. dubna 2020 mezi společníky: |
|  |  |
| **Česká pošta, s.p.** |  |
| Sídlo: | Politických vězňů 909/4, 225 99 Praha 1 |
| Zápis v obchodním rejstříku: | Městský soud v Praze, oddíl A, vložka 7565 |
| IČO: | 47114983 |
| DIČ: | CZ47114983 |
| Osoba oprávněná k podpisu Smlouvy: | Mgr. Richard Gajdoš, manažer specializovaného útvaru VIP obchod, pověřen Ing. Romanem Knapem, generálním ředitelem na základě pověření ze dne 22.10.2020 |
|  |  |
| ID datové schránky: | kr7cdry |
| Kontaktní osoby: | xxx |
| Společník A |  |
|  |  |
| **Software602, a.s.** |  |
| Sídlo: | Hornokrčská 15, 140 00 Praha 4 |
| Zápis v obchodním rejstříku: | Městský soud v Praze, oddíl B, vložka 3044 |
| IČO: | 63078236 |
| DIČ: | CZ63078236 |
| Osoba oprávněná k podpisu Smlouvy: | Ing. Jiří Vacovský, provozní a finanční ředitel pověřen Ing. Richardem Kauckým , jediným členem představenstva, na základě plné moci ze dne 2.4.2019 |
| ID datové schránky: | 7dcsfzg  |
| Kontaktní osoby: | xxx |
|  | xxx |
| Společník B(dále jen „Poskytovatel“)(Společně dále též „Strany“) |  |
|  |  |

1. ÚVODNÍ UJEDNÁNÍ

Strany uzavřely Smlouvu, neboť Objednatel v Zadávacím řízení vybral Poskytovatele k uzavření Smlouvy na Veřejnou zakázku.

1. DEFINICE, VÝKLAD A PŘÍLOHY
	1. Ve Smlouvě mají níže uvedené pojmy a zkratky následující význam:
* **CENDIS, s.p.** je jiný subjekt s pověřením Objednatele se sídlem: nábřeží Ludvíka Svobody 1222/12, 110 15 Praha 1, IČO 00311391, pro kterého bude Poskytovatel zajišťovat Službu.CENDIS, s.p. vyvíjí a následně bude provozovat na základě uzavřené smlouvy s Objednatelem informační systém elektronické dálniční známky; dále také jen „CENDIS“;
* **DPH** je daň z přidané hodnoty;
* **Elektronický podpis** je platný elektronický podpis ve smyslu zákona č. 297/2016 Sb.;
* **IS EDAZ** je informační systém veřejné správy, který je definován zákonem č. 227/2019 Sb., kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů, a dalšími souvisejícími právními předpisy;
* **Kontaktní osoby** jsou osoby uvedené v úvodu Smlouvy;
* **Místem plnění** je sídlo Poskytovatele;
* **Nařízení eIDAS** Nařízení 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);
* **Objednatel** má význam uvedený v úvodu Smlouvy;
* **OZ** je zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů;
* **Poskytovatel** má význam uvedený v úvodu Smlouvy;
* **Právní předpisy** jsou obecně závazné právní předpisy České republiky a přímo použitelné právní předpisy Evropské unie v účinném znění;
* **SLA** (Service Level Agreement) definuje rozsah a kvalitu Služeb;
* **SLA report** je vyhodnocení průběhu poskytování Služeb a kvality Služeb včetně dostupnosti Služeb Poskytovatele a dalších výkonnostních požadavků;
* **Smlouva** je tato smlouva včetně všech jejích příloh;
* **Strana** je Objednatel nebo Poskytovatel;
* **Služba** je služba vytváření kvalifikovaných elektronických pečetí na dálku poskytovaná v souladu s požadavky uvedenými v Nařízení eIDAS, konkrétně článku 38 a 39, Příloze II a Příloze III., a v souladu s touto Smlouvou. Data pro vytváření kvalifikovaných elektronických pečetí vytváří a spravuje Kvalifikovaný poskytovatel služeb vytvářejících důvěru pro elektronické transakce jménem pečetící osoby (tj. jménem Objednatele);
* **Testovací prostředí** je prostředí s funkcionalitou obdobnou Službě poskytované v ostrém provozu, které Poskytovatel zpřístupní za účelem otestování Služby před nasazením do ostrého provozu;
* **Veřejná zakázka** je veřejná zakázka malého rozsahu „Poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku“, č.j. 7353/SFDI/310173/13593/2020;
* **Zadávací řízení** je zadávací řízení Veřejné zakázky;
* **Zákonem č. 297/2016 Sb.** zákon o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů;
* **ZRS** je zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
	1. Nedílnou součástí Smlouvy jsou následující přílohy:
		1. příloha Popis Služby.
1. PŘEDMĚT SMLOUVY
	1. Předmětem této Smlouvy je závazek Poskytovatele řádně a včas poskytovat Službu a závazek Objednatele za poskytování Služby zaplatit sjednanou cenu.
	2. Prostředky pro vytváření kvalifikovaných elektronických pečetí musí být uvedeny na seznamu vedeném Evropskou komisí: „Compilation of Member States notification on SSCDs and QSCDs“ https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.
2. POVINNOSTI POSKYTOVATELE
	1. Poskytovatel se zavazuje za účelem otestování Služby před nasazením do ostrého provozu zpřístupnit CENDIS Službu v Testovacím prostředí, s funkcionalitou obdobnou Službě v ostrém prostředí, a to nejpozději do 2 pracovních dnů od účinnosti Smlouvy.
	2. Pro Testovací prostředí platí SLA 95 % za kalendářní den a kapacita 5 vytvořených kvalifikovaných elektronických pečetí za minutu. Testovací prostředí bude poskytováno po celou dobu platnosti Smlouvy.
	3. Poskytovatel se zavazuje poskytovat Službu v ostrém provozu nejpozději do 5-ti pracovních dnů od účinnosti Smlouvy.
	4. Poskytovatel se zavazuje poskytovat Službu v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, se SLA 99,5 % za kalendářní den a kapacitou až 30 vytvořených kvalifikovaných elektronických pečetí za minutu.
	5. Poskytovatel se zavazuje poskytovat:
		1. provozní pohotovost Služby v režimu 24/7, technickou podporu při provozu Služby, řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím telefonního čísla xxx; a emailové adresy xxx.
		2. právní a technickou aktuálnost komponenty pro zajištění komunikace Poskytovatelem, jakož i celou Službu, v souladu s relevantními právními a technickými předpisy a normami v návaznosti na Nařízení eIDAS.
	6. Poskytovatel je povinen zpracovat za každý kalendářní měsíc rozpis skutečně poskytnutých Služeb a SLA report a předložit jej Objednateli do 5-ti kalendářních dnů po uplynutí každého kalendářního měsíce.
3. POVINNOSTI OBJEDNATELE
	1. Objednatel se zavazuje poskytovat součinnost při plnění této Smlouvy.
	2. Objednatel se zavazuje neposkytovat plnění poskytnuté Služby dalším osobám bez souhlasu Poskytovatele a nezneužívat poskytování Služeb. Služba bude využívána v rámci IS EDAZ.
4. CENA A PLATEBNÍ PODMÍNKY
	1. Cena Služby byla stanovena na základě cenové nabídky Poskytovatele podané v rámci Zadávacího řízení a činí:

|  |  |  |
| --- | --- | --- |
| **Počet kvalifikovaných elektronických pečetí od - do za měsíc** | **Paušální poplatek (Kč bez DPH/měsíc)** | **Cena za 1 ks** **kvalifikované elektronické pečeti(Kč bez DPH)** |
| 1 – 100 | 39 000,00 | 0,00 |
| 101 – 300 | 39 000,00 | 0,00 |
| 301 – 500 | 39 000,00 | 0,00 |
| 501 - 1 000 | 39 000,00 | 0,00 |
| 1 001 - 3 000 | 39 000,00 | 0,00 |
| 3 001 - 5 000 | 59 000,00 | 0,00 |
| 5 001 - 10 000 | 59 000,00 | 0,00 |
| 10 001 - 30 000 | 59 000,00 | 0,00 |
| 30 001 - 50 000 | 59 000,00 | 0,00 |
| 50 001 - 100 000 | 59 000,00 | 0,00 |
| 100 001 - 300 000 | 59 000,00 | 0,00 |
| 300 001 - 500 000 | 59 000,00 | 0,00 |
| 500 001 - 1 000 000 | 99 000,00 | 0,00 |
| 1 000 001 - 5 000 000 | 99 000,00 | 0,00 |

* 1. Cena za poskytování Služby v daném kalendářním měsíci bude stanovena podle počtu skutečně vytvořených kvalifikovaných elektronických pečetí v daném kalendářním měsíci a ceny za 1 kus kvalifikované elektronické pečeti podle příslušného objemového pásma. K této ceně bude připočten paušální poplatek ve výši pro dané objemové pásmo. K celkové ceně bude připočteno DPH podle aktuálně platných předpisů.
	2. Cena Služby je cenou konečnou a nepřekročitelnou zahrnující veškeré náklady Poskytovatele související s poskytováním Služby.
	3. Písemné odsouhlasení rozpisu skutečného poskytnutí Služeb a SLA reportu dle odst. 4.6 Smlouvy Kontaktní osobou Objednatele je nutnou podmínkou pro vznik práva Poskytovatele pro vystavení faktury a požadavku na úhradu příslušné částky Poskytovateli.
	4. Poskytovatel je povinen doručit fakturu a společně s fakturou předat Objednateli podklady k fakturaci, a to odsouhlasený rozpis skutečně poskytnutých Služeb a SLA report dle předchozího odst. této Smlouvy v příslušném kalendářním měsíci.
	5. Objednatel neposkytuje zálohy. Poskytovatel vystaví fakturu vždy jednou měsíčně za uplynulý kalendářní měsíc.
	6. Daňový doklad (faktura) bude obsahovat počet skutečně vytvořených kvalifikovaných elektronických pečetí; cenu za 1 kus kvalifikované elektronické pečeti v Kč bez DPH podle příslušného objemového pásma + paušální poplatek v příslušném pásmu.
	7. Úhrada za poskytování Služby bude provedena bezhotovostně Objednatelem na základě Poskytovatelem vystaveného daňového dokladu (faktury) na účet Poskytovatele uvedený v záhlaví Smlouvy. Faktura musí obsahovat všechny náležitosti daňového dokladu podle § 29 a násl. zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
	8. Pro úhradu faktury se sjednává doba splatnosti 30 dnů ode dne prokazatelného doručení faktury na e-mail Objednatele: podatelna@sfdi.cz. Splatnost faktury je dodržena, jestliže v poslední den lhůty splatnosti je fakturovaná částka odepsána z účtu Objednatele ve prospěch účtu Poskytovatele uvedeného v záhlaví Smlouvy.
	9. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit fakturu, která neobsahuje požadované náležitosti řádného účetního a daňového dokladu ve smyslu příslušných Právních předpisů, není doložena požadovanými nebo úplnými doklady, nebo obsahuje nesprávné cenové údaje. Ve vrácené faktuře musí Objednatel vyznačit důvod vrácení faktury. Poskytovatel je povinen vystavit novou fakturu s tím, že oprávněným vrácením faktury přestává běžet původní lhůta splatnosti a běží nová lhůta 14 kalendářních dní ode dne prokazatelného doručení opravené a všemi náležitostmi opatřené faktury Objednateli.
1. SMLUVNÍ SANKCE
	1. V případě nedodržení parametru SLA dostupnosti Služby uvedeného v odst. 4.4 této Smlouvy, tj. pokud dostupnost Služby klesne pod 99,5 % za kalendářní den, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 1.000,- Kč za každých započatých 0,1 %, o kterých klesne dostupnost poskytované Služby pod požadovanou hodnotu.
	2. V případě nedodržení parametru SLA dostupnosti Služby v Testovacím prostředí uvedeného v odst. 4.2 Smlouvy, tj. pokud dostupnost Služby klesne pod 95 % za kalendářní den, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 1.000,- Kč za každých započatých 0,1 %, o kterých klesne dostupnost poskytované Služby v Testovacím prostředí pod požadovanou hodnotu.
	3. V případě nesplnění povinností uvedených v odst. 4.5 písm. a) Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 1.000,- za každé takové porušení.
	4. V případě nesplnění povinností uvedených v odst. 4.5. písm. b) Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč za každé takové porušení.
	5. V případě prodlení Poskytovatele se zpřístupněním Služby dle odst. 4.1 Smlouvy, příp. s prodlením s poskytováním Služby dle odst. 4.3 Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 5.000,- Kč za každý i započatý den prodlení.
	6. V případě prodlení Objednatele se zaplacením faktury, je Objednatel povinen zaplatit Poskytovateli úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení.
	7. Smluvní pokutu nebo úrok z prodlení se povinná smluvní Strana zavazuje uhradit do 14 kalendářních dnů ode dne, kdy jí bude prokazatelně doručena písemná výzva k úhradě oprávněnou smluvní Stranou.
	8. Strany se dohodly, že uplatnění smluvní pokuty, dle jednoho ze shora uvedených ustanovení tohoto článku nevylučuje uplatnění smluvní pokuty dle jiného ustanovení tohoto článku nebo uplatnění náhrady vzniklé újmy.
2. ZÁVĚREČNÁ USTANOVENÍ
	1. Každá ze smluvních Stran má právo od Smlouvy odstoupit za podmínek uvedených v OZ.
	2. Tato Smlouva může být ukončena písemnou výpovědí i bez uvedení důvodu, a to s jednoměsíční výpovědní lhůtou ze strany Objednatele a tříměsíční výpovědní lhůtou na straně Poskytovatele, která počíná běžet prvním dnem kalendářního měsíce následujícího po měsíci, ve kterém byla doručena výpověď druhé Straně.
	3. Stranami bylo výslovně ujednáno, že vzájemné vztahy a právní vztahy Smlouvou neupravené se řídí obecně závaznými Právními předpisy.
	4. Smlouvu lze měnit pouze vzestupně očíslovanými písemnými dodatky podepsanými statutárními zástupci obou smluvních Stran nebo jimi písemně k tomu zmocněnými osobami.
	5. Strany souhlasí s uveřejněním Smlouvy v souladu se ZRS. Strany nepovažují obsah Smlouvy za obchodní tajemství. Uveřejnění Smlouvy zajistí Objednatel.
	6. Smlouva je uzavřena dnem připojení Elektronického podpisu poslední Strany k tomuto dokumentu a nabývá účinnost dnem uveřejnění Smlouvy v souladu se ZRS. Smlouva je uzavřena na dobu určitou, a to do vyčerpání finančního limitu 2 000 000 Kč bez DPH.
	7. Uzavřením této Smlouvy každá Strana předává druhé Straně za účelem zajištění řádného plnění Smlouvy seznamy kontaktních osob, které se budou podílet na plnění Smlouvy, s uvedením jejich osobních údajů: jméno, příjmení, titul, funkce, telefonický a e-mailový kontakt, u kterých právním důvodem pro jejich zpracování i Stranami, jako správci těchto osobních údajů, je jejich oprávněný zájem na splnění Smlouvy, na kterém se v mezích své kompetence podílejí subjekty údajů. Spolu s tím se každá Strana zavazuje zajistit informování subjektů těchto údajů a dalších subjektů údajů, jejichž osobní údaje se vyskytují ve Smlouvě, že byly při poskytnutí těchto osobních údajů informovány dle článku 13 nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) o zpracování poskytnutých osobních údajů pro účel plnění této Smlouvy, a že toto zpracování je v souladu s úpravou dle článku 6 odst. 1 písm. f) uvedeného nařízení a se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a dále, aby subjekty údajů byly informovány o svých právech v rozsahu, jak pro ně vyplývají z uvedeného nařízení a z citovaného zákona. Vzor prohlášení o informování je ke stažení na webových stránkách: www.sfdi.cz/gdpr.
	8. Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s dodávkou služeb hrazených z veřejných výdajů.
	9. Poskytovatel prohlašuje a zavazuje se, že po celou dobu platnosti této Smlouvy bude mít zajištěno plnění z pojistné Smlouvy na pojištění odpovědnosti za škodu s limitem plnění min. 2 000 000,- Kč.
	10. Strany prohlašují, že Smlouva vyjadřuje jejich svobodnou, vážnou, určitou a srozumitelnou vůli prostou omylu a tísně. Strany si Smlouvu přečetly, s jejím obsahem souhlasí, což stvrzují Elektronickými podpisy.
	11. Smlouva byla vyhotovena a podepsána v elektronické podobě a každá Strana obdržela její elektronický originál.

|  |  |  |
| --- | --- | --- |
| **Za Objednatele:** |  | **Za Poskytovatele:** |
|  |  |  |
| **Ing. Zbyněk Hořelica** |  | **Mgr. Richard Gajdoš** |
| ředitel |  | manažer specializovaného útvaru VIP obchod |
| **Státní fond dopravní infrastruktury** |  | **Česká pošta, s.p.** |
|  |  |  |
|  |  | **Ing. Jiří Vacovský** |
|  |  | provozní a finanční ředitel |
|  |  | **Software602, a.s.** |
|  |  |  |
|  |  |  |

Příloha č.1

# Popis služby

Dodavatel poskytuje služby vzdáleného pečetění pro vytváření kvalifikovaných pečetí se souhlasem Ministerstva vnitra jakožto orgánu dohledu.

<https://www.mvcr.cz/clanek/oznameni-o-udeleni-souhlasu-s-poskytovanim-sluzby-vytvareni-kvalifikovanych-elektronickych-podpisu-a-peceti-na-dalku-poskytovatel-software602-a-s.aspx>

Pro tyto služby poskytuje aplikační rozhraní pro integraci služeb pečetění do aplikací a informačních systémů Zadavatele, tak i pro použití na koncových stanicích uživatele. Aplikační rozhraní je integrováno v bezpečném perimetru Zadavatele.

Služba vytváření kvalifikovaných elektronických pečetí na dálku na svém vstupu akceptuje hash dokumentu určeného k opečetění a zajišťuje opatření tohoto hash kvalifikovanou elektronickou pečetí. Na tomto rozhraní garantujeme propustnost dle požadavků zadavatele.

## Vzdálené pečetění

Kvalifikovaný elektronický certifikát pro elektronickou pečeť pro vytváření kvalifikovaných elektronických pečetí je uložený na HSM prostředku nCipher nShield s odpovídající certifikací dle eIDAS. HSM jako kvalifikovaný prostředek pro vytváření elektronických pečetí (dále také jako QSealCD) je spravován kvalifikovaným poskytovatelem služeb vytvářejících důvěru, plně v souladu s požadavky na vytváření kvalifikovaných pečetí. Součástí dodávky je aplikační rozhraní webových služeb pro čerpání služby pečetění celých dokumentů a dat a prostředí pro zajištění vytvoření a správy kvalifikovaného certifikátu pro elektronickou pečeť v HSM prostředku.

# Certifikát pro pečeť

## Akceptované formáty certifikátu

Služba je připravena zajistit vytvoření kvalifikované elektronické pečeti dat určených k pečetění na základě elektronického certifikátu pro kvalifikovanou elektronickou pečeť. Elektronický certifikát pro kvalifikovanou elektronickou pečeť je vydáván Kvalifikovaným poskytovatelem certifikačních služeb vytvářejících důvěru (dále také jako QTSP) PostSignum a je vytvářen a spravován v QSealCD s odpovídající certifikací.

## Vytvoření certifikátu

V rámci Služby jsou používány kvalifikované certifikáty pro elektronickou pečeť od QTSP PostSignum jehož externí RA s pověřením vytváření tohoto certifikátu je Poskytovatel Služby. Žádost o certifikát je vytvořena přímo v certifikovaném QSealCD a následně i certifikát pečeti. Soukromý klíč nikdy neopouští QSealCD. Proces vytvoření a vydání certifikátu splňuje požadavky definované politikou vydávání elektronických certifikátů pro kvalifikovanou elektronickou pečeť od QTSP PostSignum http://www.postsignum.cz/certifikacni\_politiky\_qca.html.

## Použití certifikátu

Použití elektronického certifikátu pro kvalifikovanou elektronickou pečeť za účelem pečetění dat určených k pečetění a opatření kvalifikovaným elektronickým časovým razítkem je vždy iniciováno aplikací pro čerpání služby. Použití je dostupné pouze přes definované Rozhraní TSP a po odpovídající autentizaci uživatele služby autentizačním certifikátem. Veškerá komunikace probíhá po šifrovaném spojení a provozovatel služby nemá přístup k obsahu podepisovaného dokumentu ani přímý přístup k certifikátu pro pečetění bez vědomí pečetícího subjektu.

# Formát podpisu pro kvalifikovanou elektronickou pečeť

## PAdES

Jde o podpis využívaný pro pečetění PDF a PDF/A dokumentů. Jeho technická specifikace ETSI TS 103172 v.2.2.2 je uvedena zde: http://www.etsi.org/deliver/etsi\_ts/103100\_103199/103172/02.02.02\_60/ts\_103172v020202p.pdf

Současně také jako evropský standard ETSI EN 319 142 https://www.etsi.org/deliver/etsi\_en/319100\_319199/31914201/01.01.01\_60/en\_31914201v010101p.pdf

## XAdES

Jde o podpis využívaný pro pečetění strukturovaných dokumentů s datovou XML strukturou. Jeho technická specifikace ETSI TS 103171 v.2.1.1 je uvedena zde: http://www.etsi.org/deliver/etsi\_ts/103100\_103199/103171/02.01.01\_60/ts\_103172v020101p.pdf

Současně také jako evropský standard ETSI EN 319 132 https://www.etsi.org/deliver/etsi\_en/319100\_319199/31913201/01.01.01\_60/en\_31913201v010101p.pdf

## CAdES

Jde o podpis využívaný pro pečetění obecných binárních dat a dokumentů, u kterých není možné použít vložený pečeť. Jeho technická specifikace ETSI TS 103173 v.2.2.1 je uvedena zde: http://www.etsi.org/deliver/etsi\_ts/103100\_103199/103173/02.02.01\_60/ts\_103172v020201p.pdf

Současně také jako evropský standard ETSI EN 319 122 https://www.etsi.org/deliver/etsi\_en/319100\_319199/31912201/01.01.01\_60/en\_31912201v010101p.pdf

## ASiC

Jedná se o druh podpisu využívaný pro možnost pečetění více dokumentů najednou v rámci jednoho kontejneru. Jeho technická specifikace ETSI TS 103 174 v2.2.1. je uvedena zde:

http://www.etsi.org/deliver/etsi\_ts/103100\_103199/103174/02.02.01\_60/ts\_103174v020201p.pdf

Současně také jako evropský standard ETSI EN 319 162

http://www.etsi.org/deliver/etsi\_en/319100\_319199/31916201/01.01.01\_60/en\_31916201v010101p.pdf

# HSM

HSM zajišťující roli bezpečného prostředku pro vytváření kvalifikovaných certifikátů pro pečeť a kvalifikovaného prostředku pro vytváření kvalifikovaných pečetí na dálku jsou umístěné v dedikovaném prostoru v datovém centru se specifikací TIER III. Tyto prostředky jsou realizovány v režimu vysoké dostupnosti. Jedná se o dva prostředky HSM nCipher Connect 1500+ CC EAL4+ augmented, model NH2061. Tyto prostředky jsou uvedeny na seznamu prostředků <https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds> publikovaných Evropskou komisí.

# Postup zřízení služby

Služba vzdáleného pečetění je zřízena na základě smlouvy o poskytování služby s Dodavatelem služby.

Nutnou podmínkou pro čerpání služby je také smlouva o poskytování certifikačních služeb s kvalifikovaným poskytovatelem PostSignum CA.

## Žádost o vydání certifikátu

Oprávněný žadatel o kvalifikovaný certifikát pro vytváření kvalifikovaných pečetí je zaveden v seznamu oprávněných žadatelů. Tomuto uživateli je nejprve vydán kvalifikovaný komerční serverový certifikát pro autentizaci. Toto vydání certifikátu se řídí odpovídající politikou QTSP PostSignum a při tomto postupu je žadatel identifikován na základě předložení OP či jiného dokladu totožnosti. Operátor HSM tomuto uživateli odesílá do emailu uvedeného v tomto certifikátu odkaz do bezpečné webové aplikace Poskytovatele, do které se autentizuje vydaným komerčním serverovým certifikátem a potvrzuje žádost o vydání certifikátu pro kvalifikovanou elektronickou pečeť do HSM prostředku.

## Ověření identity uživatele

### Klientská registrační autorita

Oprávněný pracovník Zadavatele potvrzuje identitu žadatele o certifikáty a povoluje vydání certifikátu danému Uživateli Služby. Toto předpokládá smlouvu s poskytovatelem certifikačních služeb PostSignum pro poskytování služby Klientské registrační autority a administrativu spojenou s vydáváním certifikátů a potvrzováním identity žadatelů.

### Externí registrační autorita Software602

Identitu Uživatele potvrzuje v sídle firmy pracovník externí registrační autority – Software602. Tato služba pro vydání certifikátu pro kvalifikovanou elektronickou pečeť není zpoplatněna.

### Pobočky PostSignum – Registrační autorita / Mobilní registrační autorita

Žadatel o certifikát prokazuje svoji totožnost na kterékoliv pobočce PostSignum = síť poboček České pošty nebo pracovníkovi Mobilní registrační autority PostSignum.

## Potvrzení přijetí a vytvoření certifikátu

Po ověření totožnosti žadatele a schválení žádosti o vydání certifikátu žadatel do emailové schránky dostane potvrzení o schválení žádosti o vydání certifikátu. Po autentizaci certifikátem a akceptaci vydání certifikátu dokončuje ve webové aplikaci Poskytovatele vydání elektronického certifikátu pro kvalifikovanou elektronickou pečeť.

## Vydání následného certifikátu

Vydání následného certifikátu se řídí politikou vydávání certifikátů PostSignum - - http://www.postsignum.cz/certifikacni\_politiky\_qca.html.