Česká pošta

Číslo smlouvy	

PODMÍNKY POSKYTOVÁNÍ KVALIFIKOVANÝCH CERTIFIKÁTŮ PRO ELEKTRONICKOU PEČEŤ S PŘÍZNAKEM QSealCD

(Právnická osoba)

1. Předmět poskytované služby

1.1 Poskytovatel se zavazuje k vydání kvalifikovaného certifikátu pro elektronickou pečeť s příznakem QSealCD (dále jen „certifikát") za podmínek uvedených níže.

2. Povinnosti zákazníka

2.1 Zákazník se zavazuje:

2.1.1 Seznámit se s certifikační politikou PostSignum QCA pro kvalifikované certifikáty pro elektronickou pečeť, která je dostupná na webových stránkách poskytovatele www.postsignum.cz, a při žádosti o uvedený certifikát postupovat v souladu s touto certifikační politikou.

2.1.2 Zajistit, aby kvalifikovaný prostředek pro vytváření elektronických pečetí (dále jen „prostředek"), který bude použit pro uložení soukromého klíče k certifikátu, byl uvedený na oficiálním seznamu EU kvalifikovaných prostředků, který se nachází na webové adrese: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

2.1.3 Umožnit poskytovateli správu a provoz prostředku. Prostředek bude provozován a spravován v souladu s technickými podmínkami uvedenými v příloze č. 2 těchto Podmínek.

2.1.4 Umožnit poskytovateli přístup k prostředku ve svých prostorách za účelem jeho správy a provozu.

3. Povinnosti poskytovatele

3.1 Poskytovatel se zavazuje:

3.1.1 Jednat vůči zákazníkovi poctivě a v dobré víře.

3.1.2 Sdělovat zákazníkovi informace potřebné k řádnému plnění těchto Podmínek.

3.1.3 Bez zbytečného odkladu vydat certifikát, pokud budou splněny podmínky pro vydání certifikátu dle certifikační politiky a těchto Podmínek.

3.1.5 Zajistit provoz a správu prostředku zákazníka.

3.1.6 Zajistit, že soukromý klíč k certifikátu bude vygenerovaný přímo v prostředku a nebude ho možné z prostředku vyexportovat a ani ho do prostředku naimportovat (prostředek musí mít zapnutý mód FIPS 140-2 Level 3).

3.1.7 Přijmout taková technická a bezpečnostní opatření, aby nemohlo dojít k narušení bezpečnosti a důvěrnosti uloženého soukromého klíče v prostředku.

3.1.8 Zajistit, že soukromý klíč vygenerovaný v prostředku se může vyskytnout prakticky pouze jednou. Kopírování soukromého klíče je povoleno pouze za účelem jeho zálohy, přičemž bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat a počet zkopírovaných souborů dat nepřesáhne minimum potřebné pro zajištění kontinuity služby.

3.1.9 Vyhotovit z každého generování soukromého klíče Protokol o vygenerování soukromého klíče (dále jen „protokol"), viz vzor v příloze č. 1 těchto Podmínek. Tento protokol musí být ve formátu PDF elektronicky podepsaný osobním kvalifikovaným nebo komerčním certifikátem pracovníka poskytovatele. Protokol bude nedílnou součástí e-mailové žádosti o vydání certifikátu spolu s PKCS#10 žádostí.

4. Cena

4.1 Vydání kvalifikovaného certifikátu pro elektronickou pečeť je zpoplatněno dle aktuálního ceníku uvedeného na webových stránkách poskytovatele www.postsignum.cz, případně dle smluvních cen dohodnutých se zákazníkem.

4.2 V případě nutného výjezdu k zákazníkovi v souvislosti s poskytováním služby dle těchto Podmínek je zákazníkovi účtována cena za výjezd mobilní registrační autority poskytovatele dle aktuálního ceníku uvedeného na webových stránkách www.postsignum.cz.

5. Sankční ustanovení

5.1 V případě porušení povinností zákazníka uvedených v těchto Podmínkách, které bude mít za následek udělení pokuty poskytovateli orgánem dohledu dle zák. č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce je poskytovatel oprávněn požadovat po zákazníkovi zaplacení vyměřené pokuty v plném rozsahu.

6. Závěrečná ujednání

6.1 Právní vztahy výslovně neupravené těmito Podmínkami včetně informací o zpracování osobních údajů se řídí příslušnými ustanoveními smlouvy včetně Všeobecných obchodních podmínek certifikačních služeb, ke které se tyto Podmínky vztahují, a dále dokumenty uvedenými v odst. 6.2 těchto Podmínek a obecně závaznými právními předpisy. V případě rozporu textu těchto Podmínek s textem smlouvy, má přednost text těchto Podmínek.

6.2 Zákazník prohlašuje, že se seznámil s dokumentem „Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronickou pečeť" a podpisem těchto Podmínek s nimi souhlasí. Uvedené dokumenty jsou dostupné na webových stránkách www.postsignum.cz.

6.3 Podmínky jsou vyhotoveny ve 2 stejnopisech, z nichž každá smluvní strana obdrží po jednom.

6.4 Součástí těchto Podmínek je vzor Protokolu o vygenerování soukromého klíče a podmínky správy a provozu HSM.

7. Podpisy smluvních stran

Za poskytovatele

Praha — 11.9.18

Místo — Datum

[redacted]

Jméno a příjmení

CGI IT Czech Republic s.r.o.
[illegible] 2800/4, 155 00 Praha 5
[illegible] 02412388, DIČ: CZ62412388

Podpis a razítko

Za zákazníka

11.9.18

Místo — Datum

OTE, a.s.
Sokolovská 192, 79, 186 00 Praha 8
IČ: 26463318, DIČ: CZ26463318

[redacted]

Jméno a příjmení

Podpis a razítko

Česká pošta

PROTOKOL O VYGENEROVÁNÍ SOUKROMÉHO KLÍČE

Příloha č. 1

Protokol o vygenerování soukromého klíče v kvalifikovaném prostředku pro vytváření elektronických pečetí

Údaje o zákazníkovi

Název zákazníka:

IČO:

Č. smlouvy o poskytování certifikačních služeb:

Údaje o kvalifikovaném prostředku pro vytváření elektronických pečetí

Název výrobce:

Typ:

Sériové číslo:

Verze firmware:

[redacted]

Údaje o soukromém klíči

Datum a čas generování:

ID soukromého klíče:

Modulus:

[redacted]

Datum a čas generování:

SHA256 otisk:

Modulus:

Stvrzuji svým podpisem, že soukromý klíč, který bude používaný pro vytváření kvalifikovaných elektronických pečetí na základě vydaného kvalifikovaného certifikátu pro elektronickou pečeť, byl vygenerován výhradně v kvalifikovaném prostředku pro vytváření elektronických pečetí, není ho možné z tohoto prostředku vyexportovat a vyskytuje se prakticky pouze jednou.

Datum a čas vyhotovení protokolu:

Viditelný elektronický podpis pracovníka poskytovatele:

Příloha č. 2

Nastavení HSM pro potřeby QSealCD

Nastavení HSM jako QSealCD obnáší především následující:

- provoz HSM s předepsaným certifikovaným firmwarem a předepsaným klientským SW
- vytvoření konfigurace Security Worldu v souladu s dokumentem *„ASEC1382 nShield® HSM family v11.72.02 – Common Criteria Evaluated Configuration Guide"*
- provoz HSM modulu v režimu FIPS 140-2 Level 3 garantující vytvoření klíčů přímo v HSM modulu
- vytvoření administrátorského setu čipových karet (ACS set), přičemž celý ACS set bude v držení poskytovatele
- vytvoření operátorského setu čipových karet (OCS set) nebo Softcard pro kontrolu a použití kryptografických klíčů, přičemž v případě OCS setu bude celý set v držení poskytovatele
    - vytvořený OCS set nebo Softcard musí sloužit k ochraně právě jednoho páru klíčů ke kvalifikovanému certifikátu pro elektronickou pečeť
    - zákazníkovi – vlastníkovi HSM bude v případě OCS setu zapůjčena část setu nezbytná pro aktivaci soukromého klíče kvalifikovaného certifikátu pro elektronickou pečeť

Způsob provozu HSM a řešení výjimečných situací

Při běžném provozu HSM modulů v eIDAS compliant konfiguraci pod správou QTSP mohou nastat tyto situace:

1. Rutinní operace:
    - Aktivace a používání soukromého klíče ke kvalifikovanému certifikátu pro elektronickou pečeť v aplikacích
    - Zálohování konfigurace HSM
    - Kontrola logů HSM infrastruktury, SNMP dohled
2. Provozní operace
    - Správa OCS setu nebo Softcard (vytvoření nového, obnova původního a smazání) chránícího pár klíčů ke kvalifikovanému certifikátu pro elektronickou pečeť
    - Vygenerování páru klíčů a import kvalifikovaného certifikátu pro elektronickou pečeť
    - Smazání páru klíčů ke kvalifikovanému certifikátu pro elektronickou pečeť
3. Výjimečné provozní operace vyžadující přítomnost úplného kvora karet ACS setu
    - Vybrané povolené administrátorské operace
    - Reset HSM a jeho nová inicializace do HSM infrastruktury
    - Logické zařazení nového HSM do konfigurace HSM infrastruktury (např. pro situace přidání nového modulu nebo jeho výměny za jiný v rámci standardní technické podpory výrobce)
    - Aktualizace firmware – pouze teoretická možnost, neboť se nepředpokládá jiná certifikovaná verze FW pro stávající HSM moduly

Veškeré operace uvedené v bodech 2. – 3. je povinen provádět pouze poskytovatel. Ze všech operací uvedených v bodech 2. a 3. vznikne protokol, který bude potvrzen poskytovatelem a zákazníkem – vlastníkem HSM.

Operace uvedené v bodě 1. je oprávněn provádět zákazník – vlastník HSM. Zákazník – vlastník HSM je taktéž oprávněn provádět správu vlastních OCS setů nebo Softcard včetně manipulace s klíči, které tyto OCS sety budou chránit.