Česká pošta

PODMÍNKY POSKYTOVÁNÍ KVALIFIKOVANÝCH CERTIFIKÁTŮ PRO ELEKTRONICKÝ PODPIS S PŘÍZNAKEM QSignCD
(Právnická osoba)

Česká televize

IČO: 00027383

a

Software602 a. s.

IČO: 63078236

DODATEK Č. 1

KE SMLOUVĚ OBJI-22000198

Předmět smlouvy: **vydávání kvalifikovaných certifikátů vzdáleného podepisování a pečetění**

Cena, případně hodnota dodatku: **0 Kč**

Datum uzavření: 06-10-2020

DODATEK Č. 1 (VER220-00138)
KE SMLOUVĚ Č. OBJI-22000198

Česká televize
IČO: 00027383, DIČ: CZ00027383
Sídlo: Kavčí hory, Na Hřebenech II 1132/4, 140 70 Praha 4
zřízená zákonem č. 483/1991 Sb., o České televizi, nezapisuje se do obchodního rejstříku
zastoupená: Davidem Břinčilem, ředitelem divize Finance
bankovní spojení: Česká spořitelna a.s., č.ú. 1540252/0800
(dále jako „zákazník" nebo „ČT")

a

Software602 a.s.
IČO: 63078236, DIČ: CZ63078236
Sídlo: Hornokrčská 703/15, Krč, 140 00 Praha 4
Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B3044
Zastoupená: [redacted], na základě zmocnění dle Smlouvy o zajištění externí registrační autority pro Českou poštu ze dne 3.3.2015 č. 900-1005/2015

(dále jako „Poskytovatel" nebo „Software602")

PREAMBULE

Objednávka č. OBJI-22000198 (smlouva) ze dne 4.9.2020 (v Registru smluv uveřejněna dne 7.9.2020) byla uzavřena mezi ČT a dodavatelem Software602 na základě výběrového řízení na veřejnou zakázku malého rozsahu s názvem „**Služba vzdáleného podepisování a pečetění**". Dodavatel Software602 provedl implementaci software potřebného pro správu a ověřování certifikátů a prohlašuje, že je oprávněn poskytovat služby na základě uzavřené smlouvy. Součástí služby dodavatele Software602 je i správa, vydávání a zneplatňování samotných certifikátů, a to na základě smlouvy s Českou poštou s.p. ze dne 3.3.2015, která je provozovatelem certifikační autority PostSignum.

1. Předmět poskytované služby

1.1 Poskytovatel se zavazuje k vydání kvalifikovaného certifikátu pro elektronický podpis s příznakem QSignCD (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 elektronický podpis, 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 podpisů (dále jen „prostředek"), který bude použit pro uložení soukromých klíčů k certifikátům, 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. Tuto povinnost zajišťuje společnost Software602 a.s.

2.1.3 Zajistit bezpečný přístup k odpovídajícímu soukromému klíči kvalifikovaného certifikátu pro elektronický podpis až po jednoznačné a průkazné identifikaci držitele tohoto certifikátu. Tuto povinnost zajišťuje společnost Software602 a.s.

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.

3.1.4 Zajistit provoz a správu prostředku zákazníka.

3.1.5 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).

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

3.1.7 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.

3.1.8 Zajistit vygenerování RSA klíče v prostředku, který bude sloužit pro ověření původu soukromých klíčů (dále jen „servisní klíč").

3.1.9 Vyhotovit z každého generování servisního klíče Protokol o vygenerování servisního klíče (dále jen „protokol"), viz vzor v příloze č. 1 těchto Podmínek.

4. Cena

4.1 Vydání kvalifikovaného certifikátu pro elektronický podpis je již zpoplatněno na základě objednávky č. OBJI-22000198 s dodavatelem eIDAs řešení pro vzdálený elektronický podpis.

5. Závěrečná ujednání

5.1 Zákazník a Poskytovatel prohlašují, že se seznámili s dokumentem „Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronický podpis" a podpisem těchto Podmínek s nimi souhlasí. Uvedené dokumenty jsou dostupné na webových stránkách www.postsignum.cz.

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

5.3 Součástí těchto Podmínek je vzor Protokolu o vygenerování servisního klíče a podmínky správy a provozu HSM.

6. Podpisy smluvních stran

Za poskytovatele

Praha	6.10.2020	[redacted]
Místo	Datum	Digital signature: [redacted] 10/06/2020 05:40 PM
[redacted]		
Jméno a příjmení		Podpis a razítko

Za zákazníka

Praha	6.10.2020	[redacted]
Místo	Datum	
David Břinčil, ředitel divize Finance		
Jméno a příjmení		Podpis a razítko

Česká pošta

PROTOKOL O VYGENEROVÁNÍ SERVISNÍHO KLÍČE

Příloha č. 1

Protokol o vygenerování servisního klíče v kvalifikovaném prostředku pro vytváření elektronických podpisů

Údaje o zákazníkovi

Název zákazníka:	Česká televize
IČO:	00027383
Č. smlouvy o poskytování certifikačních služeb:	101006-000132

Údaje o kvalifikovaném prostředku pro vytváření elektronických podpisů

Název výrobce:	Thales e-Security Ltd.
Typ:	nShield Connect 1500+
Sériové číslo:	[redacted]
Verze firmware:	2.55.1
Číslo certifikačního protokolu uvedeného na seznamu SSCD/QSCD EU *	[redacted]

* https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Údaje o servisním klíči

Datum a čas generování:	24. 9. 2020 8:22:38
ID soukromého klíče:	[redacted]
Modulus:	[redacted]

Stvrzuji svým podpisem, že servisní klíč, který bude používaný pro ověření původu vygenerovaných soukromých klíčů používaných k vytváření kvalifikovaných elektronických podpisů na základě vydaných kvalifikovaných certifikátů pro elektronický podpis, byl vygenerován výhradně v kvalifikovaném prostředku pro vytváření elektronických podpisů, není ho možné z tohoto prostředku vyexportovat a vyskytuje se prakticky pouze jednou (není aktivně používaný v jiném prostředku).

Datum a čas vyhotovení protokolu:	
Viditelný elektronický podpis pracovníka poskytovatele:	[redacted] Digital signature: [redacted] 10/06/2020 05:40 PM

Příloha č. 2

Nastavení HSM pro potřeby QSignCD

Nastavení HSM jako QSignCD 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 elektronický podpis
    - zákazníkovi – vlastníkovi HSM bude v případě OCS setu zapůjčena část setu nezbytná pro aktivaci soukromého klíče kvalifikovaného certifikátu pro elektronický podpis

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 elektronický podpis 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 elektronický podpis
    - Vygenerování páru klíčů a import kvalifikovaného certifikátu pro elektronický podpis
    - Smazání páru klíčů ke kvalifikovanému certifikátu pro elektronický podpis
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 bodě 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.