Číslo Smlouvy MF
18/070/0003/01
Toto číslo uvádějte při fakturaci

Dodatek č. 1

ke smlouvě o poskytování certifikačních služeb a časových služeb

uzavřené dne 24. 9. 2018
mezi
Českou republikou – Ministerstvem financí (evidovaná pod č. 18/070/0003)
a
První certifikační autoritou, a.s.

(dále jen „Dodatek“)
evidenční číslo MF: 9006/025/2019

Česká republika – Ministerstvo financí
sídlo: Letenská 15, 118 10 Praha 1
IČO: 00006947
DIČ: CZ00006947
banka: ČNB Praha 1
č. účtu: 3328001/0710
ID datové schránky: xzeaauv
za níž jedná: xxxxxxxxxx
(dále jen „Objednatel“)
a

První certifikační autorita, a.s.
sídlo: Podvinný mlýn 2178/6, 190 00 Praha 9 - Libeň
zapsaný/á v obchodním rejstříku vedeném u Městského soudu v Praze pod spisovou značkou B 7136
IČO: 26439395
DIČ: CZ26439395
banka: Československá obchodní banka, a.s.
č. účtu: 168457418/0300
ID datové schránky: a69fvfb
zastoupená: Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva a
Ing. Romanem Kučerou, členem představenstva
(dále jen „Poskytovatel“)

Objednatel a Poskytovatel dále společně jako „Smluvní strany“ a každý jednotlivě jako „Smluvní strana“)

Preambule:

A. Smluvní strany mezi sebou uzavřely dne 24. 9. 2018 Smlouvu o poskytování certifikačních služeb a časových služeb, č. smlouvy MF 18/070/0003, evidenční číslo MF 7005/010/2018 (dále jen „Smlouva“), jejímž předmětem je kompletní zajištění služeb vytvářejících důvěru, tj. výdej kvalifikovaných certifikátů pro elektronický podpis, systémových certifikátů, kvalifikovaných certifikátů pro elektronickou pečeť, komerčních certifikátů, komerčních serverových certifikátů, kvalifikovaných elektronických časových razítek, včetně jejich archivace a ověřování platnosti kvalifikovaných elektronických podpisů a pečetí, 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, a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, a dále služba klientských registračních autorit, metodická a technická podpora při napojení služeb na systémy PKI, správa vydaných certifikátů a školení operátorů klientských registračních autorit.

B. Objednatel a Poskytovatel se dohodly na upřesnění Smlouvy týkající se kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů, elektronických pečetí a kvalifikovaných elektronických časových razítek. Smluvní strany se dohodly na změně Smlouvy a to konkrétně na změně Přílohy č. 1 Smlouvy.

Článek 1 – Účel a Předmět Dodatku

1. Účelem uzavření tohoto Dodatku Smlouvy je upřesnění Smlouvy týkající se kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů, elektronických pečetí a kvalifikovaných elektronických časových razítek.

2. Předmětem této Smlouvy je doplnění a nahrazení textu bodu 3) Přílohy č. 1.

Článek 2 – Změny Smlouvy

Smluvní strany se dohodly, že Bod 3) Přílohy č. 1 Smlouvy - Specifikace předmětu plnění v části „Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů, elektronických pečetí a kvalifikovaných elektronických časových razítek“ se plně nahrazuje následujících textem:

„3) Služba je koncipována jako komponenta pro ověření platnosti podpisů instalovaná v prostředí Objednatele a volaná spisovou službou/DMS systémem. Služba ověření bude ověřovat dokumenty ve formátech PAdES a CAdES B-B a B-T (CAdES v interní i externí verzi) a XAdES B-B a B-T podle Prováděcího rozhodnutí Komise (EU) č. 2015/1506. Výstupem bude stav ověření (platný/neplatný podpis, nelze ověřit, důvod, proč nelze ověřit nebo proč je podpis neplatný), čas, ke kterému se ověřovalo, zdroj času (čas obdržení požadavku, časové razítko, parametr zadaný uživatelem, data, na základě kterých bylo ověření provedeno, legislativní typ podpisu, zda je certifikát na QESCD), tj. náležitosti uvedené v § 4 odst. 7 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů. Ověření bude mít charakter elektronicky podepsané XML odpovědi v definované struktuře, vhodné pro automatizované zpracování. Současně jsou ukládána data pro následné generování PDF protokolu v případě požadavku Objednatele (generuje Poskytovatel). Jeho účelem je potvrdit výsledek ověření i v lidsky čitelné formě v případě požadavku doložení např. před soudem.

Služba též umožňuje ověřit platnost podpisu/pečetě obálky datové zprávy Informačního systému datových schránek formátu ZFO. Službě je možné předložit prostřednictvím metody pro ověření podpisu CAdES celý ZFO soubor bez předchozího parsování. Služba však nepodporuje ověření podpisů/pečetí obsahujících atribut specifikující použitou podpisovou politiku (PP). Z tohoto důvodu nebude obvykle výsledkem ověření indikace

TOTAL-PASSED. Zároveň je třeba upozornit, že v případě vložení ZFO na vstup ověření je kompletní obsah datové zprávy považován čistě za podepisovaná data, a to včetně příloh. Nedochází tedy k rekurzivnímu prohledávání příloh uvnitř ZFO a jejich případnému ověřování. Pokud je požadováno ověření podpisů jednotlivých příloh, je odpovědností volající aplikace příslušnou přílohu z obálky ZFO extrahovat a do služby pro ověření poslat zvlášť.

Služba je dále doplněna o nekvalifikovanou nadstavbu pro ověřování platnosti uznávaných elektronických podpisů e-mailových zpráv formátu S/MIME. V tomto případě služba ověří platnost certifikátu, na němž je uznávaný elektronický podpis založen včetně kryptografické správnosti podpisu a hashe podepsaných dat a vrátí elektronicky podepsanou XML odpověď, která bude obsahovat informace o typu podpisového certifikátu, vydavateli, době jeho platnosti, zda je certifikát na QESCD, revokaci, atd. a případné info o problémech s ověřením kryptografické platnosti podpisu ve struktuře shodné s ověřením podpisu u kvalifikované služby. Výsledek ověření je však informativní a vzhledem k praktické nekonformnosti S/MIME podpisů se standardy dle eIDAS prakticky nikdy neskončí výsledkem TOTAL-PASSED. Poskytovatel neručí a nenese žádnou odpovědnost za ověření kompletního podpisu e-mailové zprávy a rozparsování S/MIME formátu na externí podpis a data, jež jsou následně zpracovávána kvalifikovanou službou. V tomto případě se neuplatní poslední odstavec bodu 1. čl. 13 nařízení eIDAS, neboť nejde o kvalifikovanou službu, byť je poskytována kvalifikovaným poskytovatelem.

Při ověřování platnosti podpisu/pečetě obálky datové zprávy formátu ZFO i e-mailové zprávy formátu S/MIME neověří služba platnost časového razítka. Důvodem je skutečnost, že dle normy EN 319 102-1, definující postup ověřování, se při ověřování podpisu s razítkem nejdříve provede Basic validační proces a pouze pokud skončí s jedním z výsledků PASSED, INDETERMINATE/CRYPTO_CONSTRAINS_FAILURE_NO_POE, INDETERMINATE/REVOKED_NO_POE, INDETERMINATE/REVOKED_CA_NO_POE, INDETERMINATE/TRY_LATER nebo INDETERMINATE/OUT_OF_BOUNDS_NO_POE, lze pokračovat na ověřování razítek. Protože ale ověření formátu ZFO kvůli přítomnosti atributu PP (podpisová politika) skončí s indikací INDETERMINATE/POLICY_PROCESSING_ERROR a ověření S/MIME kvůli chybějícímu atributu SigningCertificate skončí s indikací INDETERMINATE/SIG_CONSTRAINTS_FAILURE, proces ověřování musí být ukončen.“

Článek 3 – Závěrečná ustanovení

1. Ostatní ustanovení Smlouvy nedotčená tímto Dodatkem, zůstávají v platnosti beze změn.

2. Smluvní strany prohlašují, že se seznámily s obsahem Dodatku a že tento Dodatek byl sepsán dle jejich pravé a svobodné vůle, nikoliv v tísni či za nápadně nevýhodných podmínek, na důkaz toho připojují své podpisy.

3. Tento Dodatek Smluvní strany uzavírají elektronicky.

4. Tento Dodatek nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti okamžikem zveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb., zákon o registru smluv, ve znění pozdějších předpisů, ve kterém jej zveřejní Objednatel.

……..	……
Česká republika - Ministerstvo financí	**První certifikační autorita, a.s.**
xxxxxxxxxx	Ing. Petr Budiš, Ph.D., MBA
xxxxxxxxxx	předseda představenstva
	……
	Ing. Roman Kučera
	člen představenstva

Za finální znění Dodatku:
xxxxxxxxxx