

DODATEK Č. 1 ke smlouvě

č. smlouvy **objednatele**: INO/40/05/001296/2007
jímž se mění čl. II., XVI., a doplňuje příloha č. 10 smlouvy

Inominátní smlouva, uzavřená mezi:

1. Hlavním městem Praha

se sídlem Mariánské nám.2, 110 01 Praha 1

IČ: 00064581, DIČ: CZ00064581

bankovní spojení: PPF banka, a.s., č. ú. 27-5157998/6000

zastoupené Ing. Václavem Krausem, ředitelem odboru informatiky Magistrátu hl.m. Prahy

(dále jen „**objednatel**“)

a

2. HAGUESS, a.s.

se sídlem: Na Michovkách I. 686, 252 43 Průhonice

IČ: 25085166

DIČ: CZ25085166

bankovní spojení: ČSOB, a.s., číslo účtu: 163486703/0300

zastoupená Miroslavou Turkovou, předsedkyní představenstva
(dále jen „**poskytovatel**“)

se v souladu s ustanovením čl. XVI. odst. 3 výše uvedené smlouvy mění takto:

I.

V čl. II. s názvem Předmět smlouvy

za odst.6 se text doplňuje takto:

„7. zajistit provoz OCSP serveru v rozsahu určeném přílohou č. 10“.

II.

V čl. XVI. s názvem Závěrečná ustanovení

v odst. 9 se text nahrazuje takto:

„Příloha 1 – Specifikace provozu Servisního Kartového Centra

Příloha 2 – Specifikace provozu kontaktního místa palác Adria

Příloha 3 – Specifikace provozu kontaktního místa ve Škodově paláci

Příloha 4 – Specifikace datového propojení kontaktních míst

Příloha 5 – Specifikace provozu webové prezentace

Příloha 6 – Specifikace svozu hotovosti a přípravy dokladů

Příloha 7 – Specifikace součinnosti

Příloha 8 – Specifikace monitoringu kvality služeb

Příloha 9 – Odstraňování vad

Příloha 10 – Specifikace provozu OCSP Serveru“

III.

Za přílohu č. 9 Smlouvy se doplňuje Příloha č. 10 Smlouvy takto:

Specifikace provozu OCSP serveru

I.

OCSP Server

1. OCSP server je technické řešení, které slouží k zajištění verifikace platnosti device certifikátu na kartě opencard, ve vazbě na centrální řešení SKC. Jeho detailní specifikace je uvedena v čl. IV této přílohy.
2. Objednatel tímto prohlašuje, že je oprávněným majitelem OCSK Serveru dle specifikace uvedené v čl. IV, a má právo jeho provoz zajistit prostřednictvím třetí osoby.
3. OCSP server bude umístěn ve stejných prostorách, jako Centrální pracoviště SKC.
4. Poskytovatel tímto prohlašuje, že je oprávněn užívat část nemovitosti, v níž se nachází centrální pracoviště v rozsahu určeném touto přílohou, na základě platného právního vztahu s majitelem, nájemcem nebo podnájemcem této nemovitosti.
5. Veškeré náklady spojené s pořízením, implementací OCSP serveru do centrálního pracoviště a jeho technickou podporou, hradí objednatel na svůj účet, stejně jako náklady na činnosti spojené s ukončením poskytování služeb dle Smlouvy, jejíž je tato příloha nedílnou součástí.
6. Provozní náklady spojené s provozem OCSP serveru hradí poskytovatel na svůj účet, a objednatel je povinen hradit pouze náklady ve výši určené smlouvou, jejíž je tato příloha nedílnou součástí.

II.

Implementace OCSP serveru

1. Objednatel zajistí činnosti spojené s implementací OCSP serveru do centrálního prostředí SKC, a o způsobu jejich zajištění bude poskytovatele včas a vhodným způsobem informovat.
2. Poskytovatel zajistí součinnost nutnou pro implementaci OCSP serveru do centrálního prostředí, tedy zejména umístění pro hardwarové prvky.
3. Poskytovatel není odpovědný za kvalitu a akceptaci implementace, a není povinen převzít OCSP server, pokud nesplňuje specifikaci uvedenou v čl. IV, a není jej možné provozovat.
4. OCSP server není součástí centrálního řešení SKC.

III.

Technická podpora OCSP serveru

1. Objednatel je povinen zajistit přímo nebo prostřednictvím třetích osob technickou podporu OCSP serveru, je poskytovateli povinen sdělit na jakých kontaktech, a jakým způsobem je technická podpora poskytována.
2. Poskytovatel není odpovědný za nefunkčnost systému způsobenou chybou systému nebo jakékoli jeho části, neposkytnutou nebo neodborně poskytnutou technickou podporou objednatelem nebo jím pověřené třetí osoby.
3. Poskytovatel je odpovědný za technický stav Centrálního řešení systému SKC, a zajištění poskytování datového rozhraní pro funkci OCSP serveru.
4. Poskytovatel nezajišťuje podporu smluvním stranám objednatele, které využívají služeb OCSP serveru, ani za podporu interním uživatelům OCSP serveru.

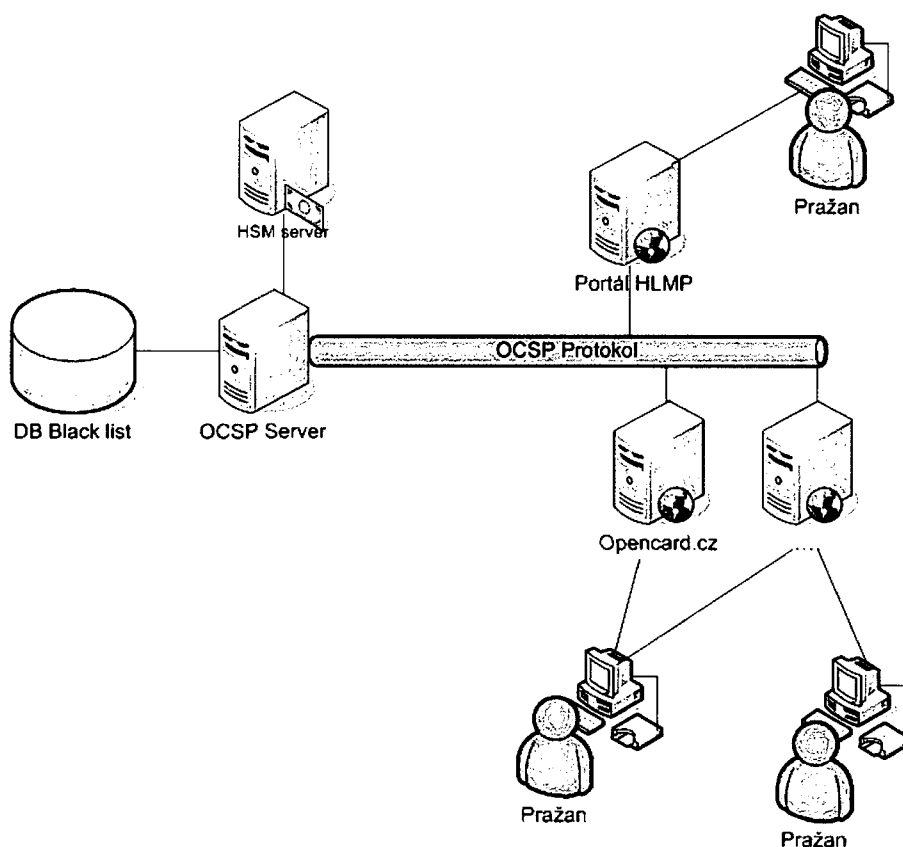
IV. Specifikace OCSP serveru

Na internetový portál Hlavního města Prahy a na informační web server opencard bude přístupováno prostřednictvím device certifikátu uloženého na čipové kartě. Přístup bude realizován prostřednictvím oboustranně šifrovaného protokolu HTTPS.

Tento postup vyžaduje ověření platnosti klientského certifikátu karty „opencard“ (certifikát C.509).

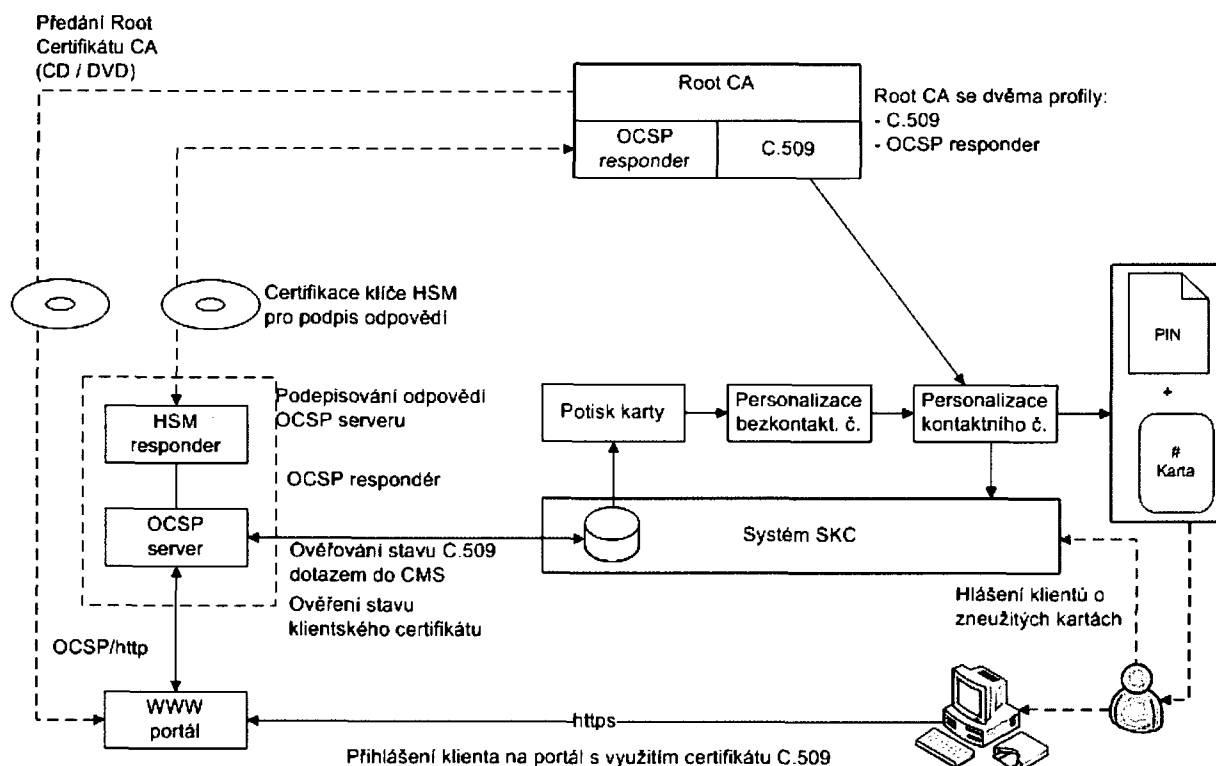
Platnost certifikátu (kromě standardních kryptografických a ověřovacích operací) bude ověřena on-line způsobem vůči serveru OCSP.

Web server se po kryptografickém ověření klientského certifikátu dotáže standardním protokolem serveru OCSP, zda je certifikát platný. OCSP server bude platnost certifikátu posuzovat na základě databázi (blacklistu) systému SKC.



Ověření platnosti certifikátu (karty) bude probíhat s využitím standardního protokolu OCSP (*Online Certificate Status Protocol*, OCSP je definovaného v RFC 2560).

OCSP je poměrně jednoduchý request- response protokol nabízející mechanismus pro on-line přenos informace o zneplatnění certifikátů (revocation status information) od důvěryhodné autority označované jako HSM respondér.



Východiska:

1. HSM respondér si vygeneruje pár klíčů a žádost o certifikát pro podepisování odpovědí OCSP serveru.
2. Root CA vystaví certifikát pro HSM respondér dle specifického profilu (nastaví ExtkeyUsage – id-kp-OCSPSigning, aby bylo možno vystavovat standardní ocsp odpovědi).
3. www portál bude mít k dispozici kořenový certifikát CA a tím umožní verifikovat jak klientské certifikáty C.509, tak také odpovědi HSM respondéru.
4. Klient (držitel certifikátu C.509) bude mít možnost vhodným kanálem nahlásit Card Management Systemu (CMS) ztrátu karty nebo možnou zneužitelnost karty a CMS zajistí její umístění na BlackList

Stručný popis funkčnosti:

1. Klient se přihlásí k www portálu s využitím čipové karty, kdy probíhá vzájemná autentizace
2. Server ověří klientský certifikát s využitím root certifikátu
3. Server se s využitím protokolu ocsp/http dotáže HSM respondéru na stav karty
4. OCSP server dotaz na stav přeneše na BlackList držený v DB Card Managementu
5. Získanou odpověď zapouzdří do odpovědi serveru a nechá si ji podepsat HSM respondérem.
6. Takto zkompleťovanou odpověď vrátí - prostřednictvím standardního OCSP protokolu - www portálu

V rámci implementace budou dodány následujících licence:

- Licence OCSP serveru (1ks)
- Licence HSM respondéru (1ks)

HSM respondér a OCSP budou dva fyzicky oddělené stroje. OCSP server bude umístěn v demilitarizované zóně provozovatele, HSM respondér bude uvnitř chráněného prostředí.

Uvedená implementace není určena pro režim HA s garantovanou dostupností 24/7.

Uvedený systém bude dodán včetně potřebné uživatelské a administrátorské dokumentace. Součástí dodávky je také implementace systému a testování kompatibility s portálem Hlavního města Prahy (www.praha.eu) a testování kompatibility se serverem www.opencard.cz.

Navržená technologie, s ohledem na kapacitní možnosti hardware, umožňuje připojení více internetových portálů pro ověření platnosti certifikátů.

Implementace OCSP bude provedena na následujícím hardware:

OCSP server:

HP ProLiant DL360G5

- Procesor: Dual – core Intel Xeon 5120 (1,86GHz)
- Memory: 1GB (2x 512MB) PC2- 5300 DDR2 667 SDRAM
- Network Cotroler: Embedded NC7782 Dual Port 10/100/1000T Gigabit network adapter
- Storage Cotroler: SMART ARRAY E200i (RAID 0,1)
- Remote Management: Integrated Ligts-Out (iLO) Standard Management (embedded)
- Power Supply One 460W (redundant power supply)
- 160GB 15.000rpm, U320 Universal Hot Plug Drive 2,5“ - 2ks
- HP DVD+R/RW 8x Slim
- Provedení – do racku

Použitý systémový software:

- Linux RH Enterprise 4

HSM respondér server:

- HP ProLiant ML310G4
 - Procesor: Dual – core Intel Xeon 3040 (1,86GHz 2MB L2)
 - Memory: 1GB (2x 512MB) Advanced ECC PC2- 5300 DDR2
 - Network Cotroler: Embedded NC320i PCI Express 10/100/1000T Gigabit network adapter
 - Storage Cotroler: Integrated four SATA controller with SATA RAID 0,1 2TB maximum (hot plug SATA)
 - 160GB SATA 1,5Gb 7.200rpm, Hard Drive - 2ks
 - HP DVD+R/RW 16x HSM modul SafeNet Gold CSA 8000 PL450
- Epson LQ300
- LCD monitor 17”, klávesnice, myš

Použitý systémový software:

- Linux RH Enterprise 4

“

IV.

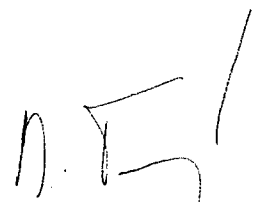
1. Ostatní ustanovení smlouvy zůstávají beze změny.

2. Dodatek nabývá účinnosti dnem podpisu oběma smluvními stranami.
3. Dodatek je sepsán ve čtyřech stejnopisech, z nichž tři obdrží objednatel a jeden poskytovatel.

V Praze dne 24.9.2007


.....
Za hlavní město Prahu


V Praze dne 24.9.2007


.....
Za Haguess, a.s.
HAGUESS, a.s.
Na Michovkách I.686
252 43 Průhonice
IČ: 25085166
DIČ: CZ25085166 3