

Výzva k poskytnutí informací v rámci průzkumu trhu

Zadavatel

Úřední název zadavatele:

ČESKÁ NÁRODNÍ BANKA

IČO: 48136450**Sídlo/místo podnikání:**

Na Příkopě 864/28

115 03 Praha 1

Kontaktní osoba:**Jméno:** Martin Hanuš**E-mail:** martin.hanus@cnb.cz

Specifikace PT

Název průzkumu trhu: Dodání kódu/frameworku na využití certifikátu uloženého na čipové kartě**Systémové číslo průzkumu trhu:** T002/17/P00055035**Dne**

10.11.2017 14:10:00

[detail PT](#)

Text oznámení

Jménem zadavatele Vás vyzývám k poskytnutí informací v rámci průzkumu trhu dle požadavků stanovených v této výzvě.

Předmět průzkumu trhu

Popis

V současné době provozuje ČNB interně vyvíjený systém v C++ ve třívrstvé architektuře. Spolu se vstupními daty odesílá klient na server také hash, který je zašifrován privátním klíčem uživatele pomocí funkce OpenSSL: RSA_private_encrypt. Certifikát uživatele včetně privátního klíče je uložen na lokálním disku klientské stanice. Na serveru jsou uloženy veřejné klíče všech uživatelů. Server nad přijatými daty spočítá vlastní hash, který poté porovná s přijatým hashem klienta, dešifrováním pomocí veřejného klíče uživatele funkcí OpenSSL:

RSA_private_decrypt .

Tlustý klient běží na platformě Windows 7(10) a Linux Redhat 7, server běží na platformě Linux Redhat 7.

Ke každé klientské stanici je připojena čtečka, vyhovující standardu PC/SC (např. HID Omnikey 3121). Uživatelé používají čipové karty firmy SafeNet (nově po spojení Gemalto) - Smart Card model 330u, 400, 4100. Nyní se testuje další typ Gemalto MD840B. Nainstalovaná podpora karet pochází od stejné společnosti a jedná se o SW Gemalto/SafeNet Authentication Client verze 10.3.25.

Cílem je upravit výše zmíněnou aplikaci tak, aby klientské certifikáty byly uloženy na některé z uvedených karet, přičemž privátní klíč uložený na kartě je označen jako neexportovatelný a je přístupný pouze pomocí služeb karty.

Požadujeme dodání vhodného řešení, které zajistí uvedený cíl.

Součástí dodávky bude zejména

- Framework s rozhraním v C++, který zajistí:

- o komunikaci s výše uvedenými typy karet
- o Identifikaci konkrétního certifikátu na kartě
- o Zašifrování nebo podpis dat na základě zvoleného certifikátu
- o Reakce na vydání karty ze čtečky, chyby čtení, apod.
- Dokumentovaný příklad konkrétního použití dodaného frameworku pro zamýšlený cíl
- Dokumentovaný příklad dešifrování na serverové straně, za předpokladu, že jej bude nutno modifikovat
- Konzultace při aplikaci úprav v systému ČNB na základě dodaných příkladů

Omezující podmínky:

Preferujeme multiplatformní řešení na open source nebo komerční bázi. Zásadní je řešení pro platformu Windows 7(10), na které budou probíhat akceptační testy. Testování funkcionality pro ostatní platformy nebude součástí dodávky.

Položky předmětu PT

Název	Balík programů určený pro specifické odvětví		
Kód z číselníku NIPEZ	48100000-9 - Balík programů určený pro specifické odvětví		
Kód z hlavního slovníku číselníku CPV	48100000-9 - Balík programů určený pro specifické odvětví		
Popis			
Přílohy			
Parametry			
Parametry	Název	Operátor	Hodnota
Identifikace			
Množství			
Měrná jednotka			

Dělení na části

- ☒ Ne
☐ Ano

Požadavek na obsah informace poskytnuté dodavatelem

Povinnost elektronicky podepisovat datové zprávy

- ☒ Ne
☐ Ano

Požadavek na obsah informace poskytnuté dodavatelem

Jiné požadavky

Po dodavatelích požadovat

zaslat přílohu, příp. informaci vložit do textového pole

Informace, které mají dodavatelé předkládat

Měna, ve které má být cena uvedena

Jiné požadavky

Prosíme o uvedení hrubého cenového odhadu v Kč a stručného popisu návrhu řešení

Příme zadání hodnot

Žádná položka nebyla nalezena.

Lhůta pro doručení odpovědi zadavateli

Datum a čas

30.11.2017 10:00:00

Do kdy jsou dodavatelé vázáni nabídnutými hodnotami

Datum

31.12.2017

Vytvořil

Jméno a příjmení

Martin Hanuš v.r.

Doručení

Datum

10.11.2017 14:46:10