**Odpoveď na žiadosť záujemcu o vysvetlenie informácií potrebných**

**na vypracovanie ponuky**
V súvislosti s výzvou na predloženie ponuky k zákazke s nízkou hodnotou podľa § 117 zákona č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“) na predmet zákazky **Bezpečnostné testovanie IS CID** bola verejnému obstarávateľovi dňa 11.04.2019 doručená žiadosť záujemcu o vysvetlenie informácií potrebných

na vypracovanie ponuky.

Verejný obstarávateľ, v súlade so zákonom o verejnom obstarávaní a s bodom 13.5. výzvy na predloženie ponuky poskytuje nižšie uvedené vysvetlenie všetkým záujemcom.

**Otázka č. 1:**

S ohľadom na stanovený termín dodávky Fázy A od 6.5.2019 do 7.6.2019, kedy bude uchádzač informovaný o úspechu resp. neúspechu ponuky?

**Odpoveď na otázku č. 1:**

Verejný obstarávateľ bez zbytočného odkladu po vyhodnotení predložených ponúk zašle uchádzačom informáciu o výsledku vyhodnotenia ponúk.

**Otázka č. 2:**

Prosíme o stručný popis na čo IS CID slúži, aby sme získali predstavu o funkcionalite, ktorú budeme testovať.

**Odpoveď na otázku č. 2:**

IS CID slúži na správu identifikátorov príjemcov inkás (Creditor Identifier – CID). Bližšie informácie o CID sú k dispozícii na stránke <https://www.nbs.sk/sk/platobne-systemy/sepa/identifikator-prijemcu>**.**

Ďalej nasledujú otázky k jednotlivým bodom zo zadania:

**Otázka č. 3:**

*2.1.3 obmedzený počet externých používateľov (pracovníci v bankách v SR)*Je medzi interným a externým používateľom rozdiel? Prihlasujú sa inak?

**Odpoveď na otázku č. 3:**

Proces prihlásenia externých aj interných používateľov je identický. Majú však rôzne prístupové role (teda sú rôzne činnosti, ktoré môžu vykonávať v IS CID).

**Otázka č. 4:**

*2.1.6 Dvojfaktorová autentifikácia (heslo, používateľský certifikát v TLS)***a)** Ako presne prebieha autentifikácia certifikátom?
**b)** Kde sa certifikát ukladá?
**c)** Koľko certifikátov bude k dispozícii pre naše testovanie?

**Odpoveď na otázku č. 4:**

1. Štandardná klientska autentizácia v TLS protokole, sprostredkovaná webovým prehliadačom používateľa.
2. V závislosti na použitej forme buď čipová karta alebo SW certifikát uložený v úložisku certifikátov OS/web prehliadača. Verejná časť certifikátu uložená v DB IS CID.
3. Štandardne predpokladáme 2 používateľské účty (aj s certifikátmi) pre každú rolu. V prípade potreby nie je problém vytvoriť aj dodatočné.

**Otázka č. 5:**
*2.1.7 Hlavné funkčné moduly (v zátvorke je uvedený približný počet stránok...*
Aj napriek tomu, že uvádzate počet stránok, pre správne nadimenzovanie testu je pre nás potrebné poznať počet vstupov ktoré formuláre obsahujú.

Môžete nám to uviesť v celkovom počte, prípadne priemerný počet vstupov na stránku.

**Odpoveď na otázku č. 5:**

Priemerný počet vstupov na stránke je 5-7.

**Otázka č. 6:**

*2.1.8 Overenie/získanie informácií v externej aplikácii prostredníctvom web services*Zo zadanie sme pochopili, že ide o ďalšie aplikácie mimo testovaného webu. Budú tieto aplikácie tiež predmetom testu? Ak áno aký je ich rozsah?

**Odpoveď na otázku č. 6:**

Testovanie externých aplikácií nie je predmetom tejto zákazky. V tomto prípade ide len o overenie/získavanie informácií z externej aplikácie.

**Otázka č. 7:**

*2.3.1 ... posúdenie implementovaných bezpečnostných riešení pre naplnenie bezpečnostných cieľov v oblastiach:*
- ...
- Dôvernosť a autentickosť údajov / dokumentov
- správa hesiel
- správa kľúčov a certifikátov

**a)** Ako / podľa čoho sa bude hodnotiť dôvernosť dokumentov, správa hesiel, kľúčov a certifikátov?
**b)** Budú tieto údaje skúmané na strane klienta alebo na strane serveru?
- Ak to bude na strane klienta, potrebujeme poznať popis použitých technológii pre jednotlivé body uvedené vyššie.

- Ak  sa jedná o stranu serveru, budeme na to potrebovať prístup na server.

**Odpoveď na otázku č. 7:**

1. Hodnotenie očakávame podľa OWASP Testing Guide v4 (ako je uvedené v bode 2.3.2), resp. relevantných „best-practice“ pre tie oblasti, ktoré nie sú OWASP Testing Guide pokryté.

Ad. „dôvernosť dokumentov“ – očakávame posúdenie toho, či používatelia (danej role) majú prístup len k príslušným informáciám, nie k dátam, ku ktorým by nemali mať prístup.

1. Domnievame sa, že vymenovanie technológií vo výzve je postačujúce na nacenenie prác uchádzača. Dodatočné technické informácie budú poskytnuté úspešnému uchádzačovi pred a počas realizácie projektu.

**Otázka č. 8:**

*2.3.2 testovanie útokov typu Denial of Service: vykonanie aplikačných DoS (kde spracovanie vstupov v aplikácii má neželaný vplyv na dostupnosť aplikácie/systému), aj záťažových testov (veľký počet spojení, dotazov a pod.)*

Aplikačný DoS vykonávame štandardne, v rámci testu webovej aplikácie.

V prípade záujmu vykonania DoS  – dokážete nám dodať parametre záťažového testu (počet simultánnych pripojení, dotazov a pod.) ?

**Odpoveď na otázku č. 8:**

Konkrétne parametre DoS budú dohodnuté počas realizácie projektu**.**

**Otázka č. 9:**

*2.3.2 testovanie pokryje všetky funkcie aplikácie*
Koľko funkcií má testovaná webová aplikácia?

**Odpoveď na otázku č. 9:**

Hlavné funkčné moduly, vrátane orientačného počtu stránok sú uvedené v bode 2.1.7.

**Otázka č. 10:**

*2.3.2 testovanie bude vykonané z pohľadu účastníka aj z pohľadu prevádzkovateľa systému*
Ako sa líšia tieto dve role?
Sú tieto dve používateľské role súčasťou udávaných 6 rolí, ktoré aplikácia obsahuje?

**Odpoveď na otázku č. 10:**

V počte 6 sú zahrnuté všetky role v IS CID (aj z pohľadu účastníka, aj z pohľadu prevádzkovateľa).

**Otázka č. 11:**

*2.3.2 bezpečnostný audit konfigurácie vybraných softvérových komponentov servera (Apache, Tomcat)*
Prosím o uvedenie čísla verzií použitých komponentov.

**Odpoveď na otázku č. 11:**

Domnievame sa, že vymenovanie technológií vo výzve je postačujúce na nacenenie prác uchádzača. Dodatočné technické informácie budú poskytnuté úspešnému uchádzačovi pred a počas realizácie projektu.