Zadavatel: Město Chropyně, IČ: 00287245
náměstí Svobody 29, 768 11 Chropyně
Zastoupený: Ing. Věra Sigmundová, starostka města
Tel.: 573 500 73, e-mail: sigmundova@muchropyne.cz

Vysvětlení zadávacích podmínek č. 1

Zadavatel na základě dotazů zájemce poskytuje toto vysvětlení zadávacích podmínek č. 1 k veřejné zakázce malého rozsahu na dodávky s názvem: „**Schránka pro oznamovatele**“.

Dotaz č. 1:

Napojení bezpečné komunikace na portál města jako schránky pro oznamovatele. Potřebovali bychom více specifikovat napojení na portál města. Jde o zpřístupnění odkazu, abyste si ho mohli vložit na portál, o modifikaci stránky z naši strany (integraci formulářů a kryptografické ochrany - pokud ano, potřebujeme znát technologie v kterých je nutné při napojení pracovat)

Odpověď č. 1:

Jedná se o propojení odkazem.

Dotaz č. 2:

Je potřeba integrovat aplikaci Schránka pro oznamovatele s jiným SW řešením co používate?

Odpověď č. 2:

Další propojení nepožadujeme.

Dotaz č. 3:

Systém umožňuje odeslání elektronických dokumentů, které jsou také zašifrovány před jejich odesláním pomocí privátního klíče bez omezení velikostí příloh. Lze předpokládat přílohy jako videa a skenované doklady. Tady nastává problém s anonymitou oznamovatele při použití jeho privátního klíče a současně při použití privátního klíče oznamovatele může číst informaci (ať už soubor nebo text) kdokoliv - to je přesně proti požadavku "Zprávu může přečíst pouze zvolený příjemce."

Odpověď č. 3:

Šifruje se veřejným klíčem příjemce. Privátním klíčem příjemce dešifruje obsah. Děkujeme za upozornění na nechtěnou záměnu pojmů. Měníme tedy požadavek „pomocí privátního klíče„ na „pomocí veřejného klíče“.

Dotaz č. 4:

Dále šifrování privátním klíčem před odesláním dat je na principu elektronického podpisu

Odpověď č. 4:

Viz předchozí odpověď.

Dotaz č. 5:

Dále asymetrická kryptografie je silně nevhodná pro šifrování velkých objemu dat - jako jsou různé multimediální soubory. Privátní i veřejný klíč je N-tice náhodně zvolených vysokých čísel v

komplikovaném matematickém vztahu a pokud šifrovaná zpráva je bitove větší než klíč pro šifrování, tak se stává šifrování nemožné - následek to má takový, že by se musel přegenerovat pár klíčů a přešifrovat veškerý obsah. A velikost klíče pro případné 4K video trvající třeba 10 minut si radši ani nechci představovat.

Odpověď č. 5:

Zadavatel nemůže předepisovat technické řešení. Je tedy na uchazeči, jak se vypořádá s tímto požadavkem a najde vhodné technické řešení problému.

Dotaz č. 6:

Řešení, které splní požadavak pro anonymitu oznamovatele, možnost čtení jen pro zvoleného příjemce a možnost přenosu neomezeně velkých souboru a zajištění jejich integrity pře přenosu je následující: Oznamovatel šifruje zprávu veřejným klíčem příjemce. Jediný kdo může zprávu číst je majitel privátního klíče (tedy příjemce). Soubory jsou šifrované symetrickou šifrou, která produkuje klíč, vektor a kontrolní součet pro zajištění interity. Tyto výstupy (klíč, vektor a kontrolní součet) jsou šifrovány opět veřejným klíčem příjemce a jediný, kdo je může číst je opět jen majitel privátního klíče (tedy příjemce). Timto by měli být splněny podmínky na anonymitu oznamovatele i nemožnost číst nebo podvrhnout přenášená data neoprávněnou osobou. Jde o princi používány u TLS, SSL a HTTPS komunikace.

Odpověď č. 6:

Viz předchozí odpovědi.

Dotaz č. 7:

Otázka k tomuto bude na základe skutečností popsaných výše - požadavek na privátní klič při odesílání dat - jde o chybu v zadávací dokumentaci, která se tam dostala z neznalosti kryptografických principů? Je námi navrhované řešení na bezpečný přenos souborů akceptovatelné z pohledu zadavatele?

Odpověď č. 7:

Viz předchozí odpovědi. Technické řešení by takto bylo v pořádku.

Dotaz č. 8:

Ochrana identity odesílatele a příjemce podle volby uživatele, kdy lze zvolit skutečně anonymní odesílání zprávy. Za odeslání anonymní zprávy se nepovažuje použití pseudonymu. Tento bod potřebujeme dovysvětlit. Jak má vypadat odeslání zprávy ze strany oznamovatele, v zadání píšete "Zprávu může přečíst pouze zvolený příjemce" - předpokládal jsem, že příjemce vybírá jmenovitě ze skupiny úředníků, kteří v systému mají účty (z důvodu použití konkrétního veřejného klíče pro zajištění, že se k datům dostane jenom určený čtenář). Při použití privátního klíče oznamovatel tuto anonymitu může snadno ztratit - viz bod výše o elektronickém podpisu

Odpověď č. 8:

Vysvětlení viz předchozí odpovědi.

Dotaz č. 9:

Jaké jiné než skutečně anonymní odesílání zprávy má jít v sytému zvolit a jaké má být následně chování systému?

Odpověď č. 9:
Lze zvolit jak anonymní, tak neanonymní, kdy lze na zprávu odpovědět.

Dotaz č. 10:
Zprávy uložené na serveru jsou zašifrovány za použití privátního a veřejného klíče klienta. Je nutné zvolit model symetrické šifry pro soubory a asymetrické (s privátním a veřejným klíčem) pro šifrování dat potřebných pro přistup k souborům (klíč, vektor, kontrolní součet) - jinak vzniká problém s přegenerováním klíčů - viz popsáno výše
Odpověď č. 10:
Vysvětlení viz předchozí odpovědi.

Dotaz č. 11:
Na doručené zprávy loze odpovědět podobně jako na mail (RE a FW). Má být šifrování při odpovědi oznamovateli taky šifrované tak aby ho mohl číst pouze oznamovatel? Pokud má být šifrovaná komunikace i k oznamovateli, je potřeba aby si oznamovatel uchoval privátní klíč pro možnost čtení zpráv. Tady jeho anonymita není porušena, protože veřejný klíč je nic neříkající a slouží k uveřejnění. Nastává problém, když oznamovatel svůj privátní klíč ztratí.
Odpověď č. 11:
Ano. Šifrování probíhá na klientské stanici.

Dotaz č. 12:
Přeposlání předpokládám pouze v rámci uživatelů interně v aplikaci Schránka pro oznamovatele, můžete to prosím potvrdit?
Odpověď č. 12:
Ano.

Dotaz č. 13:
Rozhraní má responsivní design. Máte už grafické podklady nebo vyhotovení grafického návrhu aplikace je součástí zakázky?
Odpověď č. 13:
Grafický návrh bude součástí aplikace.

Dotaz č. 14:
Pokud máme vyhotovit i grafické návrhy, jaké jsou z Vaší strany požadavky na design?
Odpověď č. 14:
Design bude vycházet z vizuálu města – viz webové stránky.

Dotaz č. 15:
Obsahuje českou a anglickou jazykovou mutaci podle preferencí uživatele. Předpokládám, že zajištění překladu Vámi dodaných českých textů je na nás jako na zhotoviteli, můžete prosím potvrdit?

Odpověď č. 15:
Zadavatel takovou textaci z logiky věci mít nemůže, protože nepožaduje konkrétní produkt. Zadavatel nebude dodávat textace, ale předpokládá lokalizaci aplikace do cizího jazyka od uchazeče.

Dotaz č. 16:
Dotaz k technickým omezení: Jsou nějaké omezení na provoz budoucí aplikace? Využíváme technologický stack, kdy serverová část běží v dockeru (využívá se Java). Webová část by za nás byla napsaná v Angularu. Otázka tedy zní, na jakém serveru - jaký HW a jaký operační systém - poběží výsledný produkt?
Odpověď č. 16:
Zadavatel předpokládá provoz na svých HW prostředcích, u klientské aplikace předpokládáme pouze prohlížeč bez nutnosti cokoliv instalovat. K dispozici jsou technologie Microsoft ve verzi windows 2012 nebo vyšší, Microsoft SQL server.

Z výše uvedených důvodů prodlužuje zadavatel lhůtu pro podání nabídek do 28. 2. 2022 do 14:00 hodin

Ostatní ustanovení zadávacích podmínek zůstávají beze změny.

V Chropyni, dne 16. 2. 2022

Ing. Věra Sigmundová – starostka města