

Príloha č. 1

Opis predmetu zákazky

VEREJNÝ OBSTARÁVATEĽ:

Národná agentúra pre sieťové a elektronické služby

NÁZOV ZÁKAZKY:

„Klientské aplikácie pre vytváranie kvalifikovaného elektronického podpisu“

TRVANIE:

Lehota dodania je 1 mesiac.

KOMPLEXNOSŤ:

Uchádzač je povinný predložiť ponuku na celý predmet zákazky, vrátane všetkých súvisiacich nákladov a licencií.

ŠPECIFIKÁCIA ZÁKAZKY:

Ústredný portál verejnej správy (ďalej aj ako „ÚPVS“) zabezpečuje centrálny a jednotný prístup k informáciám a službám verejnej správy. Správcom ÚPVS je v zmysle § 6 zákona č. 305/2013 Z. z. o elektronickom podaní a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov (ďalej aj ako „zákon o e-Governmente“) Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj ako „MIRRI SR“). Prevádzkovateľom ÚPVS je Národná agentúra pre sieťové a elektronické služby (ďalej aj ako „NASES“), ktorá na základe svojho štatútu a zriaďovacej listiny plní úlohy vyplývajúce z § 10 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a zo zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

V rámci balíka komponentov „Klientských aplikácií pre vytváranie kvalifikovaného elektronického podpisu“ (ďalej len D.Suite/eIDAS), ktorá je k dispozícii občanom na ÚPVS kde sa realizujú aktualizácie len v nevyhnutnom rozsahu. Vzhľadom na potreby nových funkcionalít ako je uvedené vo funkčných požiadavkách, je potrebný nákup aktuálnej klientskej aplikácie pre vytváranie kvalifikovaných elektronických podpisov. Aplikácia D.Signer/XAdES, ktorá je určená na vytváranie a spracovanie kvalifikovaného elektronického podpisu (KEP, resp. pôvodne v súlade so zákonom č. 215/2002 Z. z. o elektronickom podpise – zaručeného elektronického podpisu, ZEP), ktorý slúži na autorizáciu elektronických podaní a elektronických úradných dokumentov podľa zákona č. 305/2013 Z.z. o e-Governmente a v súlade s

nariadením Európskeho Parlamentu a Rady EÚ č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES. Aplikácia určená na vytváranie KEP je v zhode a spĺňa relevantné bezpečnostné, funkčné a obsahové požiadavky na aplikácie pre vytváranie elektronického podpisu, ktoré sa nachádzajú v dokumente CEN CWA 14170, v zákone č. 272/2016 Z. z. o dôveryhodných službách a príslušných vyhláškach NBÚ SR pre oblasť kvalifikovaného elektronického podpisu.

Aplikácia D.Signer/XAdES využíva pri vytváraní KEP kvalifikované zariadenie pre vyhotovovanie elektronického podpisu (QSCD – Qualified Signature Creation Device), napr. občiansky preukaz s čipom (eID karta), čipová karta Starcos a pod.

Produkt „Klientské aplikácie pre vytváranie kvalifikovaného elektronického podpisu“ D.Suite/eIDAS je detailne popísaný na webovej stránke [D.Suite/eIDAS - Klientské aplikácie pre kvalifikovaný elektronický podpis | Ditec](#)

ŠPECIFIKÁCIA PREDMETU ZÁKAZKY

Predmetom zákazky je nákup „Klientských aplikácií pre vytváranie kvalifikovaného elektronického podpisu“ používaný najmä v rámci procesov autorizácie komponentmi ÚPVS v rámci elektronickej komunikácie so štátom v rámci UPVS, vrátane základných inštalčných a konfiguračných prác pre dve (produkčné a testovacie) prevádzkové prostredia NASES v zmysle tohto Opisu predmetu zákazky.

Výstupom z verejného obstarávania bude Kúpna zmluva.

Predmetom dodania je:

- 1) „Klientské aplikácie pre vytváranie kvalifikovaného elektronického podpisu“
- 2) Základná inštalácia a konfigurácia do dvoch prostredí ÚPVS vrátane dokumentácie

Verejný obstarávateľ požaduje licencie a služby uvedené v bodoch 1 a 2 dodat' v súlade s funkčnými a nefunkčnými požiadavkami, v rozsahu, podľa podmienok a pri zachovaní požadovaných technických, bezpečnostných a iných vlastností produktu, podľa tohto opisu predmetu zákazky.

Súčasťou predmetu zákazky **nie je** dodanie:

- hardvéru (prevádzkovú hardvérovú infraštruktúru poskytne verejný obstarávateľ),
- nástroja na zber logov,
- služby monitorovania a reportingu infraštruktúry a prevádzky

Dotknutí biznis aktéri a ich role:

- FO, FO podnikatelia, PO,
- Orgány verejnej moci,
- Národná agentúra pre sieťové a elektronické služby,

ŠPECIFIKÁCIA FUNKČNÝCH, NEFUNKČNÝCH A TECHNICKÝCH POŽIADAVIEK

Funkčné, nefunkčné a technické požiadavky sú:

1. Podpora vytvárania (kvalifikovaného) elektronického podpisu pomocou nových kryptografických algoritmov (eliptické krivky – ECDSA, RSA-PSS, RSA-MGF1, DSA, SHA3, ...) v súlade s platnou podpisovou politikou NBÚ SR pre KEP (QES) a technickými možnosťami príslušných rozhraní (knižníc) PKCS#11, PKCS#12, MS CAPI, MS CNG.
2. Možnosť vyvolania procesu vytvorenia (kvalifikovaného) elektronického podpisu pomocou mobilu ako čítačky eID kariet cez NFC rozhranie; vytvorenie spojenia medzi aplikáciou D.Signer a mobilnou aplikáciou DISIG Web Signer Mobile cez QR kód.
3. Nové moderné GUI KEP komponentov D.Signer a D.Viewer implementované pomocou knižníc WPF (pre .NET platformu) a JavaFX (pre Java platformu) a zohľadňujúce požiadavky dizajn manuálu ID-SK.
4. Podpora HiDPI monitorov.
5. Vylepšené UX komponentu D.Signer navrhnuté na základe výsledkov formatívneho UX testovania a s ohľadom na UCD (User-centered Design):
 - Zapamätanie si platformy zvolenej používateľom (.NET resp. Java) pri spustení komponentu D.Signer z web stránky portálu
 - Zapamätanie si posledných troch zvolených podpisových certifikátov
 - Upozornenie používateľa na blížiacu sa expiráciu (koniec) platnosti podpisového certifikátu
 - Upozornenie používateľa, ak sa na zvolenom QSCD zariadení nenachádzajú žiadne podpisové certifikáty
 - Dashboard menu s konfiguračnými nastaveniami komponentu D.Signer
 - Vylepšená konfigurácia poskytovateľov kryptografických služieb (pre výber podpisového certifikátu)
 - Zapamätanie si poslednej veľkosti okna.
6. Možnosť pridať v komponente D.Signer do štruktúry podpisu vo formáte XAdES element IndividualDataObjectTimestamp v súlade so zákonom č. 305/2013 Z.z. o eGov, § 23, odsek 1, písmeno b) (pozn. pridanie kvalifikovanej elektronickej časovej pečiatky, ktorá určuje dátum a čas, po ktorom nastala autorizácia).
7. Vylepšené UX komponentu D.Viewer navrhnuté s ohľadom na UCD (User-centered Design)
 - Nové intuitívne GUI s dôrazom na prezentáciu podpísaných elektronických dokumentov, a až následne informácií o podpisových kontajneroch a pripojených elektronických podpisoch

- Integrácia na službu overenia platnosti podpisov portálu ePodpis.ditec.sk
 - Integrácia na službu portálu ePodpis.ditec.sk pre získanie vizualizácií ľubovoľného e-formulára, ktorý je registrovaný v module MEF ÚPVS
 - Dashboard menu s konfiguračnými nastaveniami komponentu D.Viewer
 - Zapamätanie si poslednej veľkosti okna
 - V rámci informácií o elektronickom podpise pridané vyhodnocovanie typu podpisového certifikátu a zobrazenie legislatívneho typu podpisu.
8. Podpora zobrazenia informácií z elementov IndividualDataObjectTimestamp, AllDataObjectsTimestamp v podpise vo formáte XAdES a informácií z atribútu content-time-stamp v podpise vo formáte CAdES v komponente D.Viewer v súlade so zákonom č. 305/2013 Z.z. o eGov, § 23, odsek 1, písmeno b) (pozn. zobrazenie kvalifikovanej elektronickej časovej pečiatky, ktorá určuje dátum a čas, po ktorom nastala autorizácia)
9. Zapracovanie súladu s aktuálnym znením prílohy č. 8 vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov v komponente D.Viewer (podpora prípony .xdcf pre XMLDataContainer)
10. Podpora zobrazenia samostatných dátových objektov povinných formátov pre podpisovanie podľa vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov – § 46, odsek 2, písmená a) – c)

V rámci technického návrhu riešenia je zhotoviteľ povinný dodržať technologické a dátové princípy definované rámcovými dokumentami MIRRI SR (NKIVS a pod.) a príslušnou legislatívou (štandardy a pod.).

Výstupy/dokumenty v jednotlivých aktivitách/etapách projektu musia byť vytvorené a dodané v súlade s:

- Vyhláškou č. 401/2023 MIRRI SR o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy,
- Súčasťou dodania bude prevádzková dokumentácia minimálne v rozsahu:
 - Inštalčná a konfiguračná príručka
 - Príručka administrátora
 - Používateľská príručka
 - Licenčná a právna dokumentácia
 - DGR plány vrátane zálohovania
 - Testovacie akceptačné scenáre pre overenie funkcionality nainštalovaného a nakonfigurovaného produktu

ŠPECIFIKÁCIA LEGISLATÍVNYCH POŽIADAVIEK

Produkt musí byť najmä v súlade s nasledujúcimi Legislatívnymi požiadavkami:

- 1) Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov,

- 2) Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov (predovšetkým príloha č. 1),
- 3) Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- 4) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28. 8. 2014),
- 5) Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy, Úrad podpredsedu vlády SR pre investície a informatizáciu, v. z. n. p.
- 6) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti,
- 7) Vyhláška č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- 8) Vyhláška č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- 9) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR) a v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- 10) Vykonávacie rozhodnutie Komisie EÚ č. 2015/1506, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Text s významom pre EHP)
- 11) Zákon 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- 12) Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu (zverejnená na webovom sídle NBÚ)
- 13) Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 385/2022 Z.z. o jednotnom formáte elektronickej správy a elektronickej doručky

POŽIADAVKY NA SÚČINNOSŤ A SLUŽBY

Dodávateľ je povinný zabezpečiť, v súčinnosti so zamestnancami prevádzky verejného

obstarávateľa, inštaláciu a konfiguráciu dodaného riešenia v testovacom a produkčnom prostredí verejného obstarávateľa. Verejný obstarávateľ zabezpečí pripravenosť prostredí podľa vzájomne odsúhlasenej, odporúčanej špecifikácie na infraštruktúru.

HARMONOGRAM REALIZÁCIE ZÁKAZKY

V rámci dodania zákazky bude dodávateľom definovaný termín akceptácie inštalácie a konfigurácie produktu v predprodukčnom prostredí NASES a následne termín inštalácie do produkčného prostredia v zmysle lehoty trvania do jedného mesiaca od nadobudnutia právoplatnosti zmluvy.

NÁVRH ROZPOČTU PRI DODANÍ ZÁKAZKY

Návrh rozpočtu sa nachádza v Prílohe č. 2 „Štruktúrovaný rozpočet - „Klientské aplikácie pre vytváranie kvalifikovaného elektronického podpisu“, ktorá je neoddeliteľnou súčasťou tohto dokumentu.

ZOZNAM SKRATIEK A POJMOV

Tabuľka č. 1 - Zoznam skratiek

SKRATKA	POPIS
API GW	API Gateway, integračná zbernica definovaná v strategickej prioritě Integrácia a orchestrácia
API	Aplikačné programové rozhranie
DSA	Algoritmus digitálneho podpisu, často používaný v USA.
ECDSA	Algoritmus digitálneho podpisu využívajúci eliptické krivky.
eID	Elektronický identifikačný doklad
FO	Fyzická osoba
GDPR	General Data Protection Regulation; Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
GUI	Grafické používateľské rozhranie (Graphical user interface)
ID-SK	Jednotný design manuál elektronických služieb
KEP	Kvalifikovaný elektronický podpis
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
MS CAPI	Rozhranie API pre kryptografické operácie vo Windows.
MS CNG	Moderné API pre kryptografiu na platforme Windows.
NASES	Národná agentúra pre sieťové a elektronické služby
NKIVS	Národná koncepcia informatizácie verejnej správy
OVM	Orgán verejnej moci - štátny orgán, orgán územnej samosprávy, verejnoprávna inštitúcia, orgán záujmovej samosprávy a fyzická osoba alebo právnická osoba, ktorým zákon zveril výkon verejnej moci
PDF	Portable Document Format - dokumentový formát
PKCS#11/12	Štandard pre prístup k hardvérovým kryptografickým tokenom (napr. čipové karty).
PO	Právnická osoba
PROD	Produkčné prostredie
QES	Qualified Electronic Signature – Anglický ekvivalent pre KEP.
QSCD	Kvalifikované zariadenie na vytváranie elektronických podpisov
NFC	bezdrôtová technológia umožňujúca rýchlu a zabezpečenú výmenu dát
RSA-MGF1	Funkcia na generovanie masky, používaná ako súčasť podpisových schém RSA.
RSA-PSS	Bezpečný podpisový schéma na báze RSA, odporúčaný pre moderné aplikácie.
SHA3	Kryptografická hašovacia funkcia, ktorá generuje pevne veľké výstupy (napr. 256 bitov).
Sk-Talk	Štandard pre asynchrónnu komunikáciu prostredníctvom ÚPVS
UAT (FIX)	Testovacie prostredie

UX	Užívateľská skúsenosť
ÚPVS	Ústredný portál verejnej správy, ústredný portál

Tabuľka č. 2 – Zoznam pojmov

POJEM	POPIS
Admin GUI	Rozhranie pre správu a konfiguráciu aplikácií, spravidla pre rolu Administrátor (Admin).
API First	Prístup, ktorý určuje spôsob návrhu a vývoja aplikačného softvéru, tak aby API vznikalo ešte pred samotnou implementáciou.
Biznis proces, proces	Postupnosť krokov, činností alebo aktivít, predstavujú vykonávanie činnosti v organizácii alebo v systéme. Skrátene sa tiež označuje aj ako proces.
CI/CD pipeline	Automatizovaný proces používaný vo vývoji softvéru na zefektívnenie integrácie kódu, testovania a nasadzovania nových verzií aplikácií. CI/CD pipeline umožňuje časté a spoľahlivé nasadenie zmien kódu do produkčných prostredí, čím sa zlepšuje kvalita softvéru a skracuje čas potrebný na dodanie nových funkcií.
Dokumentácia k centrálnym modulom ÚPVS	Electronical Government, elektronizácia verejnej správy
eGOV, e-Government	Electronical Government, elektronizácia verejnej správy
GitLab	GitLab je webový nástroj pre kompletný vývojový cyklus software. Poskytuje gitový repozitár, wiki, sledovanie chýb, kontinuálnu integráciu (CI/CD), vytváranie skupín, tvorbu statických webových stránok či management projektu. Umožňuje vývojovým, prevádzkovým a bezpečnostným tímom navrhovať a spravovať softvér pomocou jediného nástroja.
Pravidlá publikovania elektronických služieb	Pravidlá publikovania elektronických služieb do multikanálového prostredia verejnej správy https://mirri.gov.sk/wp-content/uploads/2018/10/Pravidla_Publikovania_Sluzieb_v1_0-1.pdf
Representational State Transfer (REST)	Protokol sieťovej komunikácie pri poskytovaní elektronických služieb potrebných na spracovanie elektronických podaní alebo úspešné vyplnenie a prípravu elektronického podania prostredníctvom modulu procesnej integrácie a integrácie údajov podľa Vyhlášky o štandardoch 78/2022, §11, písm. a)