SPRÁVA ŽELEZNIC

Naše zn. 114632/2025-SŽ-GŘ-O25

Vysvětlení zadávací dokumentace č. 1

Sektorová nadlimitní veřejná zakázka dle § 60 a § 161 zákona č. 134/2016 sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***Zákon***“) na služby s názvem:

„**Nasazení MFA a pořízení nosičů certifikátů**“

Správa železnic, státní organizace (dále jen „***Zadavatel***“) obdržela dne 11. 11. 2025 v 10:38 hodin žádost o vysvětlení zadávací dokumentace. Zadavatel formou Vysvětlení zadávací dokumentace odpovídá na tuto žádost doručenou k veřejné zakázce následovně:

Dotaz č. 1:
Výklad požadavku na QSCD
Rozumíme správně, že pokud má karta technicky splňovat požadavky na kvalifikovaný prostředek pro vytváření elektronických podpisů (QSCD) dle nařízení eIDAS, měla by být uvedena na oficiálním seznamu oznámených kvalifikovaných prostředků (EU QSCD Trust List), který je veřejně dostupný na portálu Evropské komise (https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd)?
Pokud nikoli, prosíme o upřesnění, jakým způsobem má dodavatel prokázat splnění technických požadavků na QSCD, když karta není uvedena v oficiálním seznamu.

Odpověď č. 1:
V souladu se zadávací dokumentací (Příloha č. 1 - Technická specifikace, Příloha č. 4 - Požadavky na fyzické nosiče identifikačních údajů a certifikátů) musí dodavatel prokázat, že nabízený nosič certifikátů (čipová karta) splňuje technické požadavky na kvalifikovaný prostředek pro vytváření elektronických podpisů (QSCD) dle nařízení eIDAS (EU) č. 910/2014.
Na základě dotazu Zadavatel upřesňuje, že dodavatel může prokázat splnění technických požadavků libovolným z následujících způsobů:

a) Odkazem na uvedení zařízení v oficiálním seznamu oznámených kvalifikovaných prostředků (EU QSCD Trust List) vedeném Evropskou komisí;
b) Platným certifikátem Common Criteria vydaným akreditovanou laboratoří podle EN 419 221-5 nebo EN 419 241-2 s dosaženou úrovní EAL4+ nebo vyšší, uznaným v rámci SOGIS-MRA;
c) Bezpečnostním hodnotícím protokolem vydaným akreditovaným subjektem (např. BSI, ANSSI, TÜViT), který prokazuje shodu s EN 419 221-5.

Z důvodu otevřenosti zadávacího řízení a neomezování tržního prostředí ponechává Zadavatel na dodavateli, který z uvedených způsobů prokázání splnění uvedeného technického požadavku na nosič certifikátů zvolí.

Dotaz č. 2:
Účel a způsob použití karty
Prosíme o potvrzení, zda je záměrem Zadavatele, aby uvedený nosič (čipová karta) byl využíván pro vytváření **kvalifikovaného elektronického podpisu**, který vychází z **kvalifikovaného certifikátu pro elektronický podpis** vydaného kvalifikovaným poskytovatelem důvěryhodných služeb podle nařízení eIDAS.

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

V případě, že tomu tak není, prosíme o upřesnění, pro jaký typ elektronického podpisu či autentizačního účelu bude karta používána.

Odpověď č. 2:
V souladu se zadávací dokumentací (Příloha č. 1 - Technická specifikace) Zadavatel v současnosti neplánuje dodaný nosič (čipovou kartu) využívat pro vytváření kvalifikovaného elektronického podpisu založeného na kvalifikovaném cerfifikátu pro elektronický podpis vydaném kvalifikovaným poskytovatelem důvěryhodných služeb podle nařízení eIDAS.

Záměrem Zadavatele je využívat nosič pro generování a bezpečné uložení uživatelských certifikátů a příslušných privátních klíčů vydávaných systémem interních certifikačních autorit. Tyto nosiče a vydané certifikáty budou především využity k bezpečné autentizaci uživatelů vůči systému poskytující autentizační služby (konkrétně zejména Active Directory).

V souladu se zadávací dokumentací (Příloha č. 1 - Technická specifikace, Příloha č. 4 - Požadavky na fyzické nosiče identifikačních údajů a certifikátů) však Zadavatel současně požaduje, aby nabízený nosič certifikátů (čipová karta) technicky odpovídal požadavkům na kvalifikovaný prostředek pro vytváření elektronických podpisů (QSCD) a dodavatel tak získal bezpečný a technicky přesně definovaný nosič certifikátů (čipovou kartu), který bude moci případně v budoucnu využít i pro bezpečné ukládání kvalifikovaných certifikátů a vytváření kvalifikovaných elektronických podpisů v souladu s požadavky nařízení eIDAS a příslušných technických norem (např. EN 419 211, EN 419 221-5).

Dotaz č. 3:
Požadavek na prokázání shody
Bude Zadavatel požadovat doložení shody s požadavky QSCD prostřednictvím konkrétního dokumentu (např. Common Criteria – Security Target), nebo jiného ekvivalentního dokladu)?

Odpověď č. 3:
Zadavatel nepožaduje doložení shody s požadavky na kvalifikovaný prostředek pro vytváření elektronických podpisů (QSCD) prostřednictvím konkrétního jediného dokumentu. Jak je uvedeno již ve vysvětlení k dotazu č. 1, Zadavatel požaduje, aby v případě, že nabízený nosič (čipová karta) není uveden v oficiálním seznamu oznámených kvalifikovaných prostředků (EU QSCD Trust List) vedeném Evropskou komisí, dodavatel doložil technickou shodu prostřednictvím uznatelných a ověřitelných dokumentů prokazujících splnění příslušných požadavků dle nařízení eIDAS.
V souladu se zadávací dokumentací (Příloha č. 4 - Požadavky na fyzické nosiče identifikačních údajů a certifikátů) a běžnou praxí Zadavatel za takový uznatelný doklad považuje zejména:

a) platný Common Criteria certifikát vydaný akreditovanou laboratoří podle odpovídajícího Protection Profile (např. EN 419 221-5, EN 419 241-2) s dosaženou úrovní EAL4+ nebo vyšší, nebo
b) Security Target a Evaluation Technical Report (ETR) vydané akreditovanou certifikační laboratoří v rámci uznávané dohody SOGIS-MRA, případně
c) jiné ekvivalentní nezávislé posouzení shody provedené akreditovaným subjektem uznávaným v rámci evropského systému eIDAS.

Zadavatel upozorňuje, že pouhé prohlášení výrobce (čipu/nosiče certifikátu) bez doložení odpovídající certifikace nebo nezávislého posudku nebude Zadavatel považovat za dostačující.

Dotaz č. 4:
Doplňující dotaz k požadavkům na technické řešení QSCD karty
Rozumíme správně, že pokud má karta **technicky splňovat požadavky QSCD dle eIDAS**, musí být části pro komerční a kvalifikované certifikáty **striktně odděleny** a chráněny **samostatnými přihlašovacími údaji (PIN/PUK/Kvalifikovaný PIN/Kvalifikovaný PUK)**, přičemž přístup k QSCD části smí mít **výhradně držitel karty**?
Pokud tomu tak není, prosíme o upřesnění, jakým způsobem má být zajištěna bezpečnost a výlučná kontrola držitele nad soukromými klíči uloženými v QSCD části zařízení, aby byly splněny požadavky článku 29 nařízení eIDAS a příslušných prováděcích aktů.

Odpověď č. 4:
Dodavatel správně chápe požadavek Zadavatele, aby nabízený nosič (čipová karta) umožňoval oddělení prostoru určeného pro kvalifikované certifikáty a související privátní klíče od prostoru určeného pro komerční (nekvalifikované) certifikáty. Tato skutečnost vyplývá z požadavku na splnění technických požadavků na kvalifikovaný prostředek pro vytváření elektronických podpisů (QSCD) dle nařízení eIDAS (EU) č. 910/2014. Oddělení prostoru pro kvalifikované a komerční certifikáty a odpovídající privátní klíče musí být tedy zajištěno v souladu s příslušnými bezpečnostními standardy a certifikacemi, které nosič certifikátů (čipová karta) deklaruje (např. Common Criteria, EN 419 211, EN 419 221-5).

Zadavatel v zadávací dokumentaci neurčuje konkrétní způsob ochrany jednotlivých částí karty bezpečnostními kódy (PIN/PUK/Kvalifikovaný PIN/Kvalifikovaný PUK), požaduje však, aby použité mechanismy přístupu odpovídaly certifikovanému bezpečnostnímu návrhu daného typu karty a zajišťovaly splnění požadavků článku 29 nařízení eIDAS, tj. aby byla zajištěna výlučná kontrola držitele nad soukromými klíči uloženými v části určené pro kvalifikované certifikáty.

Zadavatel tedy připouští, že bezpečnostní kódy (např. PUK) mohou být sdílené nebo oddělené pro jednotlivé části karty, pokud takové řešení odpovídá certifikovanému bezpečnostnímu modelu zařízení a neohrožuje výlučnou kontrolu držitele nad privátními klíči kvalifikovaných certifikátů.

Dotaz č. 5:
Dotaz k požadavkům na bezpečnostní prvky čipové karty
V zadávací dokumentaci (příloha č.1) je uvedeno, že čipová karta musí být opatřena potiskem (**hologramem).** V příloze č.4. Zadavatel uvádí, že nosič má být opatřen ochranným prvkem pro ověření autenticity nosiče (např. hologram). Není tedy jasné, zda hologram je nezbytně nutný a jediný uznatelný bezpečnostní prvek na nosiči certifikátů.
Prosíme o upřesnění, jakým způsobem Zadavatel definuje pojem „bezpečnostní prvek" ve smyslu zadávací dokumentace.
Konkrétně si dovolujeme požádat o potvrzení, zda může být za bezpečnostní prvek považováno například:

- vygravírované nebo vytištěné unikátní číslo kontaktního čipu na povrchu karty, které jednoznačně kartu definuje
- jiný fyzický identifikační znak, který není hologramem, ale umožňuje jednoznačnou vizuální identifikaci nosiče a omezuje možnost záměny či neoprávněné manipulace.

Pokud takové řešení není považováno za dostatečný bezpečnostní prvek, prosíme o specifikaci, **jaké parametry** (např. typ, úroveň ochrany, vizuální nebo fyzikální charakteristiky) musí alternativní bezpečnostní prvek splňovat, aby vyhověl požadavkům zadávací dokumentace.

Odpověď č. 5:
Zadavatel v souladu se zadávací dokumentací (Příloha č. 1 - Technická specifikace) požaduje, aby dodaný nosič (čipová karta) byl opatřen vizuálním ochranným prvkem pro ověření jeho autenticity, a to konkrétně hologramem.

Zadavatel požaduje, aby hologram byl umístěn přímo na těle karty nebo byl součástí laminační ochranné fólie, která je po provedení potisku s kartou trvale a neoddělitelně spojena. Účelem je zajištění trvalé fyzické ochrany karty proti neoprávněné manipulaci, kopírování nebo záměně.

Jiné formy identifikace nosiče (např. vytištěné nebo gravírované číslo čipu či jiné fyzické znaky) nemohou být považovány za plnohodnotný bezpečnostní prvek ve smyslu zadávací dokumentace, neboť nesplňují požadavek na vizuální ověřitelnost autenticity a odolnost proti falzifikaci.

Dotaz č. 6:
Kontinuita služeb
Prosíme o upřesnění, zda Zadavatel požaduje, z důvodu zajištění dlouhodobé udržitelnosti projektu, **kontinuity služeb** a jeho bezproblémového provozu, aby dodané nosiče (čipové karty) **umožňovaly vydávání a používání kvalifikovaných certifikátů** od **více kvalifikovaných**

poskytovatelů důvěryhodných služeb (QTSP), a nikoliv pouze od jednoho konkrétního poskytovatele.
Pokud ano, prosíme o uvedení, zda má být tato interoperabilita s více QTSP prokázána již v rámci nabídky, nebo postačí její zajištění v průběhu následné implementace.

Odpověď č. 6:
V souladu se zadávací dokumentací (čl. 2.1 Přílohy č. 1 - Technická specifikace) Zadavatel nepožaduje v rámci nabídky prokázání interoperability s kvalifikovanými poskytovateli služeb vytvářejících důvěru (QTSP).

Dotaz č. 7:
Archivace privátních klíčů v procesu vydávání šifrovacích certifikátů
Prosíme o upřesnění, zda Zadavatel požaduje, aby privátní klíče šifrovacích certifikátů byly archivovány **přímo v HSM** (HSM key storage), nebo zda je přípustné jejich **uložení mimo HSM** při současném **zajištění ochrany prostřednictvím HSM klíče** (HSM-encrypted key storage / key wrapping).

Odpověď č. 7:
Zadavatel v souladu se zadávací dokumentací (Příloha č. 3 - Požadavky na systém řízení životního cyklu certifikátů, nosičů certifikátů a obslužný software) trvá na požadavku archivace privátních klíčů šifrovacích certifikátů v bezpečném hardware HSM (HSM Key Storage). Příslušné HSM jsou součástí PKI prostředí Zadavatele.

Dotaz č. 8:
Podpora schvalovacích procesů a segregace rolí správy certifikátů a jejich nosičů
Prosíme o specifikaci, **v jakém rozsahu a počtech** bude nutné implementovat procesy schvalování a segregace rolí správy certifikátů a jejich nosičů, aby bylo možné správně navrhnout kapacitu a rozsah řešení.

Odpověď č. 8:
Zadavatel v souladu se zadávací dokumentací (Příloha č. 1 - Technická specifikace) upozorňuje dodavatele, že návrh procesů schvalování a segregace rolí správy certifikátů a jejich nosičů je součástí před-implementační analýzy (čl. 4.1 Přílohy č. 1 - Technická specifikace).

Současně Zadavatel vysvětluje svůj požadavek dodavatele následovně:

Cílem požadavku na *"návrh obslužných procesů systému správy životního cyklu osobních uživatelských certifikátů, včetně definování rolí a jejich bezpečnostní segregace, a detailní návrh schvalovacích procesů/workflow, detailní návrh automatizace anonymizace osobních údajů, detailní návrh řešení registračních autorit, detailní návrh notifikačních procesů"* je zajistit, aby byla důsledně uplatněna zásada segregace odpovědností a aby žádný správce neměl výhradní kontrolu nad kritickými procesy, jako je vydávání, obnova nebo zneplatnění certifikátů.

Zadavatel tedy požaduje, aby v rámci implementace systému byla zajištěna segregace rolí a procesů správy certifikátů a jejich nosičů tak, aby žádný jednotlivý správce neměl výhradní kontrolu nad procesem vydávání či správou certifikátů.

Konkrétně Zadavatel předpokládá využití mechanismů „Enrollment Agent" při vydávání certifikátů, kdy proces vydání certifikátu vyžaduje účast alespoň dvou subjektů s odlišnými rolemi (např. správce infrastruktury a schvalovatele žádosti).

Dále Zadavatel předpokládá, že oprávnění správců budou omezena na úrovni šablon certifikátů, tj. aby jednotliví správci mohli vydávat certifikáty pouze z předem definovaných šablon a pro určené skupiny držitelů karet.

Dotaz č. 9:
Podpora schvalovacích procesů a segregace rolí správy certifikátů a jejich nosičů
Prosíme o specifikaci, **v jakém rozsahu a počtech** bude nutné implementovat procesy schvalování a segregace rolí správy certifikátů a jejich nosičů, aby bylo možné správně navrhnout kapacitu a rozsah řešení.

Odpověď č. 9:
Jedná se o dotaz duplicitní s dotazem č. 8 - viz odpověď na dotaz č. 8.

Dotaz č. 10:
Evidence aktualizací systémů využívajících nosiče certifikátů
Prosíme o potvrzení, zda Zadavateli postačuje, aby evidence aktualizací systémů využívajících nosiče certifikátů byla **dostupná v prostředí Excelu nebo webového rozhraní**, případně o upřesnění, jaká forma evidence je požadována.

Odpověď č. 10:
Zadavatel nemá pro oblast evidence aktualizací systémů využívajících nosiče certifikátů specifické požadavky a volbu nástroje nebo prostředí pro evidenci aktualizací těchto systémů ponechává na dodavateli.

Dotaz č. 11:
Příprava dat pro personalizaci karet a automatizované zpracování
Prosíme o upřesnění, **jakým způsobem** mají být připravována data pro personalizaci karet, **která konkrétní data** mají být součástí tohoto procesu, a **jaké technické parametry přenosu** dat Zadavatel požaduje (např. formát, způsob zabezpečení, komunikační rozhraní apod.).

Odpověď č. 11:
V souladu se zadávací dokumentací (čl. 2.4.3.4 Přílohy č. 1 – Technická specifikace) jsou zdrojová data pro personalizaci nosičů obsažena v personálním systému Zadavatele. Pro zajištění maximální otevřenosti zadávacího řízení neurčuje Zadavatel v zadávací dokumentaci formát či způsob předání a zabezpečení personalizačních dat. Konkrétní formáty a způsoby předání budou stanoveny v před-implementační analýze (čl. 4.1 Přílohy č. 1 – Technická specifikace).

Změna termínu pro podání nabídek
Zadavatel současně s tímto Vysvětlením zadávací dokumentace oznamuje změnu v údaji o uplynutí lhůty pro podání nabídek, která je na profilu Zadavatele v elektronickém nástroji E-ZAK stanovena na 24. 11. 2025, 00:00 hodin, přičemž údaj o čase byl takto automaticky stanoven elektronickým nástrojem, jelikož ze strany Zadavatele došlo při uveřejňování zadávací dokumentace na profilu zadavatele k opomenutí vyplnění tohoto údaje. Z údajů uvedených ve věstníku veřejných zakázek (Oznámení o zahájení zadávacího řízení) ovšem vyplývá, že lhůta pro podání nabídek končí až 24. 11. 2025 v 09:00 hodin. Zadavatel tak tímto dává do souladu tyto rozdílné údaje. Pro vyloučení pochybností Zadavatel uvádí, že tato změna nepředstavuje prodloužení lhůty pro podání nabídek, pouze odstraňuje předchozí administrativní pochybení.

Závěr
Zadavatel zcela setrval na zadávacích podmínkách. Lhůta pro podání nabídek se tak nemění a je stanovena na den 24. 11. 2025 do 09:00 hod.

Ing. Dalibor Fajkus
14.11.2025 08:08
Podepsáno
elektronicky

.....
Ing. Dalibor Fajkus
ředitel organizační jednotky
Správa železniční telematiky