VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE – SOUBOR DODATEČNÝCH INFORMACÍ ZADAVATELE Č. 1

Společnost:	**ExpertaLabs, s.r.o.**
Se sídlem:	Nové sady 988/2, Staré Brno, 602 00 Brno
IČO:	11791667
Zastoupen:	Ing. Milošem Ohlídalem, Ph.D., jednatelem

***Název zakázky*:**

„Vývoj Expertalabs ITS Platformy pro využití v inteligentních dopravních systémech“

Zadavatel poskytuje toto následující vysvětlení zadávací dokumentace vztahujícím se k výše uvedené zakázce.

Znění žádosti o vysvětlení zadávací dokumentace č. 1:
„Jaké jsou USE CASES (cíl využití)?“

Znění vysvětlení zadávací dokumentace č. 1:
Cílem je vytvořit robustní, plně škálovatelnou a generickou PKI platformu, která bude tvořit páteř bezpečnosti naší ExpertaLabs ITS Platformy. Mezi kritické use-cases mimo jiné patří:

* Komplexní správa životního cyklu zařízení v masivně distribuovaném prostředí.
* Vydávání a správa device-specific certifikátů pro striktní identifikaci a autentizaci koncových prvků.
* Plně automatizovaný životní cyklus certifikátů (provisioning, obnova, expirace a bezpečný decommissioning / revokace kompromitovaných zařízení) bez nutnosti servisních zásahů.
* Vybudování infrastruktury pro bezpečnou správu certifikátů k podpisu softwaru a aktualizací, splňující nejvyšší industry best practices.
* Striktní procesní i systémová správa vysoce citlivých, tzv. „pouze offline“ certifikátů (např. Root CA nebo certifikáty pro podpis bootloaderu v rámci mechanismu verified boot), které se za žádných okolností nesmí objevit na stroji s přístupem k síti.
* Výstupem musí být komplexní řešení dodané „na míru“, zahrnující deployment, veškeré zdrojové kódy (včetně výhradní licence) a detailní technickou dokumentaci zpracovanou výhradně v anglickém jazyce. Součástí dokumentace musí být i precizně definované procesy pro bezpečnou manipulaci s kryptografickým materiálem. PKI Infrastrukturu plánujeme provozovat a následně rozvíjet (nad rámec oprav chyb v záruce) interně.

Znění žádosti o vysvětlení zadávací dokumentace č. 2:
„Pro jaká zařízení se má využívat?“

Znění vysvětlení zadávací dokumentace č. 2:
Systém bude nasazován v silně heterogenním hardwarovém prostředí. Primárně se jedná o širokou škálu embedded Linux zařízení (postavených např. na architekturách ARM, x86, NVIDIA Tegra či sériích i.MX6/i.MX8)[1]. Architektura musí bezpodmínečně podporovat hlubokou integraci s hardwarovými bezpečnostními moduly (HSM) a Trusted Platform Moduly (TPM), a to jak na straně backendu (včetně CI serverů), tak na straně koncových edge zařízení.

[1] Zadavatel uvádí obchodní názvy z důvodu popisu současného prostředí zadavatele. Účastník nabídne jakékoli řešení (jakékoli značky), které zajistí kompatibilitu s uvedeným systémem/prostředím.

Znění žádosti o vysvětlení zadávací dokumentace č. 3:
„Která konkrétně zařízení a typy certifikátů se mají inicializovat?“

Znění vysvětlení zadávací dokumentace č. 3:
V této fázi iterativního vývoje nelze výčet koncových zařízení finálně a exaktně uzavřít. Požadujeme univerzální podporu pro všechna moderní zařízení postavená na Linuxu[2], která se využívají v rámci inteligentních dopravních systémů (ITS). Infrastruktura musí podporovat standardní typy certifikátů rodiny X.509 a pokrývat složitou certifikační hierarchii. Kromě běžných autentizačních certifikátů pro zařízení je naprosto kritickou podmínkou plná podpora správy certifikátů pro podpis softwarových balíčků. Platforma ExpertaLabs je koncipována jako masivně rozšiřitelný framework, dodané PKI řešení proto nesmí být limitováno konkrétním výčtem hardwaru a musí být vysoce rozšiřitelné.

Znění žádosti o vysvětlení zadávací dokumentace č. 4:
„Jaké typy protokolů se mají využít pro komunikaci?“

Znění vysvětlení zadávací dokumentace č. 4:
Tyto dotazy jsou v daném znění příliš obecné a abstraktní. Záleží, o jaké komunikační vrstvě a mezi kterými konkrétními prvky architektury se bavíme. Očekáváme, že dodavatel jako expert navrhne a zdůvodní použití nejvhodnějších a vysoce zabezpečených protokolů (odolných např. vůči MITM útokům) pro komunikaci mezi centrální PKI, koncovým zařízením, výrobními manufacturing tooly a správní aplikací. Konkrétní specifikace protokolů vyplyne a bude schválena až v rámci společného architektonického návrhu.

Znění žádosti o vysvětlení zadávací dokumentace č. 5:
„Jakým způsobem se do zařízení budou dostávat certifikáty a klíče?“

Znění vysvětlení zadávací dokumentace č. 5:
Primární provisioning certifikátů a kryptografických identit musí probíhat v přísně kontrolovaném prostředí během výrobního procesu nebo případně při inicializačním prvním spuštění zařízení (first boot). PKI infrastruktura pro tyto účely musí vystavovat vysoce zabezpečené a auditovatelné API (včetně alertingu) určené pro integraci s manufacturing tooly na výrobní lince. Nedílnou součástí dodávky je i detailní popis procesů pro samotnou továrnu a pro deployment manufacturing toolů u nových zákazníků. Systém musí robustně a prokazatelně eliminovat jakákoliv rizika – je technicky i procesně nepřípustné, aby například zákazník A mohl dodávat zařízení, která by se mohla autentizovat a prokazovat identitou patřící zákazníkovi B.

Znění žádosti o vysvětlení zadávací dokumentace č. 6:
„Jakým způsobem se realizují žádosti vystavení?“

Znění vysvětlení zadávací dokumentace č. 6:
Jak již bylo zmíněno, finální aplikační toky budou definovány a zpřesňovány agilním způsobem v souběhu s vývojem hlavní větve platformy. Očekáváme automatizovaný přístup, dodavatel však musí s touto mírou vstupní nejistoty a nutností iterativního dopracování API pro žádosti jasně počítat ve své nabídce.

Znění žádosti o vysvětlení zadávací dokumentace č. 7:
„Co znamená požadavek na " řízením SW licencí" a "řízení softwarových licencí vázaných na konkrétní zařízení"?“

Znění vysvětlení zadávací dokumentace č. 7:
Tímto se rozumí komplexní systém pro generování, distribuci a centrální správu podepsaných licencí, které na daném zařízení (a pouze na něm) odemknou, omezí, nebo naopak časově či

[2] Zadavatel uvádí obchodní názvy z důvodu popisu současného prostředí zadavatele. Účastník nabídne jakékoli řešení (jakékoli značky), které zajistí kompatibilitu s uvedeným systémem/prostředím.

modulárně zpřístupní specifickou funkcionalitu. Jde o správu celého životního cyklu licence (aktivace, deaktivace, obnova) s vysokým stupněm ochrany proti neoprávněnému kopírování či zneužití softwaru.

Systém bude vyžadovat robustní a vysoce zabezpečené uživatelské rozhraní (GUI/WebUI)[3] s pokročilou správou uživatelů. Neočekáváme pouhý základní přístup, ale komplexní implementaci řízení přístupu na základě rolí (RBAC - Role-Based Access Control) a striktní uplatnění principu nejmenších oprávnění (least privilege). Toto rozhraní musí umožňovat granulární nastavení oprávnění pro různé úrovně administrátorů, operátorů a servisních techniků. Naprostou nutností je podpora vícefaktorového ověření (MFA) a detailní auditní logování veškerých uživatelských aktivit spojených se správou licencí a kryptografických materiálů, aby byla zajištěna stoprocentní prokazatelnost jakéhokoliv zásahu do systému.

Znění žádosti o vysvětlení zadávací dokumentace č. 8:
„Jaká je vazba na centralizovanou správu certifikátů a centralizovanou správu a licencí?“

Znění vysvětlení zadávací dokumentace č. 8:
Z našeho pohledu jsou tyto agendy technologicky neoddělitelné. Licenční systém je organickou součástí poptávané PKI infrastruktury, jelikož se přímo opírá o distribuované klíče a certifikáty daných zařízení.

Znění žádosti o vysvětlení zadávací dokumentace č. 9:
„V čem má spočívat ta integrační vrstva?“

Znění vysvětlení zadávací dokumentace č. 9:
Tento dotaz je bez hlubšího kontextu nejasný a nevíme, k jakému přesnému bodu zadání směřuje. Znovu však upozorňujeme, že celý systém musí plně podporovat integraci s výrobním provisioningem zařízení a poskytovat moderní integrační rozhraní (např. REST API) pro komunikaci s centrální správou zařízení.

Znění žádosti o vysvětlení zadávací dokumentace č. 10:
„Co představuje požadavek: "Licence musí být kryptograficky vázána."?“

Znění vysvětlení zadávací dokumentace č. 10:
Tento požadavek představuje absolutní technickou pojistku proti neoprávněné manipulaci. Znamená to, že vydaná licence musí být kryptograficky spojena s unikátní identitou konkrétního kusu hardwaru (např. s jeho specifickým certifikátem či hardwarovým kořenem důvěry). Technicky to musí být implementováno a garantováno tak, že jakýkoliv pokus o přenesení licenčního souboru nebo licenčních dat na jiný fyzický hardware povede k okamžité neplatnosti licence bez příslušné autorizace.

---

[3] Zadavatel uvádí obchodní názvy z důvodu popisu současného prostředí zadavatele. Účastník nabídne jakékoli řešení (jakékoli značky), které zajistí kompatibilitu s uvedeným systémem/prostředím.

Informace o prodloužení lhůty pro podání nabídek:

Zadavatel prodlužuje lhůtu pro podání nabídek do **27. 2. 2026 do 10:00**.
Místo a způsob podávání nabídek zůstávají nezměněné.
Otevírání obálek s nabídkami proběhne **27. 2. 2026. v 10:05.**

V Brně, dne 18. 2. 2026

Ing. Jan Ševčík
Digitálně podepsal Ing. Jan Ševčík
Datum: 2026.02.18 10:20:40 +01'00'

RPA LEGAL, s.r.o.
Ing. Jan Ševčík, jednatel
Zástupce zadavatele