Deloitte.

Prezentace pro Sdružení pro dopravní telematiku

Studie proveditelnosti – vrstva „C-ITS bezpečnost“

Představení výstupu projektu

Březen 2021

Obsah

1. Výchozí situace a cíl projektu

Studie proveditelnosti – vrstva „C-ITS bezpečnost“ (dále jen „Studie“) je prvním krokem pro zajištění bezpečnostní vrstvy PKI, který je centrálním a nezbytným prvkem pro provoz a další rozvoj kooperativních (C-ITS) systémů v ČR.

Výchozí situace

⇒ **ČR v letech 2015-2021 realizuje pilotní projekty kooperativních systémů (C-ITS)** v rámci evropského projektu C-ROADS. V rámci projektu je provozována i bezpečnostní vrstva PKI, díky níž je zajištěn přenos zabezpečených C-ITS zpráv.

⇒ **Stávající poskytovatel PKI ke konci projektu C-ROADS CZ ukončí provoz centrálních prvků C-ITS systému v ČR** (bezpečnostní vrstva PKI, Integrační platforma).

⇒ **ŘSD ČR bylo ze strany MD pověřeno k realizaci nezbytných kroků pro zajištění provozu C-ITS po ukončení projektu C-ROADS CZ**.

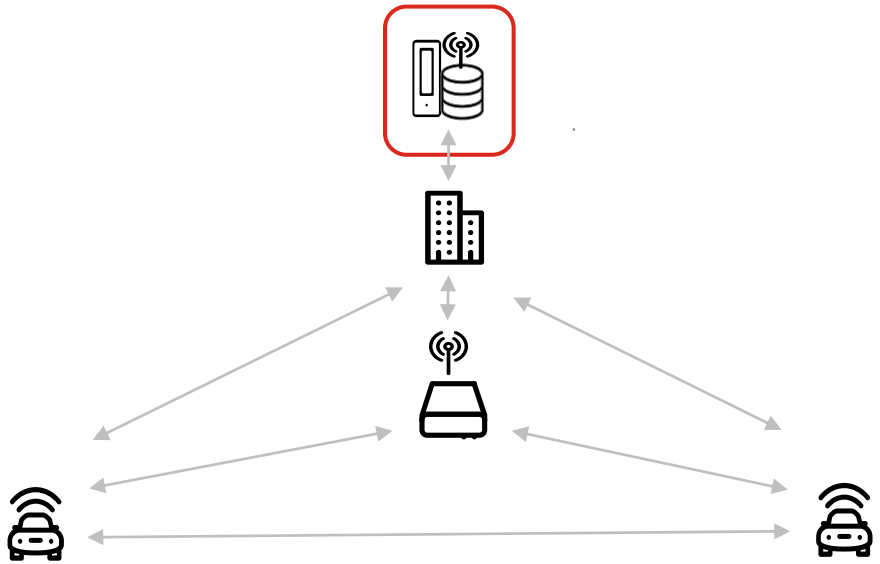
⇒ ŘSD ČR zadalo zpracování Studie proveditelnosti pro bezpečnostní vrstvu PKI, která má za úkol **posoudit možnosti nastavení provozního modelu PKI jako centrálního prvku pro zajištění bezpečnosti C-ITS systému.**

Centrální prvky C-ITS
- *Bezpečnostní vrstva PKI*
- *Integrační platforma*

C-ITS Back-Office

C-ITS jednotky na infrastruktuře (RSU)

C-ITS jednotky ve vozidlech (OBU, RVU)

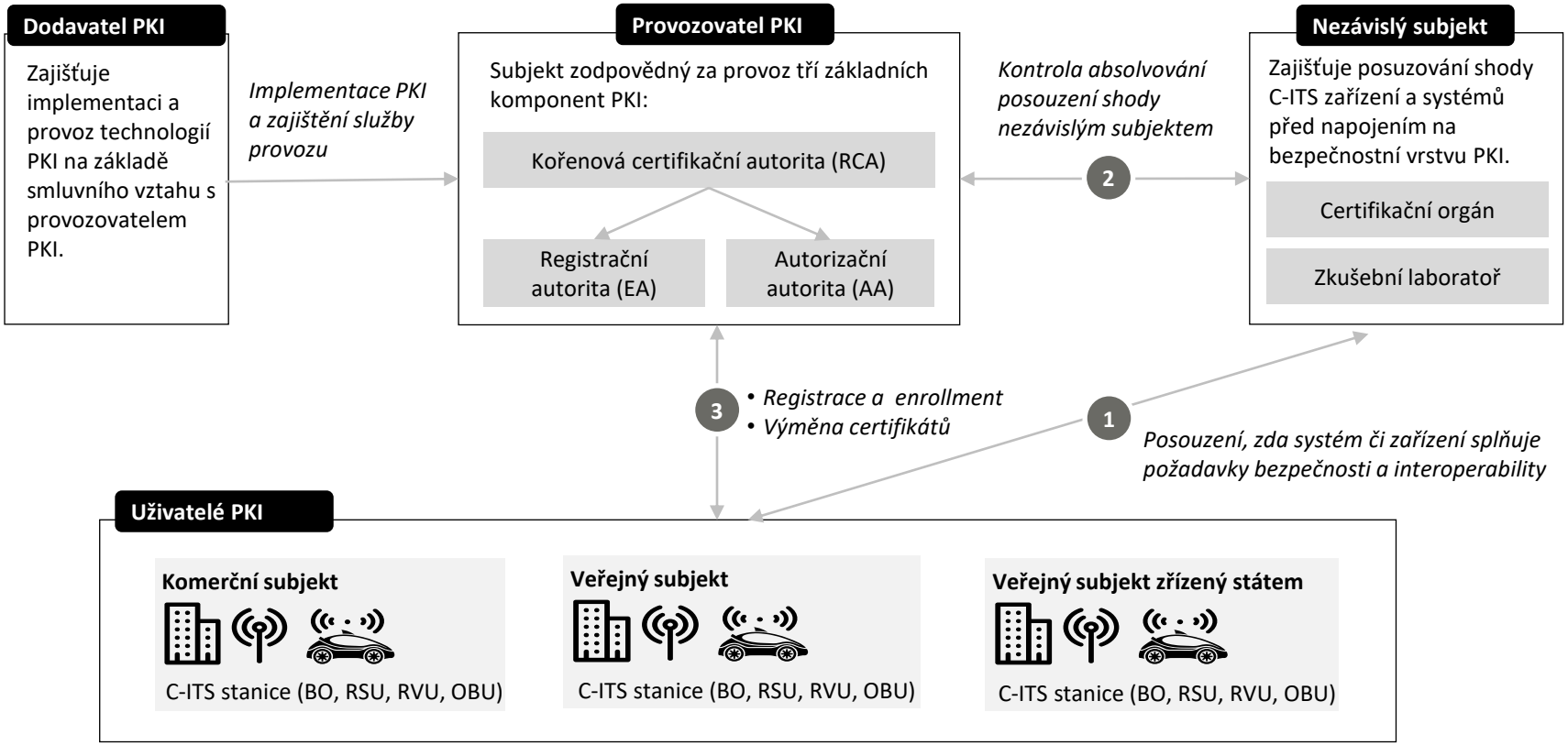


Cíl projektu / studie

Definování požadavků pro dodavatele a provozovatele centrálních komponent za účelem zajištění bezpečné a důvěryhodné služby C-ITS na území ČR, včetně navržení různých variant provozních modelů, které budou vycházet z požadavků na jednotlivé komponenty.

2. Stručný popis C-ITS ve vztahu k PKI

Ekosystém C-ITS bude tvořen několika subjekty – provozovatelem PKI, uživateli PKI (veřejnými i komerčními provozovateli C-ITS systémů) a nezávislým subjektem, který zajišťuje posuzování shody C-ITS zařízení a systémů před napojením na bezpečnostní vrstvu PKI.

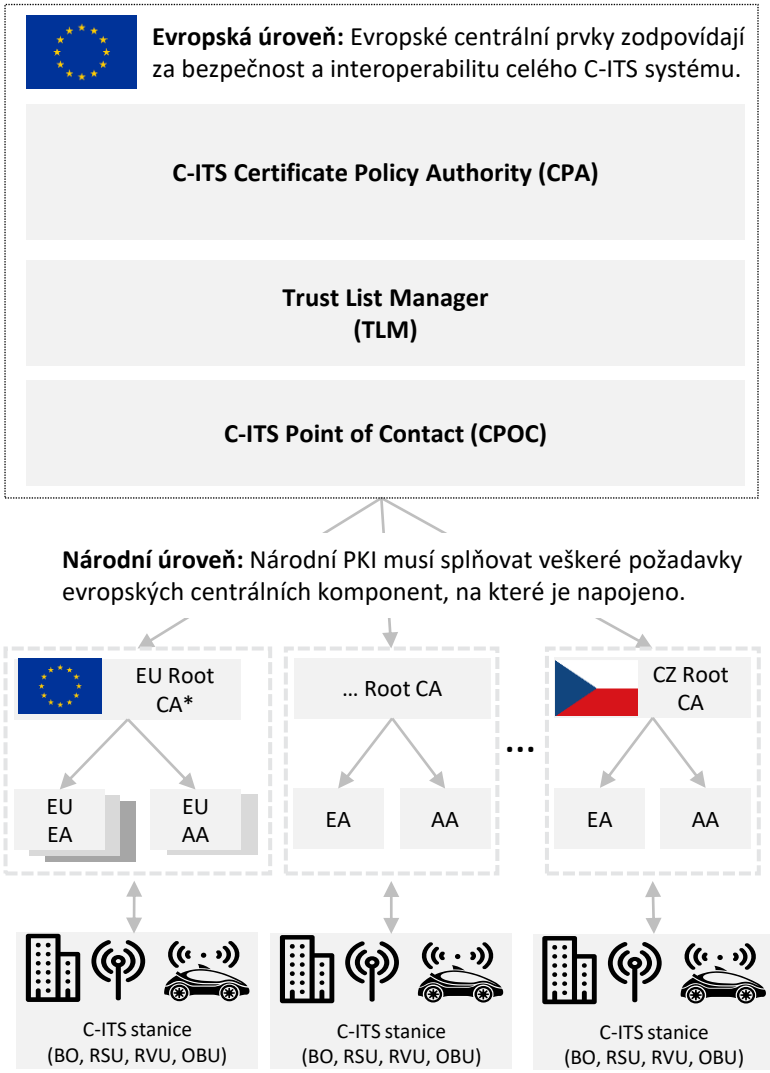


3. Stručný popis základních funkcionalit PKI v mezinárodním prostředí

Studie popisuje bezpečnostní vrstvu PKI z pohledu jejích komponent a funkcionalit, popisuje kritéria interoperability a bezpečnosti.

Bezpečnostní vrstva PKI

⇒ Bezpečnostní vrstva C-ITS je vystavěna na principu infrastruktury veřejných klíčů, které zajišťují digitální podepisování veškeré elektronické komunikace mezi aktéry, a tím garantuje integritu a nepopiratelnost dat.



⇒ **CPA je autorita, kterou tvoří zástupci veřejných a soukromých subjektů.**

⇒ **CPA spravuje certifikační pravidla**, jimiž řídí provozovatelé PKI autorit a C-ITS stanic.

⇒ **CPA spravuje autorizace PKI**, tedy autorizuje evropské centrální prvky, schvaluje RCA a definuje audity a kontroluje auditní zprávy.

⇒ **TLM** je centrální komponenta, nejvyšším **správcem všech RCA.**

⇒ **TLM tvoří vzájemnou důvěru mezi RCA** díky European Certificate Trust List (ECTL), ve kterém jsou vloženy a zveřejněny certifikáty všech důvěryhodných RCA.

⇒ **CPOC** je centrální prvek, který **zajišťuje procesy související s distribucí certifikátů mezi TLM a RCA.**

Kořenová certifikační autorita (RCA), vydává certifikáty žadatelům a zajišťuje management certifikátů.

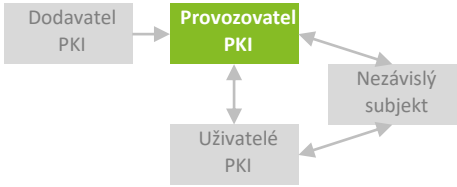
Registrační autorita (EA), registruje žadatele a ověřuje jeho identitu.

Autorizační autorita (AA), poskytuje registrovaným subjektům autorizaci k využívání C-ITS služeb.

*** Evropské PKI** (EU Root CA, EU EA, EU AA) slouží pro subjekty, které nemají vlastní PKI.

4. Požadavky na provozovatele PKI

Studie popisuje hlavní principy PKI a nezbytné podmínky pro vytvoření prostředí pro vznik PKI, které jsou zároveň požadavkem na provozovatele.



ŘEDITELSTVÍ SILNIC A DÁLNIC ČR

Provozovatel PKI: Na základě pověření Ministerstva dopravy ze dne 8. 10. 2020 je **pro zajištění provozu centrálních prvků navržen subjekt ŘSD ČR.**

Vybrané požadavky na provozovatele PKI:

Zajištění fyzické bezpečnosti bezpečnostní vrstvy

Veškeré operace musí být realizovány ve fyzicky chráněném prostředí. Prostředí musí být zabezpečeno a být fyzicky kontrolováno v souladu s normami ISO 27001 a ISO 27005. Jedná se například o požadavky:

⇒ **Budovy a místnosti splňují požadavky na provoz systémů** s vysokou hodnotou a citlivými informacemi.

- *Prostředí funguje v samostatné síti bez propojení mimo důvěryhodné prostředí, je rozděleno do více perimetrů.*
- *Citlivá data jsou bezpečně uložena s vícenásobným řízením přístupů a bezpečnostní opatření musí odolat většině útoků (souvisí např. s vícefaktorovou autentizací, CCTV či ostrahou objektu v režimu 24/7).*

⇒ **Zařízení a data musí být zabezpečena proti neautorizovanému přístupu**.

Zajištění procesu registrace systémů a zařízení

⇒ Proces registrace systémů a zařízení bude automatizován. Pro složitější operace, kdy je nutné pro **manuální proces schvalování registrací systémů a zařízení zajištění personální kapacity obsluhy.**

⇒ V rámci registrace systémů a zařízení je nezbytné **zajištění správních a smluvních okolností registrace.**

Zavedení systému pro nezávislé posuzování shody

Provozovatel musí zajistit, aby do RCA byly napojovány pouze zařízení a systémy, které prošly certifikačním procesem. Pro umožnění napojení subjektů je nutné:

⇒ **Definovat podmínky pro napojení** na národní centrální komponenty.

Zajištění procesní a personální bezpečnosti

Bezpečnost a její kontrola by měla být popsána v Certifikační prováděcí směrnici nově vznikajícího RCA. Zapracovány by měly být například požadavky:

⇒ **Stanovení důvěryhodných osob a rolí.**

⇒ **Poskytování přiměřené autorizace pro plnění stanovených úkolů** při zachování odpovídající míry bezpečnosti.

Zajištění logování, auditu, zálohování, archivace, incident managementu a kontinuity

Součástí provozu PKI musí být:

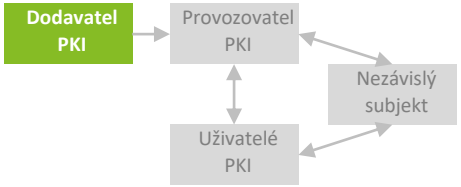
⇒ Vytváření auditních logů, které zaznamenávají nejen události, ale také činnosti zaměstnanců a systémových prostředků.

⇒ **Pravidelná kontrola a ukládání auditních logů**, logy musí být ukládány na dedikovaná úložiště pro potřeby auditu.

⇒ **Nastavení zálohovacích zařízení a procesů, kdy data musí být ukládána do zabezpečeného úložiště**, které je oddělené od provozního PKI, ale musí splňovat stejné požadavky na bezpečnost.

5. Požadavky na dodavatele PKI

Studie definuje požadavky na dodavatele PKI a poskytuje tak vstupy do technické specifikace zadávací dokumentace na dodavatele PKI.



Přístup:

⇒ Architektura a definice funkcionalit bezpečnostní vrstvy **vychází z platných směrnic, norem, předpisů a nařízení.**

⇒ Byly stanoveny požadavky na řízení projektu, funkční a technické požadavky a požadavky na provoz. **Požadavky jsou využitelné pro tvorbu zadávací dokumentace na dodavatele PKI.**

⇒ **Požadavky na PKI byly srovnány s požadavky na evropské komponenty PKI** (RCA a interní EA a AA).

A Řízení projektu

A.1. Etapizace

Etapa 1: Implementace bezpečnostní vrstvy včetně:

- návrhu implementace
- testování systému, pilotního provozu v délce 6 měsíců
- předání veškeré dokumentace, licencí, zdrojových kódů SW a HW

Etapa 2: Provoz PKI, včetně rozvoje

A.2. Požadavky na dokumentaci

Sestaven seznam minimálního rozsahu dokumentace.

A.3. Doporučení k testování systému

B Funkční požadavky

Definovány minimální funkcionality bezpečnostní vrstvy pro oblasti:

⇒ Obecné funkční požadavky

⇒ Minimální funkční požadavky na kořenovou certifikační autoritu

⇒ Minimální funkční požadavky na interní registrační autoritu

⇒ Minimální funkční požadavky na interní autorizační autoritu

C Technické požadavky

Definovány technické požadavky na realizaci bezpečnostní vrstvy:

⇒ Škálovatelnost

⇒ Požadavky na prostředí

⇒ Požadavky na HW

D Požadavky na provoz

Definovány parametry pro provoz bezpečnostní vrstvy:

⇒ Dostupnost systému a podpory

⇒ Uživatelská podpora

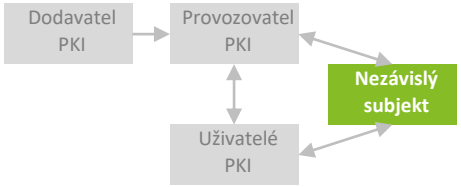
⇒ Definice incidentů

⇒ Maximální odezva na incidenty

⇒ Maximální doba pro řešení kritických problémů

6. Požadavky na nezávislý subjekt

Studie popisuje bezpečnostní vrstvu z pohledu ověření, jakým způsobem má být C-ITS systém uživatele posouzen z pohledu bezpečnosti a interoperability. Studie definuje možné varianty, jakým způsobem certifikaci zajistit:



1 Agenda činnosti nezávislého subjektu:

Cílem je ověření C-ITS systému (posouzení shody), zda splňuje kritéria bezpečnosti a interoperability před připojením do národních centrálních prvků C-ITS. Mezi dílčí části kontroly patří:

- ⇒ Kontrola autentizačních, autorizačních a bezpečnostních mechanismů
- ⇒ Kontrola integrity
- ⇒ Kontrola dostupnosti
- ⇒ Kontrola důvěryhodnosti a soukromí
- ⇒ Kontrola zabezpečení enrollmentu
- ⇒ Kontrola zabezpečení autorizace
- ⇒ Kontrola nastavení ověřování seznamu zneplatněných certifikátů
- ⇒ Kontrola interoperability vysílaných/přijímaných C-ITS zpráv

2 Varianty provedení posouzení shody:

Byly identifikovány 3 varianty posouzení shody, u kterých byly ve studii posouzeny jejich přínosy a potenciální rizika:

A SAMOHODNOCENÍ A POSOUZENÍ SHODY DRUHOU STRANOU

- Posouzení shody prováděno výrobcem, výstupem je prohlášení o shodě.
- Odpovědnost je přenesena na výrobce.

- **Varianta není dostatečná, pokud by byla realizovaná samostatně.**
- Variantu je možné aplikovat dočasně, v rámci prozatímní varianty.

B POSUZOVÁNÍ NEZÁVISLÝM SUBJEKTEM

- Posouzení provádí třetí nezávislá strana zastoupena certifikačním orgánem a zkušební laboratoří.
- Certifikace prováděna na začátku životního cyklu systému, zařízení nebo výrobku.

- **Varianta je hodnocena jako minimální.**

C POSUZOVÁNÍ NEZÁVISLÝM SUBJEKTEM S RECERTIFIKACÍ

- Posouzení provádí třetí nezávislá strana zastoupena certifikačním orgánem a zkušební laboratoří.
- Certifikace prováděna opakovaně při každé významnější změně.

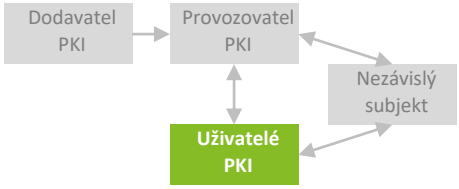
- **Varianta je hodnocena jako optimální.**

3 Subjekty identifikované jako vhodné pro roli nezávislého subjektu:

- ⇒ **Organizace zřízené státem** (např. CDV, v.v.i., CENDIS, s.p.).
- ⇒ **Vybrané veřejné vysoké školy**, které mají zkušenosti z oblasti ITS/C-ITS.
- ⇒ **Organizace, které již provozují Certifikační orgán** pro jiné stanovené výrobky nebo **provozují zkušební laboratoř** pro jiné stanovené výrobky.

7. Požadavky na uživatele

Studie se zabývá požadavky z pohledu dostupnosti, respektive přístupu uživatelů, pro které je bezpečnostní vrstva určena, a jejich podílu na financování.



1 Přístup uživatelů k PKI

	A	B	C
	NÁRODNÍ PKI DOSTUPNÉ PRO VŠECHNY UŽIVATELE	**NÁRODNÍ PKI DOSTUPNÉ PRO VEŘEJNÉ SUBJEKTY**	**NÁRODNÍ PKI JE DOSTUPNÉ PRO VEŘEJNÉ SUBJEKTY ZŘÍZENÉ STÁTEM**
POPIS VARIANT	• Služba národního PKI je nabízena všem uživatelům z veřejného i komerčního sektoru.	• Služba národního PKI je nabízena zájemcům o službu, kteří jsou veřejným subjektem (obce, dopravní podniky) a subjektům zřízeným státem (ŘSD, Správa železnic, ŘVC).	• Služba národního PKI je nabízena zájemcům o službu, kteří jsou veřejným subjektem zřízeným státem (ŘSD, Správa železnic, ŘVC).

2 Podíl uživatelů na financování PKI

	A	B	C
	SLUŽBA POSKYTOVÁNA BEZÚPLATNĚ (MODEL NDIC)	**SLUŽBA SPOLUFINANCOVÁNA VŠEMI UŽIVATELI**	**SLUŽBA PRO VEŘEJNÉ SUBJEKTY BEZÚPLATNĚ, PRO KOMERČNÍ SUBJEKTY ZA POPLATEK**
POPIS VARIANT	• ŘSD ČR poskytuje informace z NDIC zdarma, uživatel má povinnost je šířit zdarma. • Pokud uživatel vytvoří službu s přidanou hodnotou, pak může službu zpoplatnit.	• Jedná se o spolufinancování nákladů vzniklých při sběru a poskytování dat, tedy provozu PKI. Výše poplatku bude vypočtena jako podíl na vzniklých nákladech a rozdělena mezi uživatele služby PKI.	• ŘSD ČR poskytuje informace z NDIC veřejným subjektům bezúplatně, tyto subjekty mají za povinnost je šířit zdarma. V případě vytvoření služby s přidanou hodnotou je možné službu zpoplatnit.

⇒ Základním kritériem pro rozhodnutí o variantách je rozhodnutí o míře podpory C-ITS v ČR. Variantou bezúplatné služby dostupné pro všechny uživatele stát stimuluje další rozvoj C-ITS systémů v ČR.

⇒ Pro iniciační fázi provozu PKI (např. 5 let) lze doporučit bezúplatné poskytování PKI, případně podíl na financování ze strany uživatelů ve výši provozních nákladů PKI.

Deloitte.