C-ROADS CZECH REPUBLIC
MEMBER OF C-ROADS PLATFORM

Co-financed by the European Union
Connecting Europe Facility

C-ROADS Czech Republic
PKI v C-ITS implementaci

Miloslav Pavelka/ O2 Czech Republic / Teska Labs / C-ROADS Czech Republic /
5.11.2019

C-ROADS Czech Republic

- Projekt zaměřený na implementaci kooperativních ITS systémů (C-ITS) na pozemních komunikacích a ve městech (V2V a V2I komunikace)
- Projekty C-ITS v 18 dalších evropských zemích - C-ROADS Platform
- V ČR funguje plně „hybridní“ řešení – ITS G5 (DSRC) + GSM/LTE

C-ROADS Czech Republic

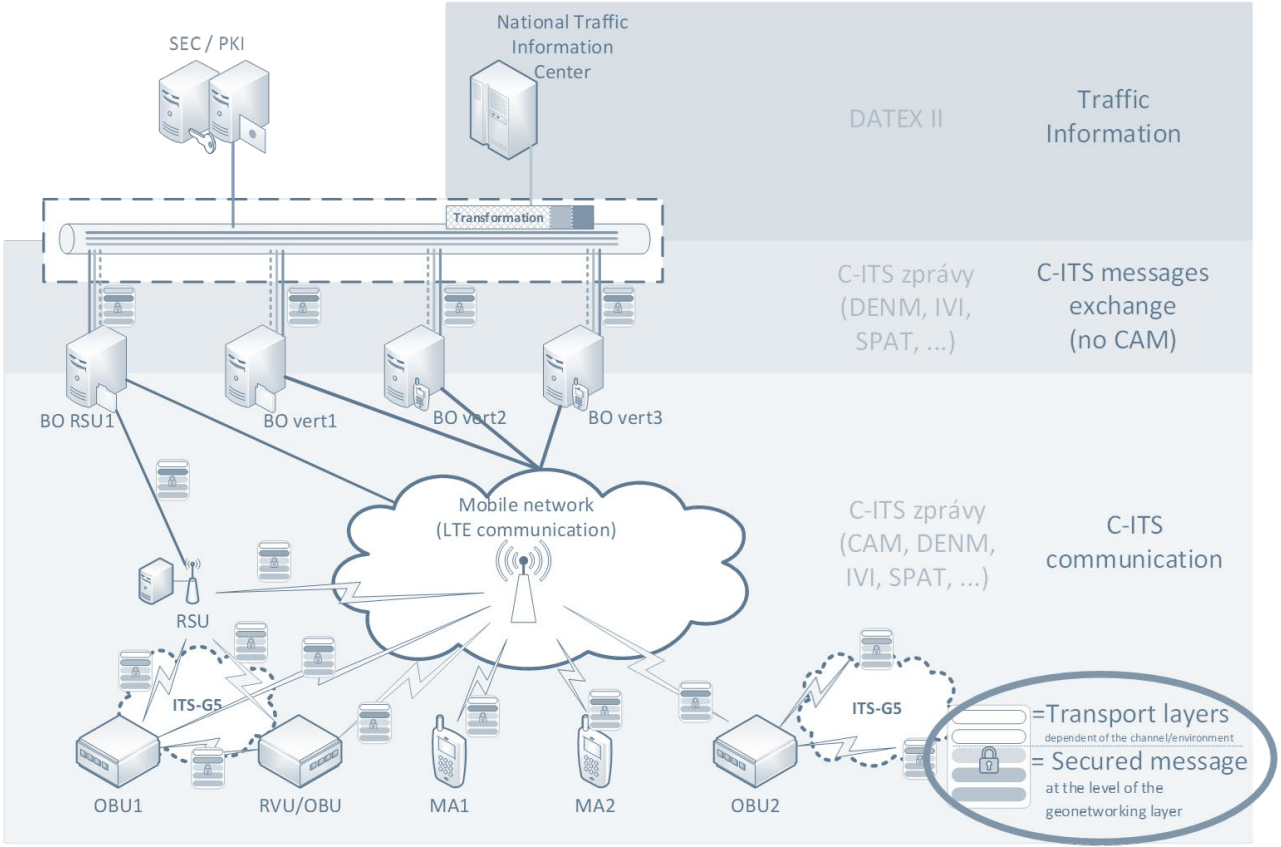
Ministerstvo dopravy

ŘEDITELSTVÍ SILNIC A DÁLNIC ČR

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Plzeňské městské dopravní podniky, a.s.

C-ROADS Czech Republic - hybridní architektura

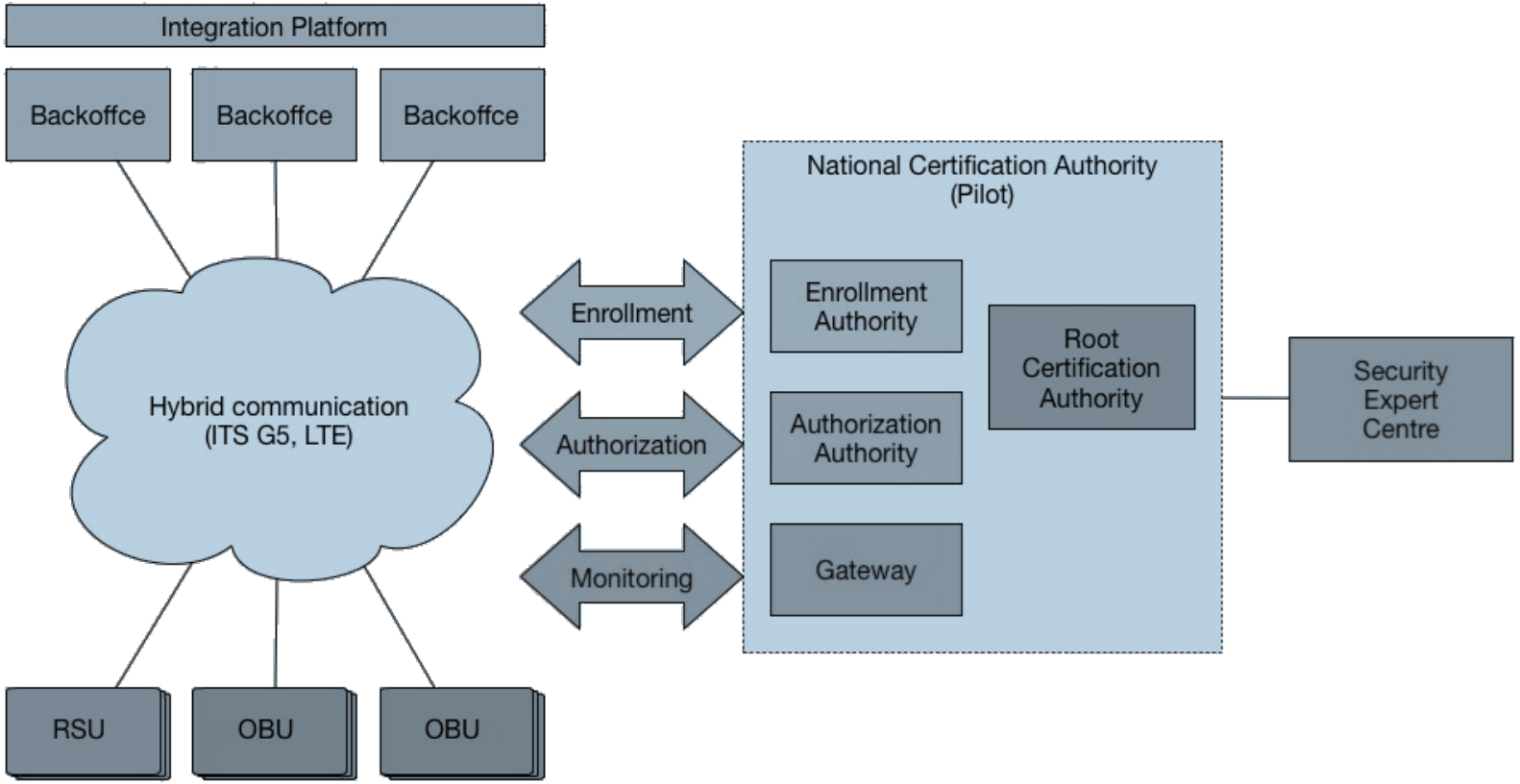


C-ROADS CZECH REPUBLIC
MEMBER OF C-ROADS PLATFORM

Co-financed by the European Union
Connecting Europe Facility

PKI v C-ITS

PKI v C-ITS


Integration Platform
Backoffce
Backoffce
Backoffce
Hybrid communication
(ITS G5, LTE)
RSU
OBU
OBU
Enrollment
Authorization
Monitoring
National Certification Authority
(Pilot)
Enrollment
Authority
Authorization
Authority
Gateway
Root
Certification
Authority
Security
Expert
Centre

PKI – interoperabilní implementace

- Podpora RootCA a všech procesů dle:
  - TS 103097 v1.2.1
  - **TS 103097 v1.3.1**
- Využívání centrálních komponent - TLM a CPOC pro zajištění interoperability v rámci celé EU C-ROADS Platform

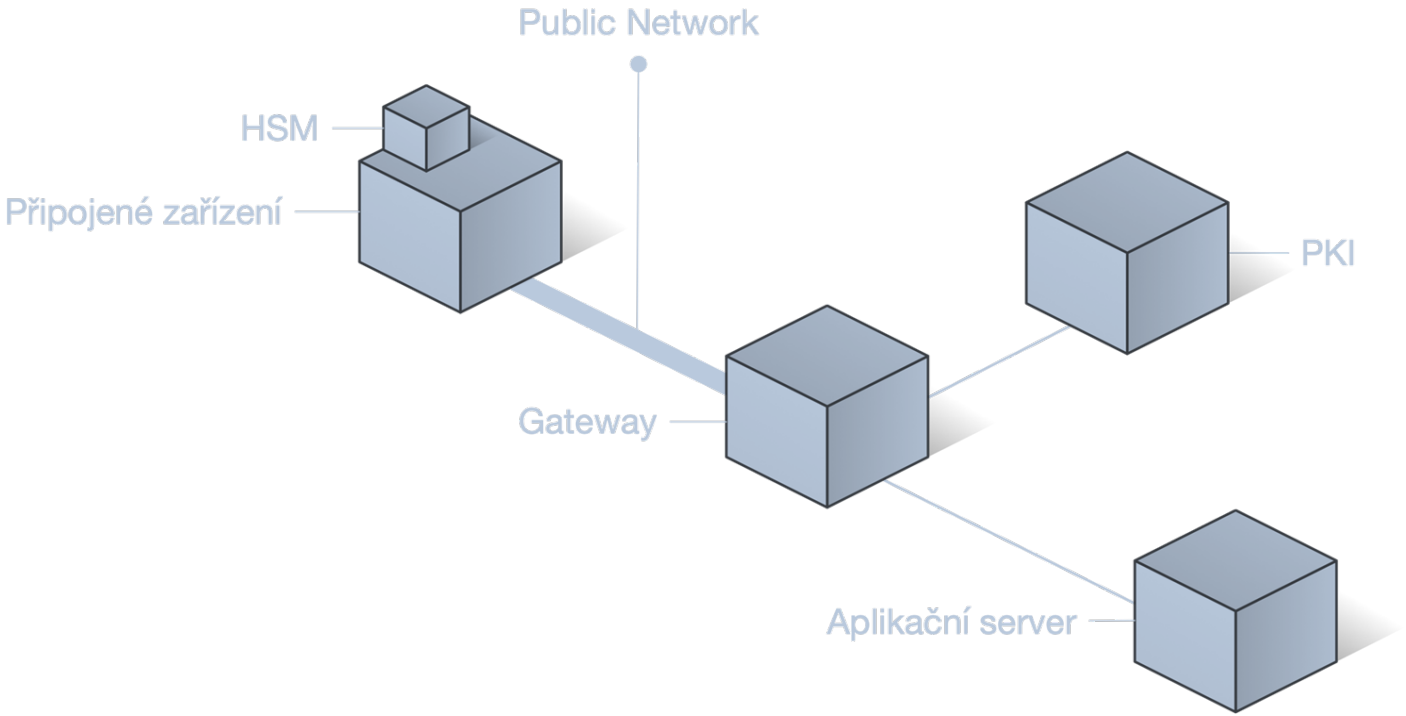
C-ROADS CZECH REPUBLIC
MEMBER OF C-ROADS PLATFORM

Co-financed by the European Union
Connecting Europe Facility

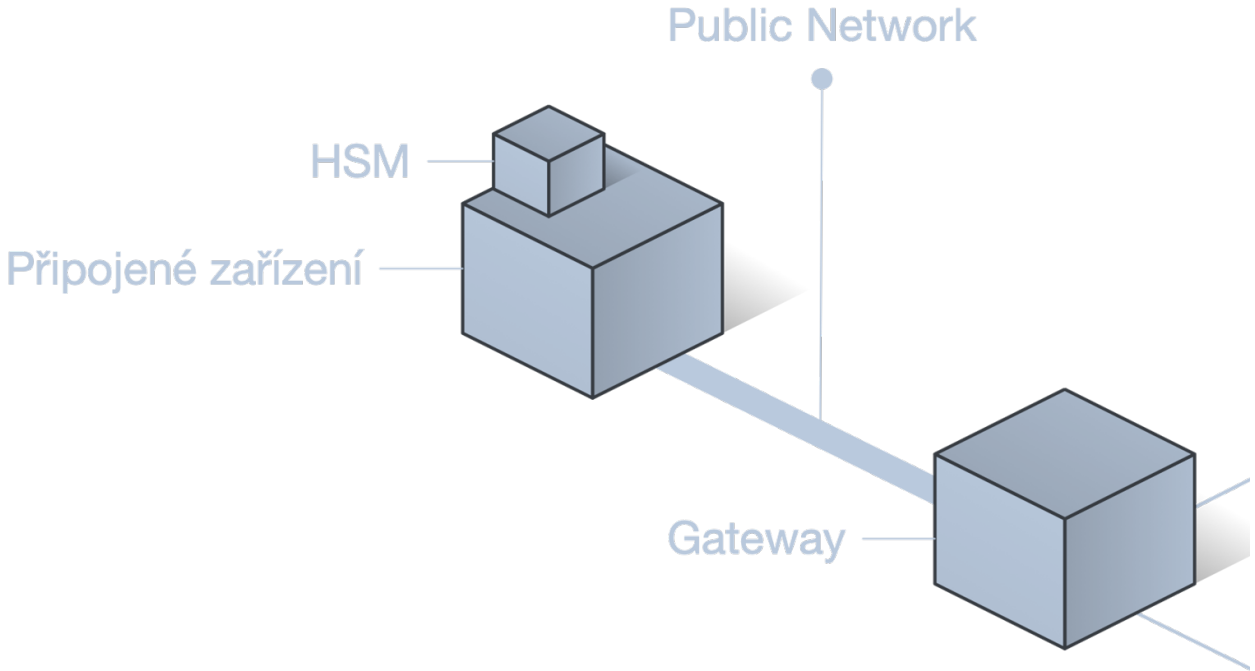
C-ROADS řeší:

- Distribuované aplikace
- Propojená zařízení

Typická architektura distribuované aplikace

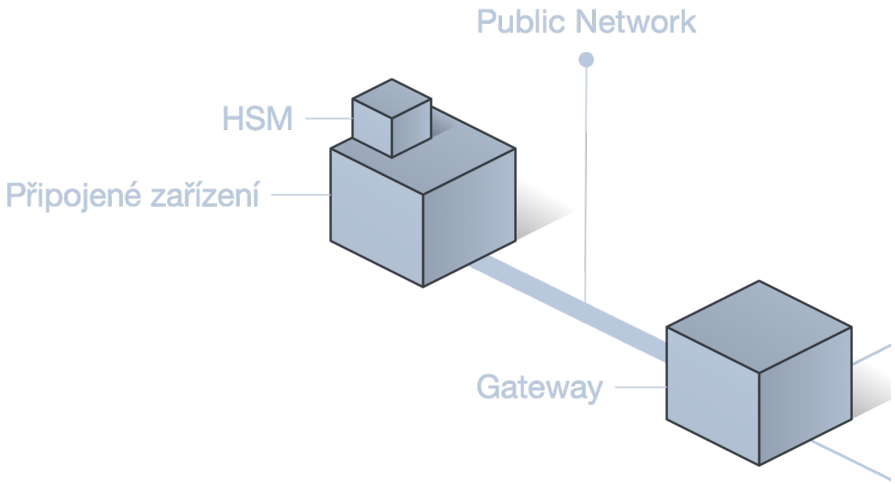


Man-in-the-Middle attack



Útočník chce odposlouchávat a případně i měnit komunikaci.

Vzájemná TLS autentizace

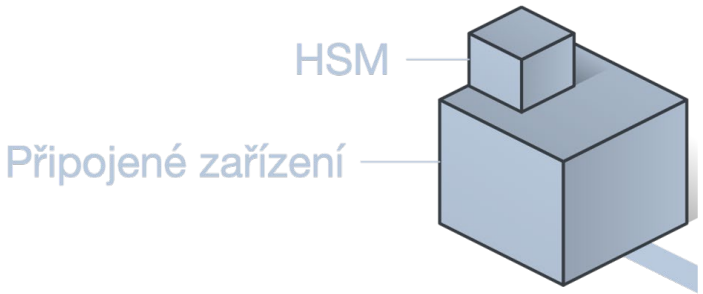


- Komunikace pouze mezi důvěryhodnými stranami

- Brání proti odposlechu
- Brání proti předstírání identity
- Brání proti změnám komunikace

- Ochrana na úrovni VPN
- Bezpečná komunikace ve veřejné síti

HSM = Hardware Security Module

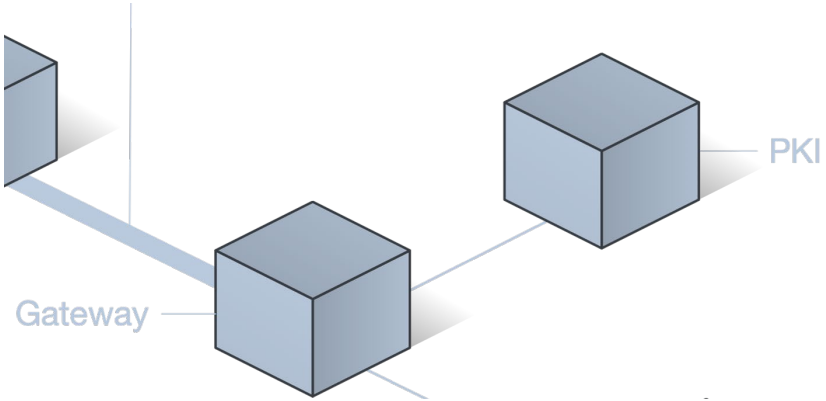


- Bezpečné úložiště privátního klíče
- Privátní klíč je generován v HSM
- Privátní klíč nelze z HSM vyextrahovat a přečíst

- Nepřenosná, silná identita
- Víte, kde máte svoje klíče (na rozdíl od SW klíčů)
- Nezbytná komponenta v ochraně kritických systémů

- PKCS#11

PKI = Public Key Infrastructure



- Certifikační autorita
- Zdroj “důvěry“ pro distribuovanou aplikaci

- Řízení oprávnění k přístupu
- White-listing

- Důvěrnost (Confidentiality)
- Integrita (Integrity)
- Autentičnost
- Nepopiratelnost (Non-repudiation)

Registrace nového zařízení

- Proces vyjádření důvěry

- Certificate Signing Request (CSR)
- Enrollment
- Onboarding

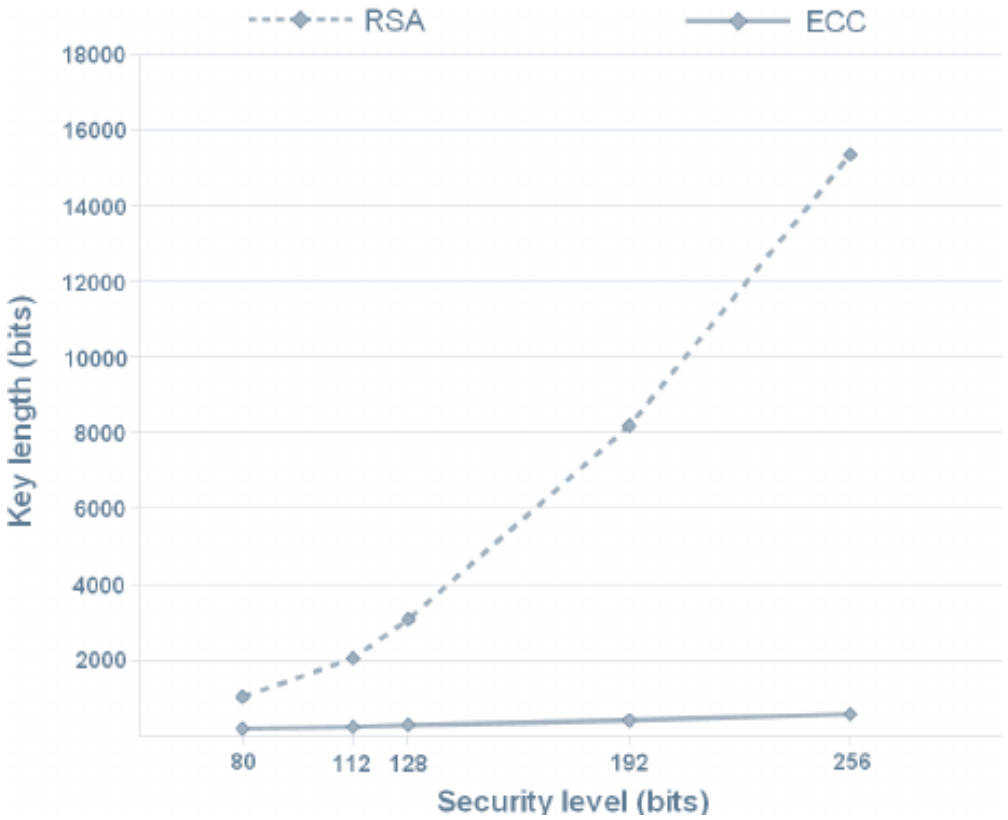
Automatické prodlužování platnosti certifikátů

- Nezbytná vlastnost pro snadný provoz velké flotily zařízení
- např. C-ITS certifikát má trvanlivost 7 dní

Revokace vydaných certifkátů

- Reakce na bezpečnostní incident jako např. odcizení zařízení nebo neplánovaný odchod zaměstnance z organizace
- Revokace není expirace

Jaký algoritmus zvolit? RSA nebo ECC?



Monitoring

- Log Management
- SIEM

- Detekují se neobvyklé komunikační vzory.
- Připojená zařízení komunikují velmi šablonovitě, útočník má velmi odlišný vzor chování.

Vaše otázky?

Miloslav Pavelka
O2 Czech Republic / Teska Labs

miloslav.pavelka@teskalabs.com
+420 776 008 228

Děkuji za pozornost.

C-ROADS CZECH REPUBLIC
MEMBER OF C-ROADS PLATFORM