V2X PKI
BY microsec

V2X-PKI

üzenethitelesítés az intelligens közlekedésben

A közlekedésbiztonság fejlődése

- A balesetek döntő többsége a sofőrön múlik
- Megjelent számos passzív és aktív eszköz
- A modern járművek szenzorainak viszonylag korlátozott az alkalmazhatósága
- Vezeték nélküli kommunikációs technológia

Kooperatív járműkommunikáció alapvető céljai:

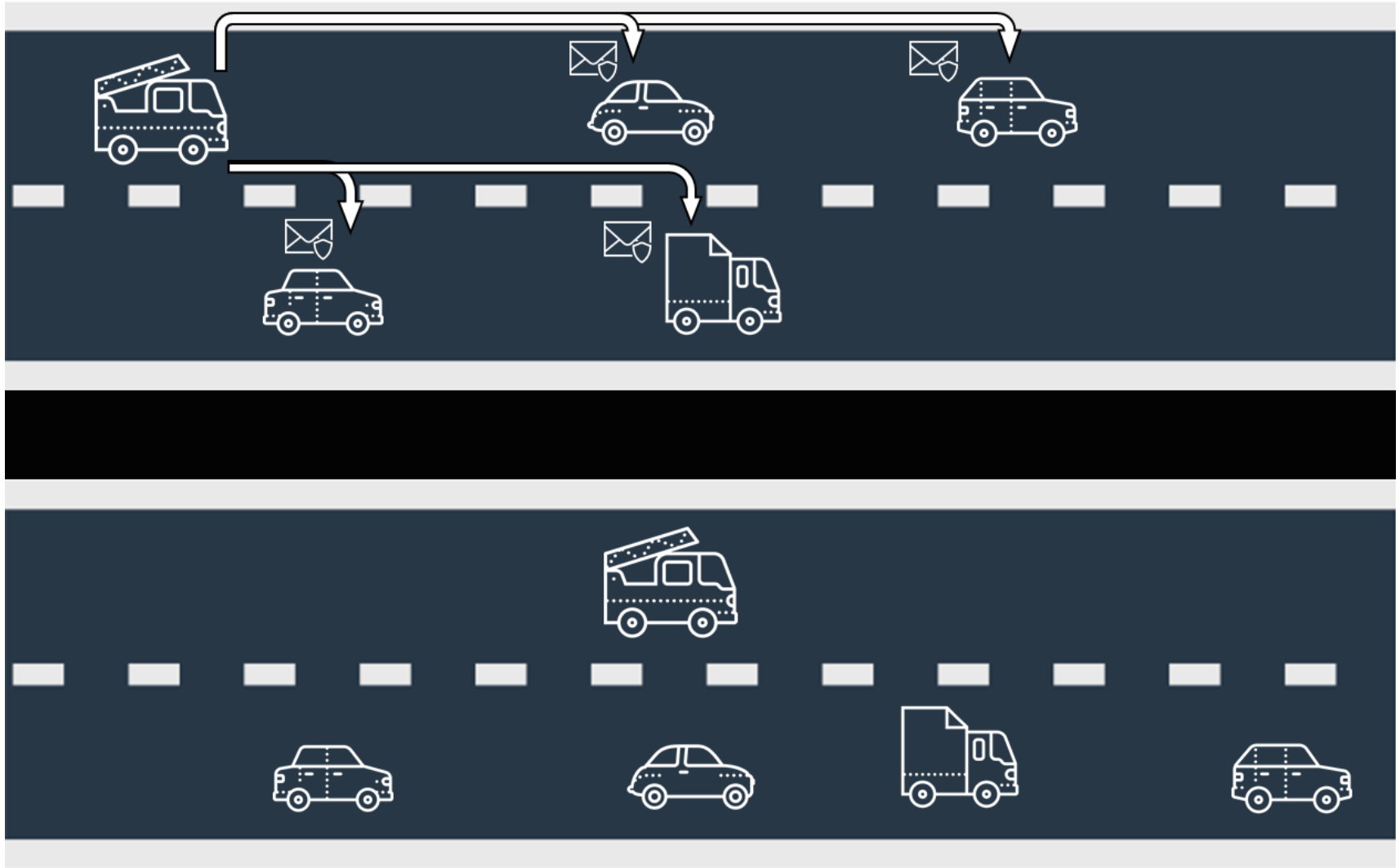
- balesetek számának csökkentése
- jármű forgalom optimalizálása, dugók elkerülése
- CO2 kibocsátás csökkentése
- az önvezető autók számára lehetőség a kooperatív közlekedés biztosítására

Mi a C-ITS és mi a V2X?

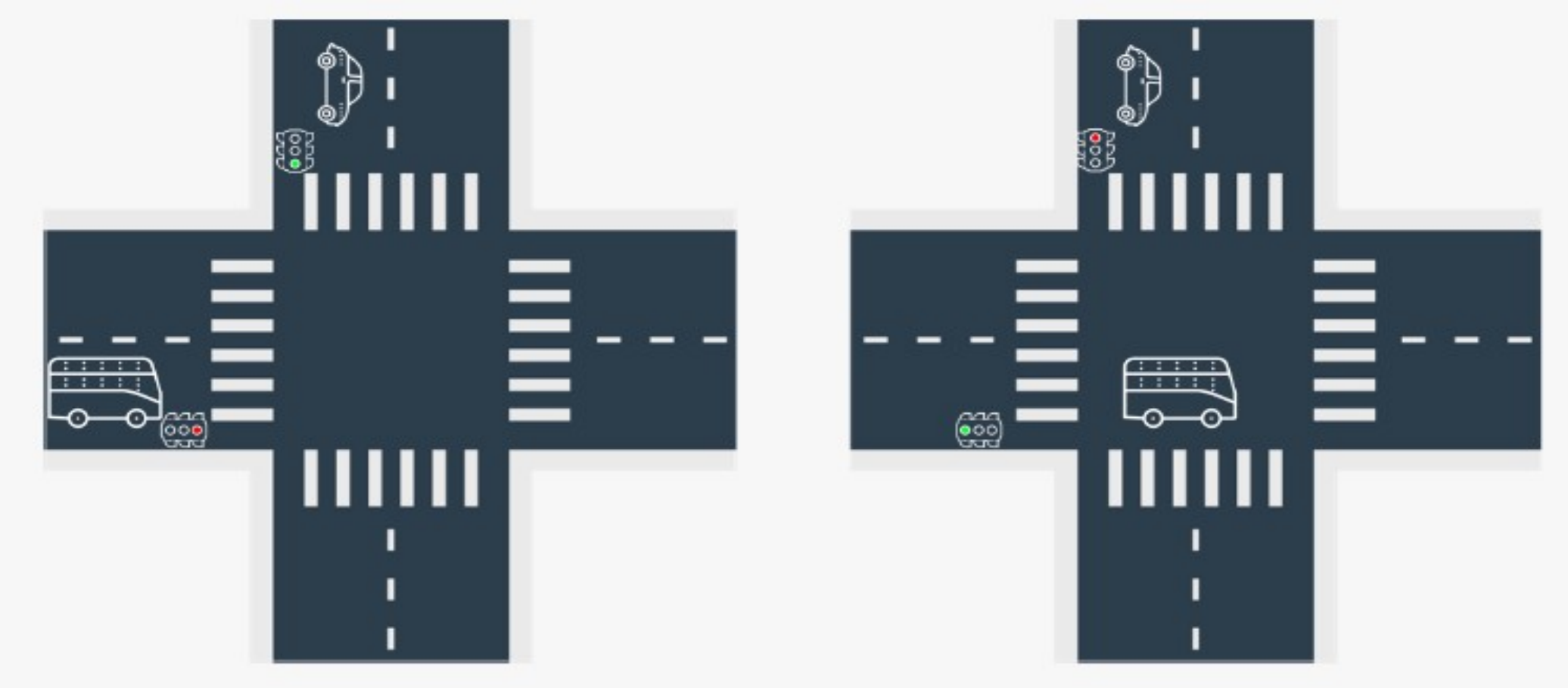
- Kooperatív járműkommunikáció, napjaink egyik lényeges vezetéstámogató rendszere
- Segítségével a közlekedés résztvevői valós időben oszthatnak meg egymással adatokat (pl. sebesség, pozíció, gyorsulás)
- Intelligent Transport System – ITS
- Cooperative Intelligent Transport System – C-ITS
- Vechicle-to-Vechicle – V2V
- Vechicle-to-Infrastucture – V2I
- Vechicle-to-Everything – V2X

Kereszteződés

Tűzoltók vagy mentők



Tömegközlekedés



V2X veszélyforrások, és a megoldás

- DoS támadások
- Szándékos félrevezetés
- Autókról (és a vezetőről) begyűjthető személyes adatok

PKI és digitális tanúsítványok a különböző entitások (pl. jármű) részére, mellyel biztonságos (hiteles, titkosított) üzenetek küldhetők

V2X-PKI különbözőségek

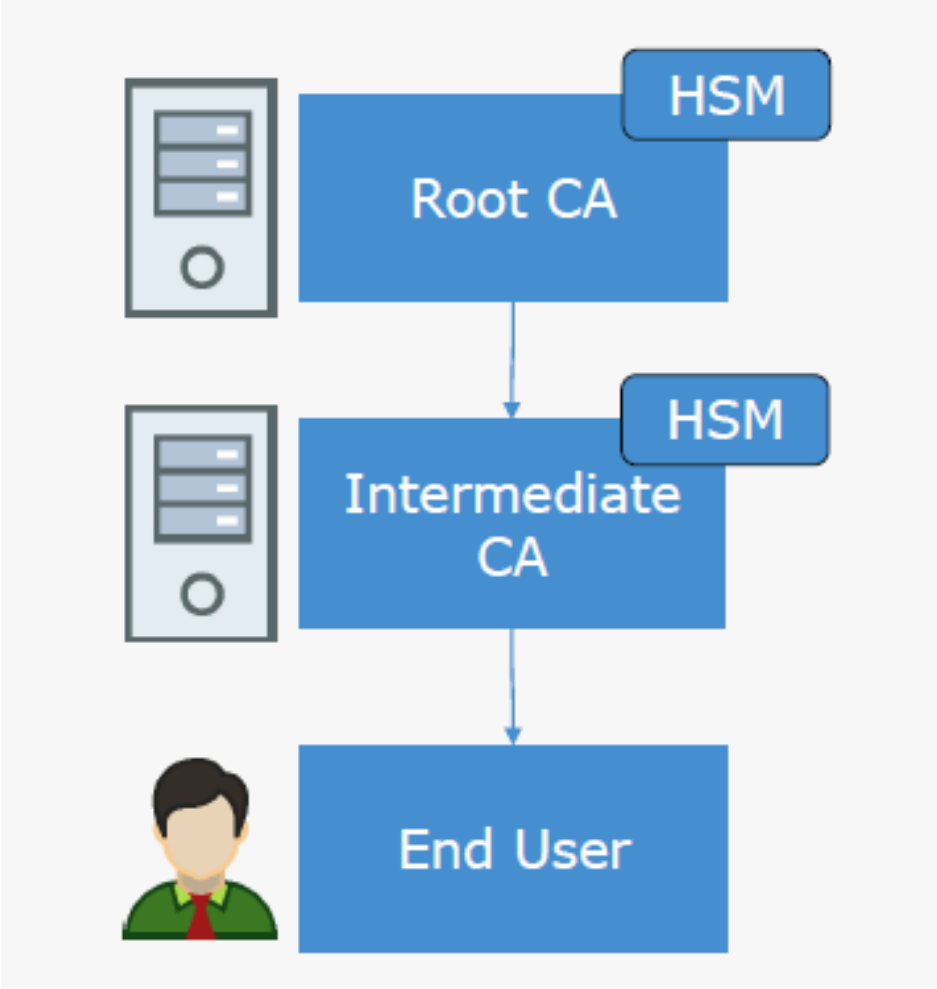
- Privacy
  - anonimitás
  - pszeudonimitás
  - személyhez köthetetlenség
  - megfigyelhetetlenség
- Hozzáférések. Folyamatok

V2X PKI BY microsec

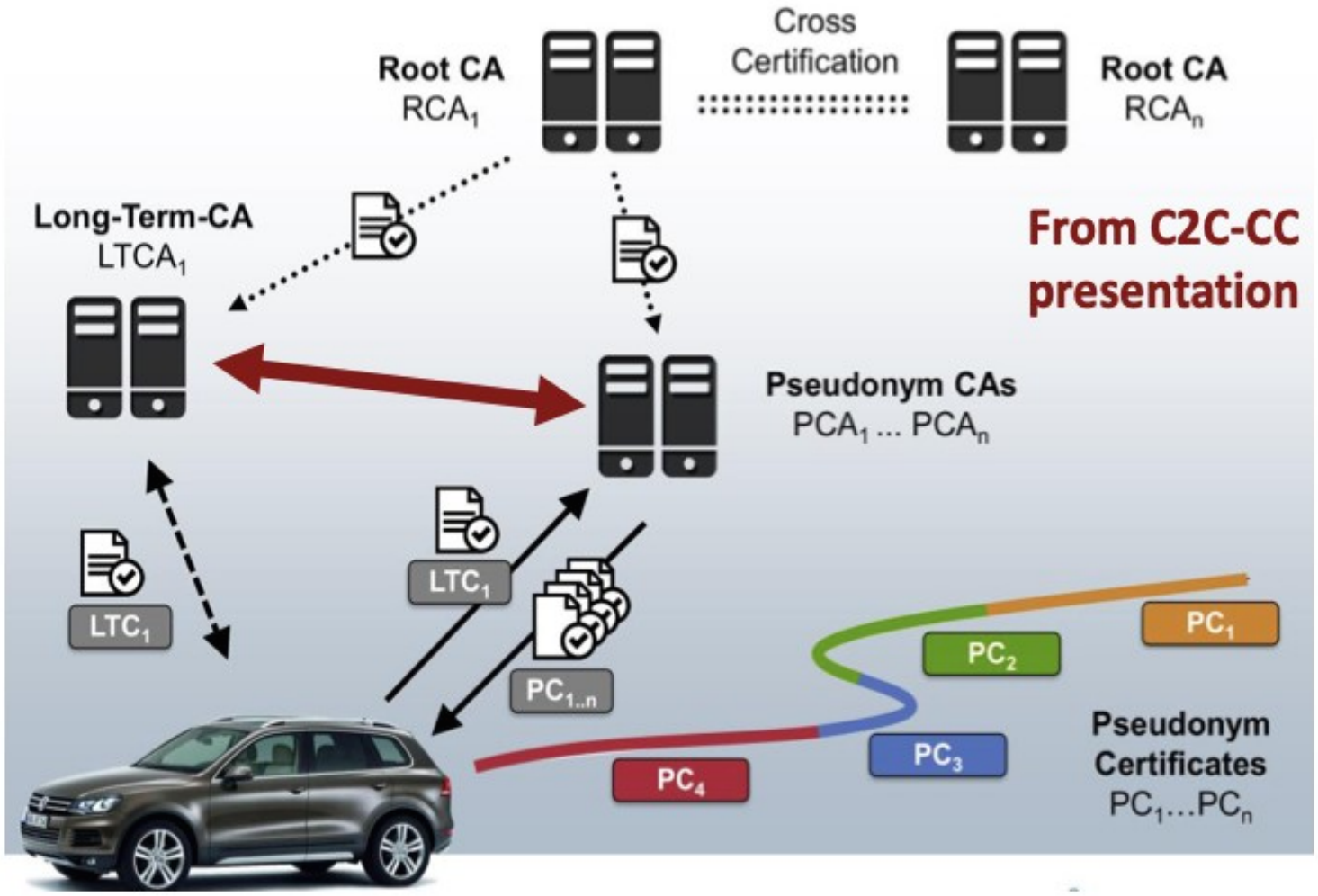
V2X vs X.509

	Standard PKI	eIDAS PKI	C-ITS PKI (EU's ITS standard)
Certificate Format	ITU-T X.509v3, IETF RFC 5280 and RFC 6818	ITU-T X.509v3, IETF RFC 5280 and RFC 6818	IEEE Std 1609.2
Certificate extensions and profiles	ITU-T X.509v3	ITU-T X.509v3, ETSI EN 319 412-5	ETSI TS 103 097
Certificate Request Protocols	PKCS#10	PKCS#10	ETSI TS 102 941
Anonymity/Pseudonymity (Trust Model)	No	No	Yes
Separation of duties between CAs	No	No	Yes
Trusted List Manager (levels)	No (RA/OCSP for certificates)	No (RA/OCSP for certificates)	Yes
Encoding	PEM,DER,CRT, CER	PEM,DER,CRT, CER	COER ITU-T X.696
Revocation information	YES (ITU-T X.509v2 CRL distribution)	YES (ITU-T X.509v2 CRL distribution)	YES for Enrolment CAs, Not allowed for Authorisation CAs
Typical Certificate Volume	standard	Middle	Extremely high
High Availability & Geo-redundancy requirement	standard	Middle	Extremely high
Typical Performance requirement	standard	Middle	Extremely high
Typical Algorithm	RSA (ECDSA)	RSA or ECDSA	ECDSA/ECIES

Egy „klasszikus” PKI hierarchia



Általános V2X PKI felépítés



EU CCMS PKI hierarchia 1/2

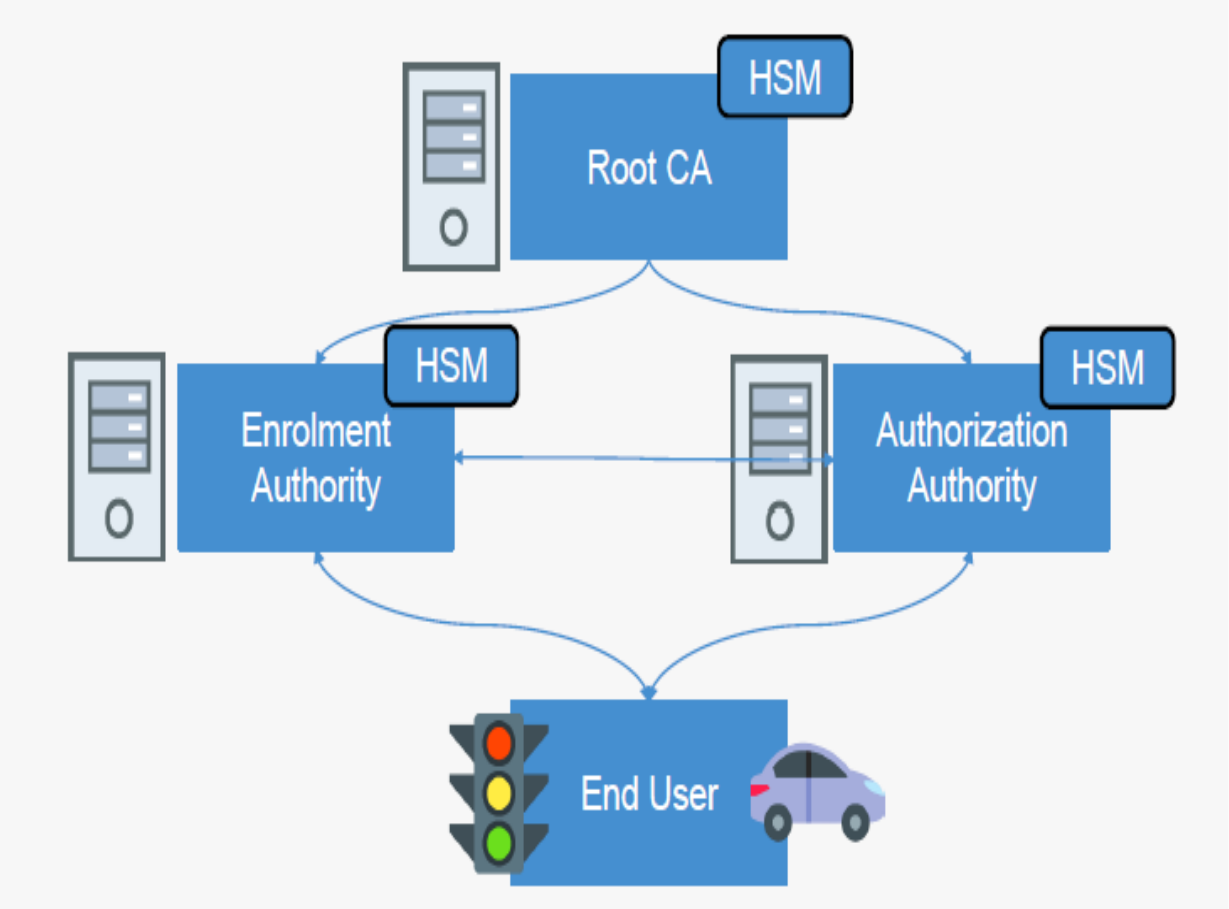
CCMS - C-ITS Certificate Management System

Root CA

- Off-line CA
- SubCA-k hitelesítése
- CRL és CTL kiadása

Enrolment Authority

- End User menedzsment
  - Egyedi azonosító (Canonical ID) és publikus kulcs
  - Regisztráció
  - Engedélyek
- Enrolment Credential (EC) kiadása
- On-line CA
  - EC request
  - AuthorizationValidationRequest/ Response



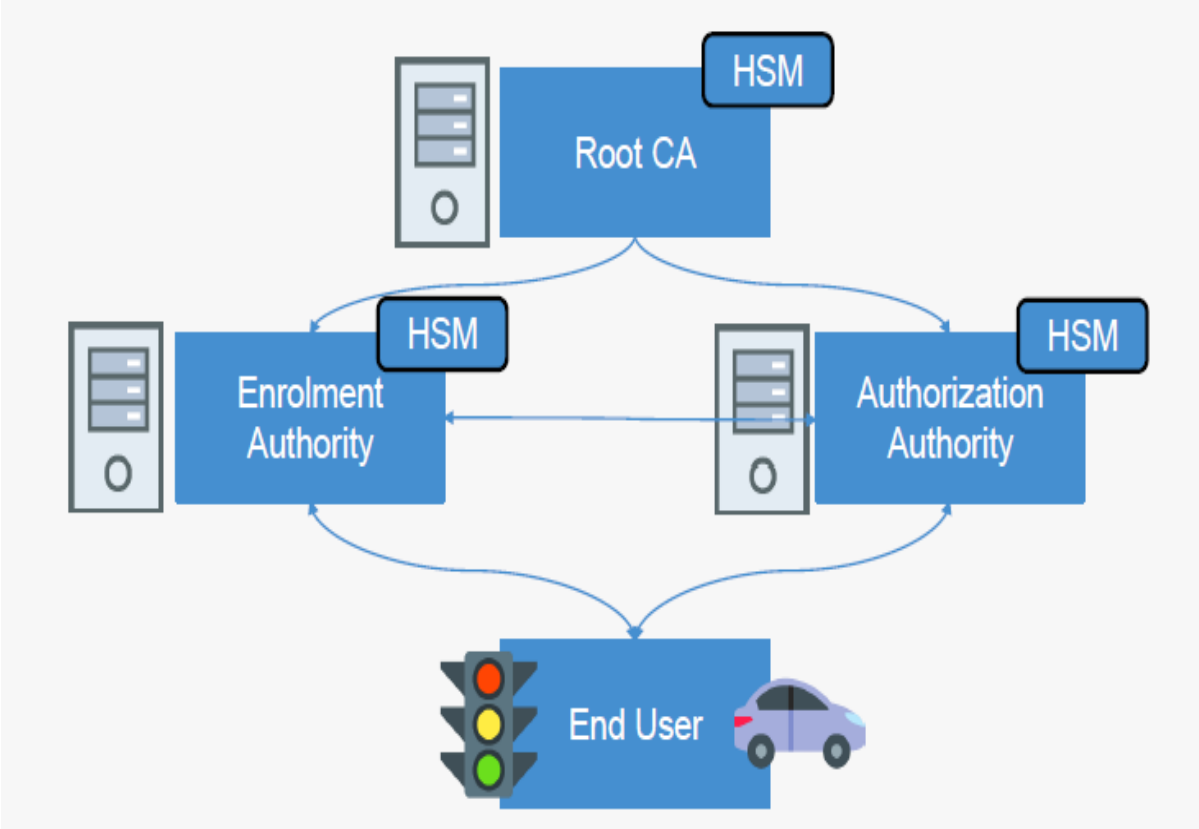
EU CCMS PKI hierarchia 2/2

Authorization Authority

- Authorization Ticket (AT) kiadása
- On-line CA
  - AT request
  - AuthValRequest/Response

End User (C-ITS Stations) – Ügyféloldal

- Típusok:
  - Fix stations (RSU – Road side unit)
  - Mobile stations (OBU – On-board unit)
- Teendők:
  - Regisztráció az Enrolment Authority-nál
  - EC Request / AT Request



A bizalom forrása EU CCMS-ben

Hierarchia csúcsán levő szereplők:

- (EU) C-ITS Policy Authority
- (EU) TLM
- (EU) CPOC
- https://cpoc.jrc.ec.europa.eu/

Trust List Manager (TLM):

- Offline CA, self-signed
- ECTL aláírása

Bizalmi szintek:

- ECTL Level 2
- ECTL Level 1
- ECTL Level 0

CPOC:

- TLM tanúsítvány és ECTL publikálása

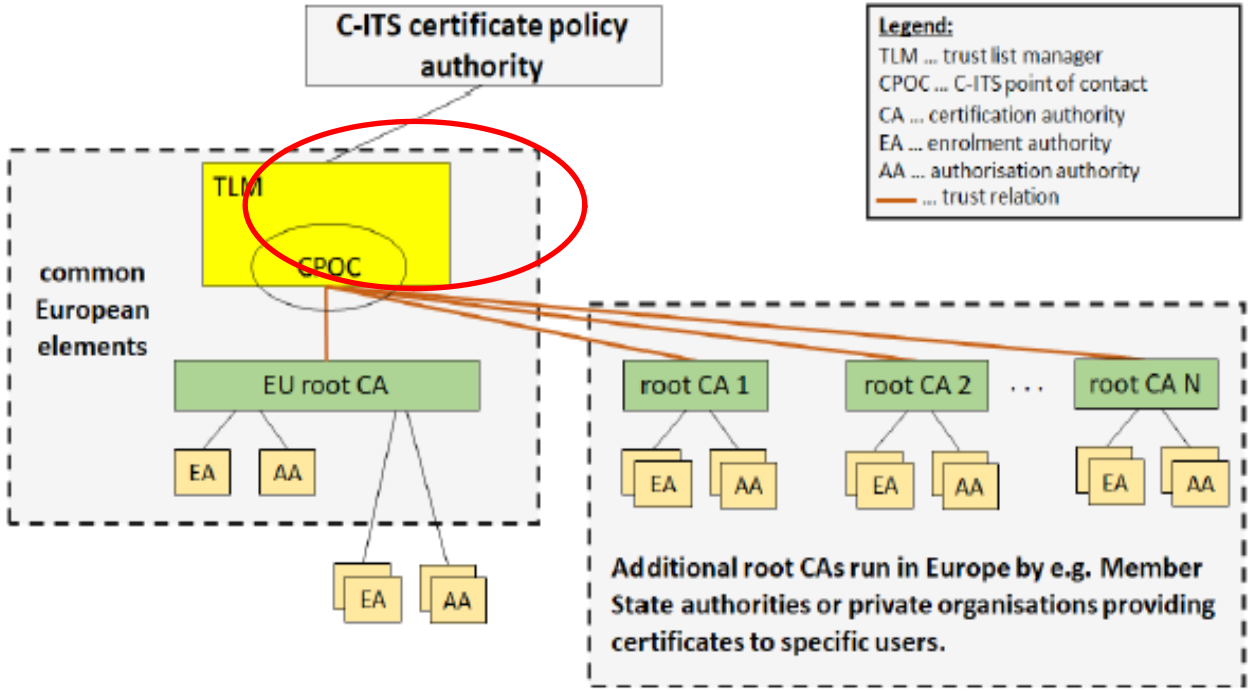


Figure 1: C-ITS trust model architecture

Megjegyzés: nincs még CPA, TLM/CPOC/ECTL sincs L1-L2 szinten

SCMS - V2X PKI Amerikában

SCMS - Security Credential Management System
Részben eltérő komponensek:

- SCMS Manager
- Root CA mellett van Intermediate CA is
- ECA (Enrolment CA)
- ACA (Authorisation CA)
- Registration Authority
- Linkage Authority

Főbb jellemzők:

- Robusztus architektúra
- Implicit tanúsítványok

Szabványok:

- IEEE1609.2
- IEEE1609.2.1

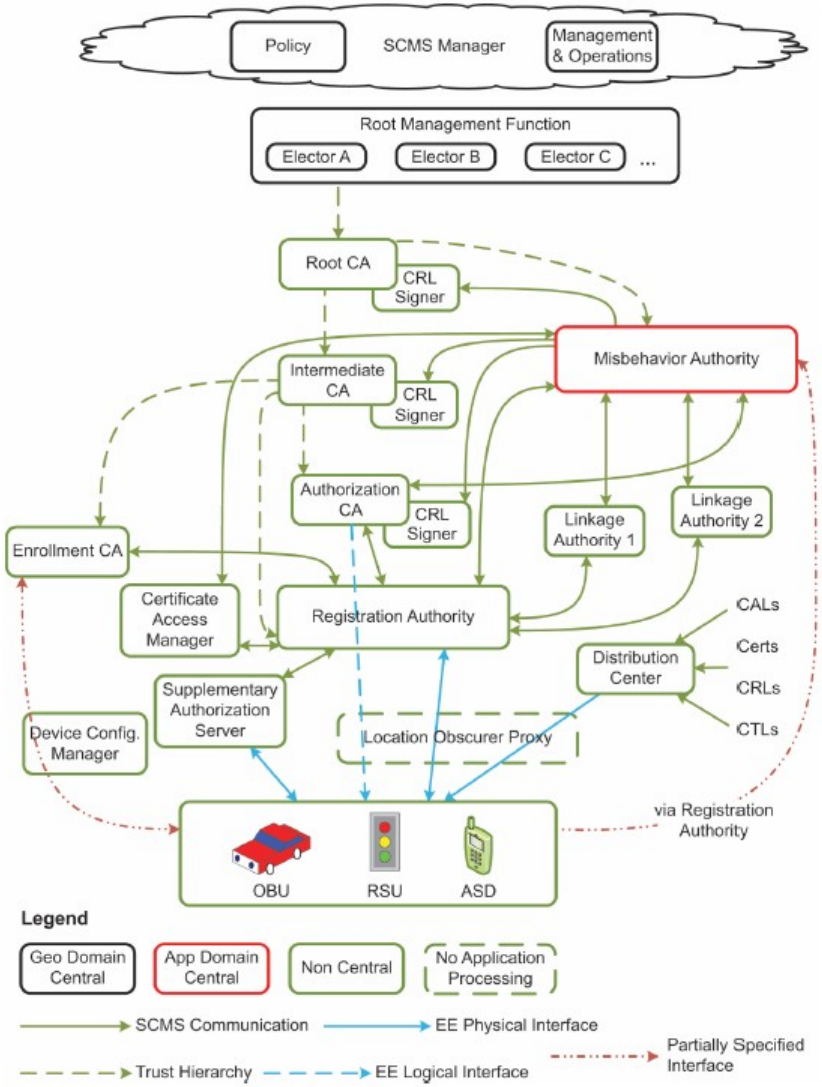


Figure 1—Conceptual SCMS architecture

Hol tartunk

- Európai Unióban elindultak már pilot projektek, köztük van éles szolgáltatás is:
  - Autobahn – Microsec
- Nemzetközi szervezeteken aktív részvétel
- Elindítottuk a READY programunkat
- C-Roads nagyon aktív
  - Magyarországon is foglalkoznak már a PKI-val
  - https://www.c-roads.eu/platform.html

V2X PKI BY microsec

Köszönöm a figyelmet!