

CONCORDA

Cyber Security

Omar Alshabibi
Senior Product Manager
ESCRYPT

Email: Omar.Alshabibi@escrypt.com

Connected Corridor For Driving Automation

Organised by



Co - Organised by



Supported by



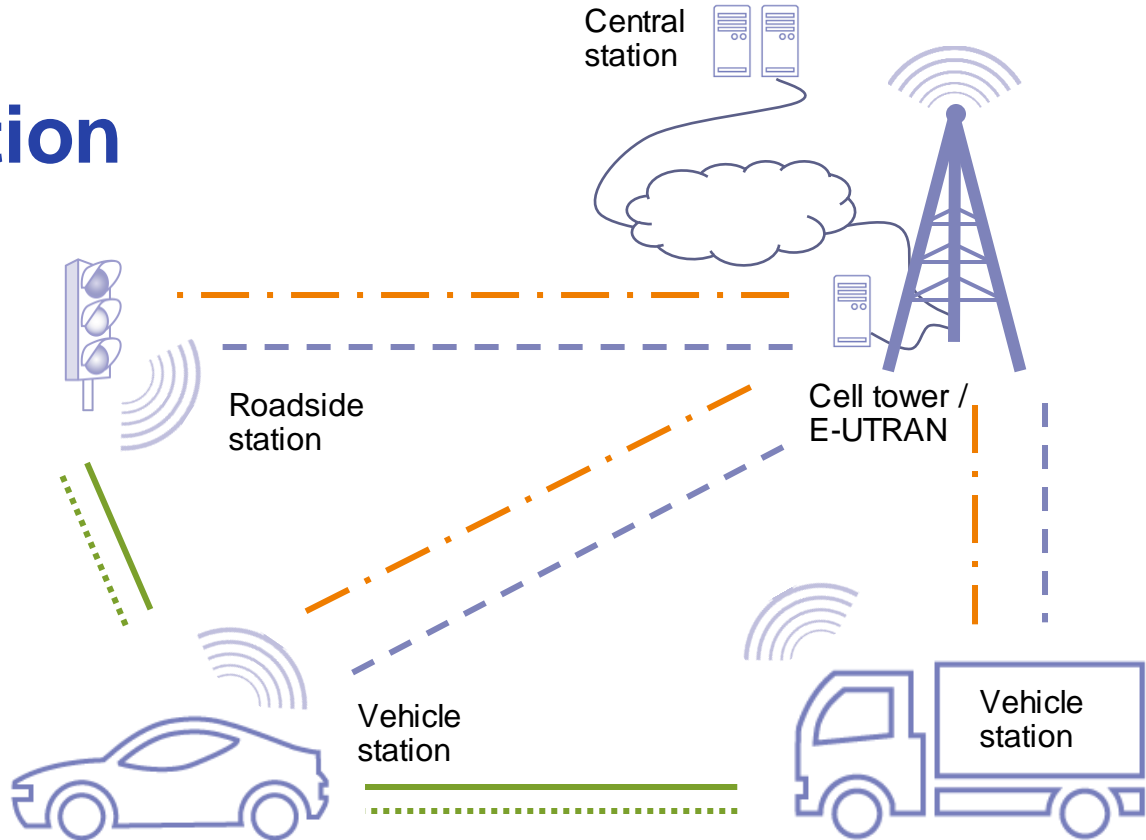
Federal Ministry
of Transport and
Digital Infrastructure

Hosted by



CONCORDA – V2X Communication

- ITS-G5 (short-range)
- ⋯ C-V2X autonomous (PC5, short-range)
- - - MEC-based Uu interface
- . - Cellular Uu interface (LTE, 5G, long-range)



Organised by



Co - Organised by



Supported by



Hosted by



CONCORDA – V2X Cyber Security

Short-range communication security based on digital signature with ETSI certificates (TS 103 097 v1.3.1)

- ITS-G5 secured with ETSI signature
- - - C-V2X secured with ETSI signature



Long-range communication security not finally specified

- . - . Uu interface secured with Transport Layer Security (TLS) with X.509 certificates used in the handshake for mutual authentication



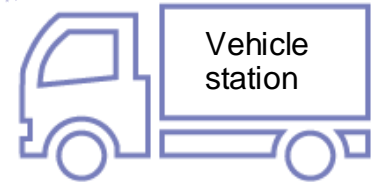
Optionally, signing of V2X messages with ETSI certificate



TLS (+ ETSI signature)



ETSI signature



Vehicle station

Central station



TLS (+ ETSI sig.)



Cell tower / E-UTRAN



Organised by



Co - Organised by



Supported by

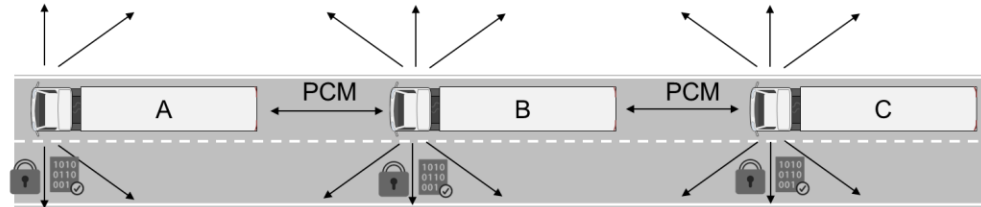


Hosted by



CONCORDA / ENSEMBLE – Platoon Cyber Security

escrypt
SECURITY. TRUST. SUCCESS.



- Authenticated joining of platoon with signed Platoon Management Message (PMM) using ETSI certificates (TS 103 097 v1.3.1) of PKI
- Signed and encrypted platoon communication with Platoon Control Message (PCM) using ETSI certificates
- Period change of symmetric encryption group key to preserve privacy and ensure that leavers of the platoon are excluded

Organised by



Co - Organised by



Supported by



Hosted by



CONCORDA / ENSEMBLE – V2X Cyber Security – PKI



- PKI with certificate type ETSI operated by ESCRYPT with root certificates listed on L0 ECTL
 - 11 companies registered at PKI as operator of C-ITS stations
 - 13715 ITS Stations registered at PKI
 - Migration of root certificate including root linking on ECTL in November 2020 to extend the PKI lifetime
 - High availability of PKI in the two years of operation
- PKI with certificate type X.509 operated by ESCRYPT to secure TLS

Organised by



Co - Organised by



Supported by



Hosted by



GET IN TOUCH

Omar Alshabibi
Senior Product Manager
ESCRYPT

Email: Omar.Alshabibi@escrypt.com

Organised by



Co - Organised by



Supported by



Federal Ministry
of Transport and
Digital Infrastructure

Hosted by

