ITS SECURITY FRAMEWORK & STANDARDS DEVELOPMENT IN ETSI BASED ON SUCCESSIVE THREAT, VULNERABILITY AND RISK ANALYSIS (TVRA) ITERATIONS

Workshop CyberSec, ITSC 2020, 20-23. September 2020
Brigitte Lonc, RENAULT

Table of contents

INTRODUCTION:
COOPERATIVE ITS STANDARDISATION IN ETSI

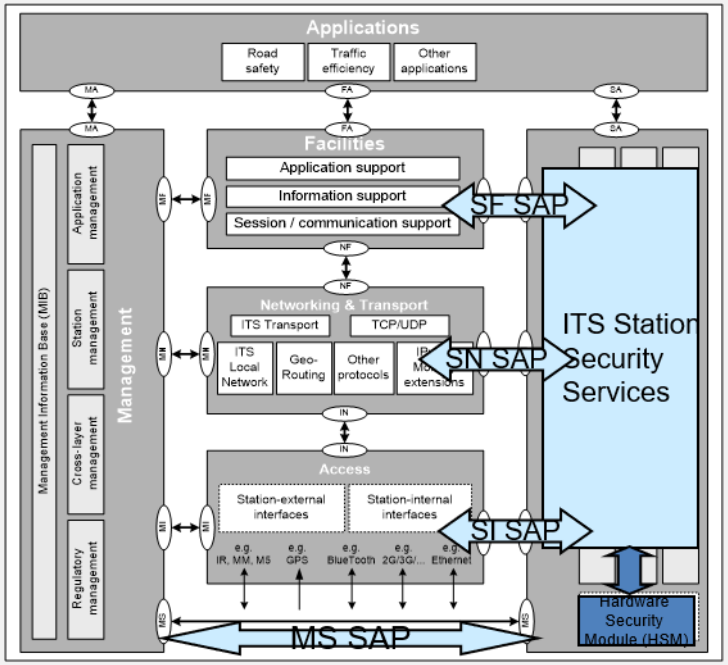
WHAT IS COOPERATIVE ITS ?

- 5.875 – 5.935 GHz allocated by EU to ITS road + urban rail (below 5.915 GHz ITS road safety & 5.915 GHz-5.935 GHz frequency band priority to Urban Rail)
- C-ITS use short-range radio technologies and cellular communications 3G/LTE, 5G

- **Short-range communication features**
  - Quick medium access (low latency)
  - Allocation of frequencies to ITS safety (high reliability)
  - Ad hoc communication (no need for an infrastructure)
  - 200-800 m com range (extended vehicle sensor for driving assistance & automated vehicles
- **Day1 services for road safety, traffic management and sustainability are under deployment in EU**
  - Validation and pre-deployment projects: **SCOOP@F, CORRIDOR, C-ROADS platform**
  - Standards profile specification and coordination V2V / V2I: **Car2Car Communication Consortium, C-ROADS**
  - **C-ITS Deployment Group** is committed to Day 1 deployment using ITS-G5/ 802.11p
- **New C-ITS services (Day2 and Beyond)**
  - Considering various automation levels in CAVs

GROUPE RENAULT

ETSI ITS ARCHITECTURE
SECURITY ARCHITECTURE



- **Security processing services**
  - Sign & verify Message, Encrypt & Decrypt data, manage security association (SA)
- **Security management services**
  - Enrolment, Authorization, Identity management, report misbehaviour
- **External communications protection**
  - Detection of misbehaving ITS-Ss
  - IDS, IPS, firewall
- **HSM requirements**
  - Secure key storage
  - Heavy computational operations (crypto)
  - Trusted and authenticated communication channel (interface with host)

ETSI TC ITS WG5 security and privacy by design

- **In ETSI TC ITS, WG5 deals with security, privacy and data protection aspects in ITS.**

- **WG5 followed a 3 steps process to develop security standards**

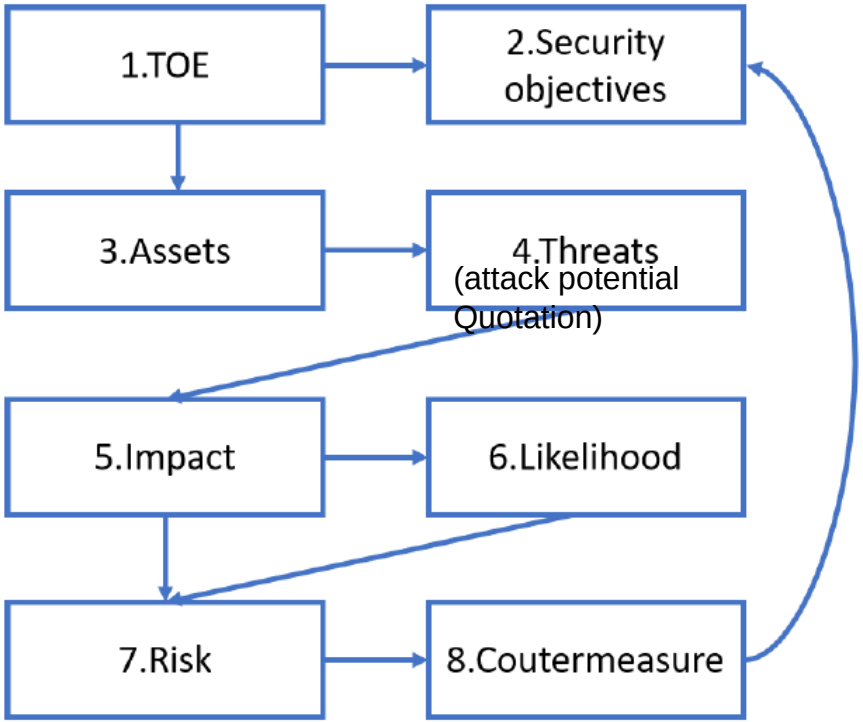
Step 1: Identify and catalogue ITS security risks using the TVRA approach

Step 2: Build security requirements and define a list of potential countermeasures (generic security services)

Step 3: specify an architecture and a standardized set of services and interfaces that enable implementation of secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications

ETSI TVRA APPROACH FOR C-ITS (DAY 1 USE CASES)

THREAT VULNERABILITIES RISK ASSESSMENT - METHOD OVERVIEW



TVRA is a "Standard" risk analysis method

- ETSI TS 102 165 -1 (2017-10): "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability and Risk Analysis (TVRA)"

TVRA aims at identifying assets, establishing their weaknesses, analyzing threats (assess how practical are attacks on these weaknesses) and estimate the resulting risk

TVRA output is a list of countermeasures

Security goals defined in ETSI TVRA

- **Security goals defined in TVRA are basically scoping on “C-I-A” (Confidentiality-Integrity-Availability)**

- **TVRA is considering 5 security objectives listed in TS 102 165-1**
  - Confidentiality, Integrity, Availability, Authenticity and Accountability

- **It is basically adapted to security risk assessment of communications systems (ITSEC)**

TVRA METHOD FOR THREATS/ATTACKS ANALYSIS & RISK EVALUATION

- **For each step, metrics are specified to assist the users**
  - Asset impact: level of harm caused by an attack on the system asset
  - Attack quotation methodology (assess the practically of threats to the system)
  - *Threat level (added in the recent version of the standard) :*
    - *evaluate to which extent a threat agent is motivated and capable to perform attacks*
  - Calculate the likelihood of attacks
  - Assess the impact of the attacks on the system
  - Establish the risk for each of the identified threats

TVRA RISK CALCULATION EXAMPLE

Table G.1: Example row entry in the TVRA risk calculation spreadsheet

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
DoS Denial of access to incoming messages	Time	<= 1 week	0	Enhanced Basic	Likely	High	**Critical**
	Expertise	Proficient	3				
	Knowledge	Restricted	3				
	Opportunity	Easy	1				
	Equipment	Specialized	3				
	Threat level	Moderate	2				
	Asset Impact	High	3				
	Intensity	Single instance	0				

Calculated Attack potential

Combine the motivation and capability of threat agent (attacker)

Combine asset Impact value and Attack intensity

Risk = Likelihood * Impact

ITS TVRA analysis for Day1 use cases

- **ETSI TR 102 893 V1.2.1 (2017-03): "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)"**
- **Consider two categories of end-equipment (TOEs): vehicle ITS-S, Road-side ITS-S**
- **TVRA used to evaluate the difficulty of "generic" attacks on typical categories of E-Es (listed in ETSI 102 893):**
  - Message saturation
  - Jamming of radio signals
  - Injection of false messages
  - Manipulation of ITS messages en route
  - Masquerade as ITS-S (Vehicle or Roadside) or ITS network
  - Injection of a high volume of false emergency vehicle warning messages
  - Replay of "expired" (old) messages
- **At design stage, estimation consists of "average values" for known attacks in the state-of-the-art**
  - not real attacks on existing specification or implementation as in CC evaluations

ITS TVRA – List of countermeasures

11.3.1	Reduce frequency of repeated messages
11.3.2	Include source address in all V2V messages
11.3.3	Limit message traffic to V2I/I2V
11.3.4	Implement frequency agility within the 5,9 GHz band
11.3.20	Implement plausibility validation on incoming information
11.3.8	Include a non cryptographic checksum of the message in each message sent
11.3.12	Include a sequence number in each new message
11.3.17	Software authenticity and integrity are certified before it is installed
11.3.18	Include an authoritative identity in each message and authenticate it.
11.3.15	Encrypt the transmission of personal and private data
11.3.22	Use hardware-based identity and protection of software on an ITS-S
11.3.19	Add an audit log to ITS stations to store the type and content of each message sent /received
11.3.7	Digitally sign each message using a PKI
11.3.18	Use a pseudonym that cannot be linked to the true identity of the user or vehicle
11.3.16	Implement a Privilege Management Infrastructure
11.3.21	Allow remote activation and deactivation of ITS-S
11.3.6	Use 3G as alternative communications path for security management purposes
11.3.13	Use INS or existing dead-reckoning methods (with regular GNSS corrections) to provide position data
11.3.14	Use differential GNSS monitoring to identify unusual changes in position

TVRA Iteration for Release 2 Bring new challenges

- **ETSI TR 102 893 – ITS TVRA is under revision within Release 2**
  - Published version (V1.2.1) is too much focused on short-range wireless communications (ITS-G5 / WiFip)
- **Need to consider hybrid communications combining cellular technology with short range C-ITS communication technology**
- **Need to consider new Cooperative ITS services and their integration in automated vehicles (Day 2 and beyond)**
  - Communication between vehicles, infrastructure and other road users needed to increase the safety of automated vehicles
  - New topics including Collective Perception Service, Cooperative maneuver, Cooperative Adaptive Cruise Control (CACC) and Platooning
  - On-going specifications on C-ITS Vulnerable Road Users (VRU) service

EXTENDED ATTACKS CLASSIFICATION AND SECURITY ASSESSMENT FOR CAVS “CONNECTED AND AUTONOMOUS VEHICLES”

New attacks model and security techniques/countermeasures for CAV

- **Extended attacks model/classification and security measures are needed for new CAV**
- **Need to consider new assets to protect in the Vehicle system**
  - Sensor information system (Perception)
    - Using lidar, cameras, radars for external perception (“Perceived road objects”)
    - sensors data acquisition/measurement
  - Automated Vehicle decision-logic (using AI-based techniques)
    - Including Data fusion, association and tracking …
    - Applications working with many sensor types, communication technologies (short-range, cellular…)
  - Based on various input sources: sensors, V2X short-range communication etc.
- **Address the full security objectives for Connected, Autonomous Vehicles**
  - Not only restricted to ‘standard’ security objectives such as in “C-I-A” TVRA method
  - More focus in Privacy and data trustworthiness goals …

Reference Papers on C-ITS and CAV attacks model & Security Risk Assessment

- R. Moalla, H. Labiod, B. Lonc and N. Simoni, Risk analysis study of ITS communication architecture, *IEEE Network of the Future, NOF 2012*

- Farah Haidar, A. Kaiser, B. Lonc, P. Urien, Risk Analysis on C-ITS pseudonymity aspects, IEEE/IFIP 10th New Technologies, Mobility and Security, NTMS 2019

- Jonathan Petit et al. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR, Black Hat Europe 2015

- Jean-Philippe Monteuuis, Houda Labiod, Jun Zhang, Alain Servel, Stefano Mafrica. Attacker model for Connected and Automated Vehicles. ACM Computer Science in Cars Symposium, CSCS 2018

- ENISA good practices for security of smart cars, Nov. 2019

Types of Attackers

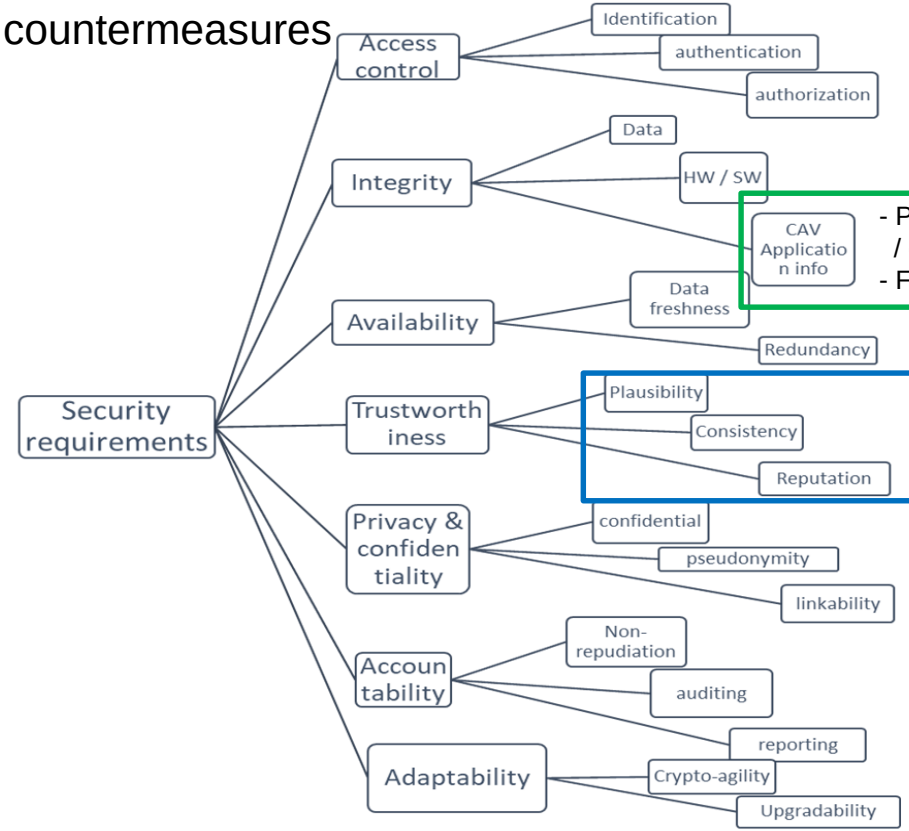
- **Different types of attackers**
  - Insider/outsider
  - Malicious/Rational
  - Local/Extended/Global
  - Active/passive
  - Direct/Indirect
  - Single/multiple e.g. DDoS

ATTACKS CLASSIFICATION ON C-ITS

Traditional Threats to wireless communications	Denial of Service (DoS)	Flooding	maliciously and artificially generating a high volume of false messages	Facilities, network, access
		Spamming	a high volume of messages introduced intentionally to increase the transmission latency and consume network bandwidth	Facilities, network, and access
		Black hole	A node dropping, misrouting or redirecting message	Network
		Malware	introduction of malicious software	Applications, facilities
		Greedy behaviour	Saturation of network by modifying access control or congestion control mechanisms to gain more throughput	Access
		Jamming	create interference on channel transmission	Access
	Manipulation of messages		modification or suppression of message fields (loss of information)	Facilities, network, transport access
	Injection of false message		generate and sending false information on messages	Facilities, network and access
	RF Fingerprinting		distinguish one radio transmitter from another by use of emission profiles	Access
	Masquerade		posing as a legitimate node of the system	Facilities, network access
	Replay		Sending old messages	Facilities, network
	Eavesdropping +data analysis		listen to communication in order to collect and analyze information	Network
Specific threats to ITS	GPS Spoofing		using GPS simulator to generate radio signals to fool GPS receiver with an arbitrary location/time	Access
	Location tracking		collect personal location info	Facilities
	Sybil attack		multiplication of fake nodes (sending multiple messages from one node with multiple identities)	Applications, Facilities, network
	Illusion attack		Create a specific traffic situation and send false traffic warning messages to mislead drivers	Applications, Facilities
	Vehicle Sensor spoofing		Manipulate sensor in order to generate faulty data complying with the implemented protocols	Access Impact on ITS safety applications

THREATS MODEL FOR CAVS

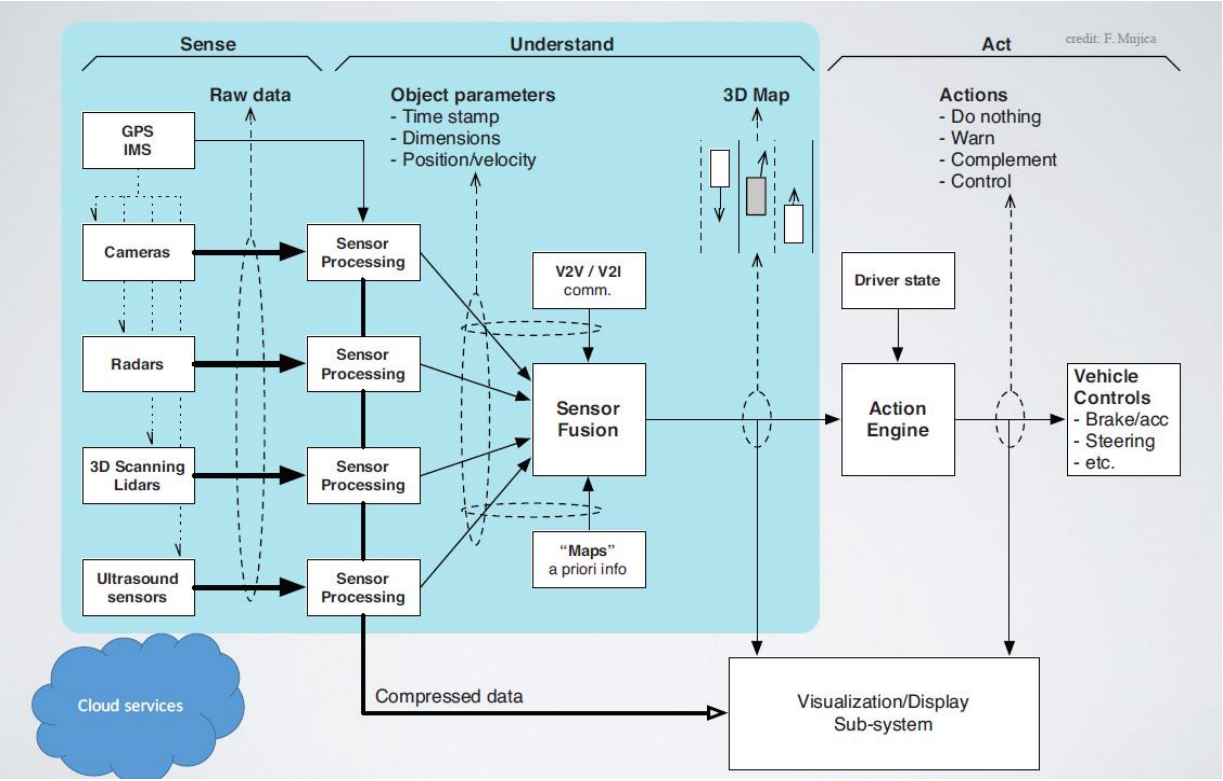
Security goals vs. countermeasures



Collective perception (CPM)
TR 103 562/TS 103 324

ETSI TR 103 460
Misbevahiour detection

PERCEPTION SYSTEM AND V2X MODEL



NEW THREATS AGAINST CAVS

Threats to perception sensors	• External sensors blinding , e.g. camera, lidar • Sensor illusionist; signal delay, relay, replay and forgery • Evil sensor calibrator, modify sensors settings to provoke incorrect/ missing measuremenst • Ground Truth Falsifier
Threats to sensor data processing	• In-vehicle data manipulation • Eavesdropping during sensor storage/processing (e.g. veh path history, behaviour of perception algorithms…)
Threats to Data Fusion (sensor, V2X)	• Fusion manipulation • Tracking Poisoner • Sybil gating e.g. create ghost vehicles via V2X • Fake perception data • Hide road objects

ETSI ITS SECURITY FRAMEWORK & STANDARDS

C-ITS Security Architecture

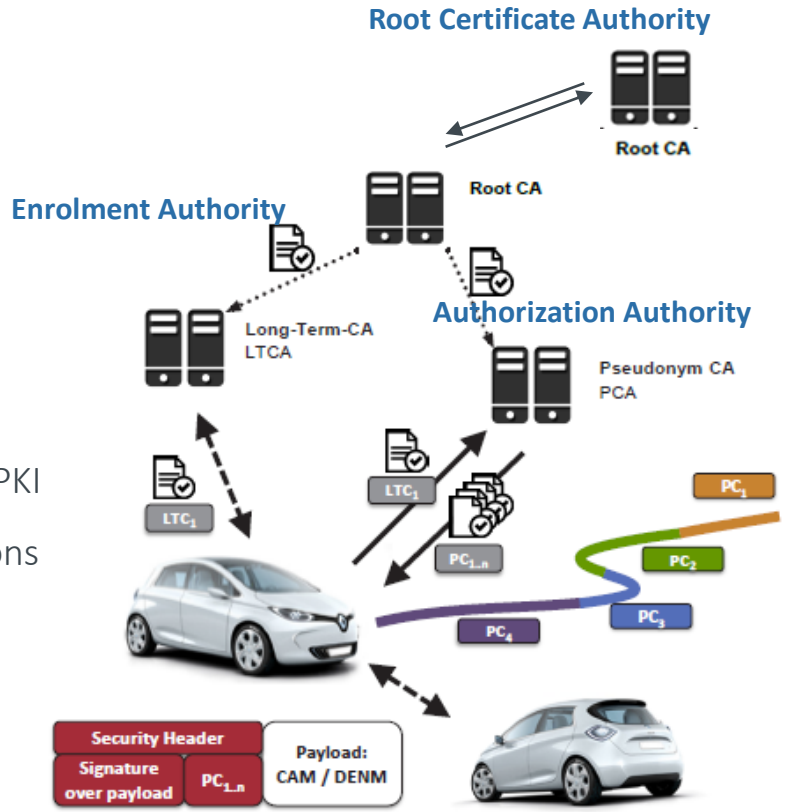
A Public Key Infrastructure enables:

- Authentication & authorization of senders
- Integrity: receivers verify data via digital signatures
- Confidentiality (optional)

Principle:

- Trustworthy stations receive certificates from PKI
- Secure ITS communications between ITS stations (vehicle, RSU, centers…)
- Pseudonymous certificates used for V2X communications (named ATs)

Authentication, Authorization
Non-repudiation

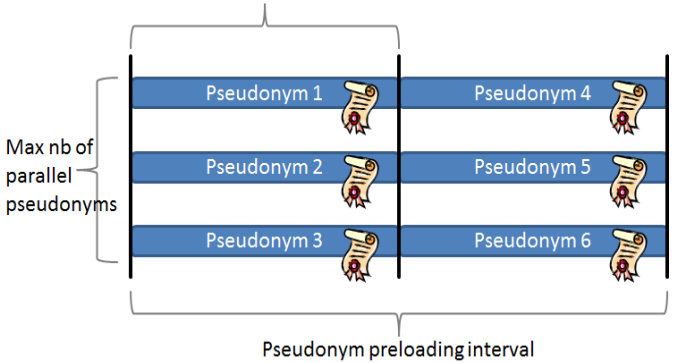


Security and privacy protections in V2X communications

- ITS stations have a pool of Pseudonyms (Authorization Tickets)
- ITS stations change **certificates** regularly and **all their identifiers**
- Reloading of pseudonyms (ATs) either **on-line** or **off-line**

- Key challenge: specify efficient and performant pseudonym change strategies
  - Increased latency, channel load
  - Impact on safety applications
  - Blocking the Change needed

  (limited distance/time period)

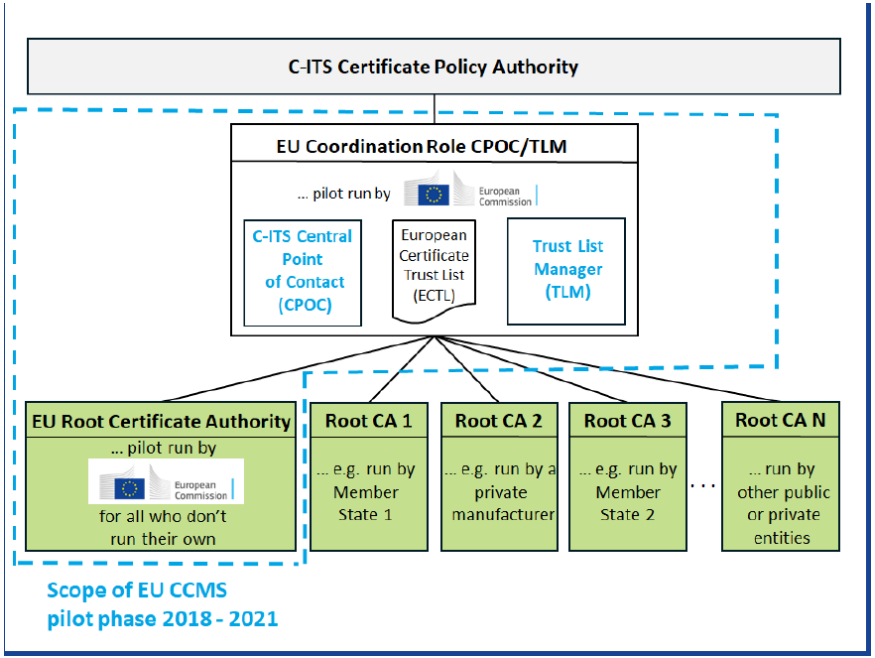


Pseudonymity

C-ITS Security – EU Common Trust model

- Based on **EU Policy & governance documents** published by Commission:
  - Certificate Policy (Annex 3 of DA)
  - Security Policy & Governance Framework (Annex 4 of DA)
- **Pilot Phase 2018-2022** funded by EC
  - Central elements (CPOC and TLM) implementation and testing in 2019
    - TLM and CPOC Web-site open (end NOV-2019)
  - EU Root CA Pilot implementation in 2020
    - Official selection of PKI operator announced
    - EU RCA, EA and AA are operational for testing purpose since August

https://cpoc.jrc.ec.europa.eu/



ETSI ITS Security Standard references

Main outcomes from ETSI WG5 -> 3 main based standards for C-ITS security

TC ITS errata Document on C-ITS Release 1 stds is available at: https://docbox.etsi.org/ITS/Open

Standard Reference	Title	Status
TR 102 893	Threat, Vulnerability and Risk Analysis (TVRA) technical report	v1.2.1 Published, Updated with GEONET risk analysis
TS 102 731	Security services and architecture	v1.1.1 Published
TS 103 097 V1.3.1	**Security header and certificate formats**	v1.3.1 Published (2017-10) revision and extensions for compliance with the European Certificate Policy
TS 102 940 V1.3.1	**ITS communications security architecture and security management**	v1.3.1 Published (2018-04) extensions for compliance with the European CP
TS 102 941 V1.3.1	**Trust and privacy management**	v1.3.1 Published extensions for compliance with the European CP
TS 103 601 V1.1.1	**Security management messages communication requirements and distribution protocol**	To be published soon. P2P distribution of CTL/CRL for fast and efficient update
TR 103 415	Pseudonym change strategies technical report	v1.1.1 Published
TR 103 460	**Release 2: Misbehavior Detection pre-standardization study**	To be Published soon

CONCLUSION

Open standardization challenges

- **ETSI security framework need to be extended to support on-going deployment and new Release 2-related C-ITS applications, and their implementation in transportation infrastructure and in autonomous vehicles for new mobilities**
  - PKI / certificate management will require extensions for new types of stations (central ITS-S, portable ITS-S), new C-ITS and CAV services…
- **Long-term security for trust management in C-ITS and CAVs**
  - Crypto-agility and quantum-safe cryptography
  - cyber-security threats monitoring and incident report
    - ETSI CVD - Coordinated Vulnerability Disclosure
  - Misbehavior detection, reporting and global analysis/ reaction by a central Misbehaviour Authority (MA)
  - integration of collective perception data / cooperative entities trustworthiness evaluation in safety applications to detect misbehavior entities (Day 2)
  - cyber-security assurance management (evaluation scheme) for cooperative ITS

THANK YOU