Q&A Session wrap-up

Questions and Answers

Question 1 by Maglione, Gregorio "In Amr's slide 3, it shows MEC to be connected directly with CV/CAVs, I thought that ETSI's specification had MEC collocated with a BS, making a direct communication link not possible"

Answer: The figure depicts the overlay connectivity and doesn't show the actual architecture of the mobile network. Notice that in the figure we don't depict any base station (BS) actually, but only the technology used, so for cellular the communication technology is just cmwave or mmwave 5G.
Now, about the location of a MEC, being collocated with a base station is just an option. Notice that MEC is access and communication technology agnostic. The way we have it here, is that the MEC is not necessarily provided by the MNO (Mobile Network Operator), but it is simply at the edge and not in a central cloud (see for example that an RSU is connected via wireline directly to the MEC without the intervention of the mobile network.

Question 2 by Altgassen, D. (Daniel) "Do you have some more info, e.g. material to read, about this authentication concept with an 'Attestor' providing credentials?"

Answer: An overview of the attestation mechanisms for authorization can be found in "Keys for device identity and attestation" [1] and the kernel integrity mechanisms[2]. The PoDIUM consortium is working on finalizing the design details and implementation of the corresponding mechanism (e.g., generation of the credentials for our CCAM broker). We expect to have more details publicly available as part of D3.2 (due in March 2024).

Question 3 by Schackmann, P.P.M. (Peter-paul) "Is usage of EU CCMS trust domain for adding trust to transmitted messages (suitable for 5G, ITS-G5, SL) not considered?"

Answer: The EU CCMS is an existing mechanism present within the ITS standard, and it adds some level of trust to transmitted messages, by signing their content with a unique key, allowing to assure that the transmitter has been given a key for that.
Signing messages is not an adequate protection mechanism to on-board unit tampering, which is a type of cyber-attack that involves the modification of the working software in order to make it function inappropriately. The signing mechanism can still function while the OBU is being tampered, but the information would not be trusted anymore. After tampering, the integrity of the OBU decays and the attestation should fail. In PODIUM we are currently able to enable security in most of the OBUs, and this would be a higher level of trust for messages, but the innovation PODIUM is

[1] Trusted Computing Group, (2021), "Keys for device identity and attestation", https://trustedcomputinggroup.org/wp-content/uploads/TPM-2p0-Keys-for-Device-Identity-and-Attestation_v1_r12_pub10082021.pdfAttestation

[2] linux-ima (2014), " Integrity Measurement Architecture (IMA)", https://sourceforge.net/p/linux-ima/wiki/Home

Co-funded by the European Union

Horizon Innovation Actions | Project No. 101069547 | Call HORIZON-CL5-2021-D6-01

introducing is the integrity detection of the OBUs. The concept of the trust computing can be found in the trust computing group website here.

Question 4 by Schaller Andreas (M/NET) "Why is a camera sending CAMs? (in additional to CPMs)"

Answer: Very well-spotted. Indeed. in none of our UCs are CAM messages going to be sent from an infrastructure sensor unit. This is simply a mistake in the figure shown. Many thanks!