CONNECT
CCAM TRUST & RESILIENCE

Never trust, always verify

CONTINUOUS AND EFFICIENT COOPERATIVE TRUST MANAGEMENT FOR RESILIENT CCAM

Message from the Coordinator

Since the publication of our first newsletter a lot happened in our project. On the one hand, we successfully concluded project period 1 (September 2022-February 2024) with first promising results. On the other - unfortunately - one partner had to leave the consortium, namely RedHat from Israel. Nevertheless, we managed to re-distribute all tasks so that the ambitious project objectives can still be achieved. On 24th April 2024 we presented the work and results of the first 18 months in Brussels, where we received very good feedback from the representatives of CINEA (European Climate, Infrastructure and Environment Executive Agency). Of course, there is still a lot to do when it comes to implementing our Trust Assessment Framework and our use cases, but together we are ready to face all upcoming challenges and to make relevant progress in the field of security and trustworthiness of CCAM systems.

Figure 1: Technical Meeting in Munich (October 2023)

Technical meetings in Munich and Paris

In October 2023 the CONNECT consortium was welcomed at the premises of DENSO Automotive in Munich. Partners intensively discussed the CONNECT Trust Assessment Framework and made collaborative efforts between WP3 and WP4, outlining plans for future demos and key milestones. In February 2024 partners travelled to Paris, where we were hosted by our project partner Huawei. Over the course of the meeting, we witnessed remarkable advancements, particularly during the plenary sessions held on the first two days. Dedicated breakout sessions allowed a focused analysis of technical components and pathed the way for first implementation activities with regard to our three use cases.

Figure 2: Technical Meeting in Paris (February 2024)

The CONNECT Consortium

The CONNECT consortium consists of 16 partners from 8 different countries (Austria, Cyprus, France, Germany, Greece, Italy, The Netherlands and United Kingdom). It includes leading organisations from the different industry domains in automated trust management and security, different stakeholders in the supply chain complemented by expertise from the research sector and SMEs.

TECHNIKON
Technikon Forschungs- und Planungsgesellschaft mbH
Austria [Villach]

Suite5
Suite5 Data Intelligence Solutions Ltd
Cyprus [Limassol]

uni.systems
Unisystems
Greece [Athens]

SystemX
Institut de Recherche Technologique SystemX
France [Paris]

UBITECH
Ubitech Ltd
Greece [Athens]

Trialog
Trialog
France [Paris]

UNIVERSITY OF TWENTE.
University of Twente, Department of Philosophy
Netherlands [Twente]

UNIVERSITY OF SURREY
University of Surrey, Department of Computer Science
United Kingdom [Guildford]

HUAWEI
Huawei Technologies
Germany [Munich]

DENSO Crafting the Core
DENSO AUTOMOTIVE Deutschland GmbH
Germany [Munich]

FSCOM
FSCOM
France [Antibes]

Politecnico di Torino
Politecnico di Torino
Italy [Turin]

ICCS
Institute of Communication and Computer Systems, I-SENSE Research Group
Greece [Athens]

intel.
Intel Deutschland GmbH
Germany [Munich]

STELLANTIS | CRF
Centro Ricerche Fiat SCPA
Italy [Turin]

uulm
University of Ulm - Institute of Distributed Systems
Germany [Ulm]

Technical summary of project period 1
(September 2022-February 2024)

The **5G C-V2X technology** is expected to greatly enhance autonomous driving through perception sharing, path planning, real-time local updates, and coordinated driving. These features facilitate the next generation of ITS solutions for cooperative autonomous driving applications (e.g. intersection movement assist, fleet management systems, cooperative routing, and parking services), and greatly reduce emissions. The core of the smart transportation vision revolves around an integrated communication and transportation network that promotes several societal benefit sand shapes a new era of advanced road safety, enhanced personal mobility, and environmental sustainability. However, in order for this vision to materialize, **security and trustworthiness** are key properties of such a system. This is where CONNECT's core contributions lie: CONNECT addresses the convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and trust reasoning framework based on which involved entities can establish trust for cooperatively executing safety-critical functions.

Towards this direction, CONNECT designed an overarching **Trust Assessment Framework (TAF)** capable of CCAM-wide trust quantification by introducing adaptive-to-changes mechanisms for capturing vehicles' trust scores, anchored to decentralized roots-of-trust, and subsequently elevated carefully to the CCAM level. These mechanisms are based on the adoption of advanced (HW-based) trusted computing primitives (CONNECT attestation extensions) for enabling the conversion of such complex ecosystems into trustable (heterogeneous) communication environments allowing for the continuous trust assessment of all involved entities and stakeholders. The core foundation behind this design (as part of CONNECT's established Architecture Reference Framework) is to facilitate the realization of a higher level of automation in connected cars and services envisioning the exchange of rich information between vehicles and the backend infrastructure towards the delivery of more accurate services that can greatly enhance the safety profile of a user on the road.

To achieve this CCAM-wide trust quantification, CONNECT has designed an overarching framework comprising of two phases, namely the Design and Runtime phase. The Set-up phase encompasses all operations needed for the correct establishment and deployment of CONNECT- related components needed to support the continuous trust assessment throughout the entire lifecycle of a (data and/or entity) resource: From the definition of the appropriate trust model templates considering the most prominent types of risks and attacks against the entire CCAM ecosystem, dictating the type of trustworthiness evidence that need to be continuously monitored to quantify its trust level and compare it to the Required Trust Level (RTL), to the deployment of all trust extensions as part of CONNECT'S Trusted Computing Base towards enforcing the circulated trust policies. The Runtime phase encompasses the

(runtime) operation of all CONNECT attestation schemes and security controls, protected through their instantiation in a Trusted Execution Environment (CONNECT adopts the use of INTEL Gramine TEE), for allowing the secure monitoring and exchange (in a verifiable manner) of a resource's trustworthiness evidence based on which the trust assessment/quantification will occur. Such trustworthiness evidence will be further processed, before been transmitted outside the vehicle, so as to be adequately abstracted (harmonized trustworthiness evidence) in order to avoid privacy implications.

The consortium has achieved the **release of the first version of all aforementioned CONNECT core technical components and mechanisms** both as it pertains to the trust assessment/quantification mechanisms, but also the trust extensions required for safeguarding the operation of the CCAM services deployed at the far-edge: This is set to shape the next generation of C-ITS technologies, thus, influencing various ongoing standardization and policy making processes in Europe, providing recommendations in the area trustworthy CCAM.

CONNECT's **involvement with 5GAA** has already started influencing such initiatives by actively contributing to the pre-standardization and regulatory discussions within the association. The produced results have already been shared with the 5GAA (published as white papers) influencing the association's activities in defining clear expecta-
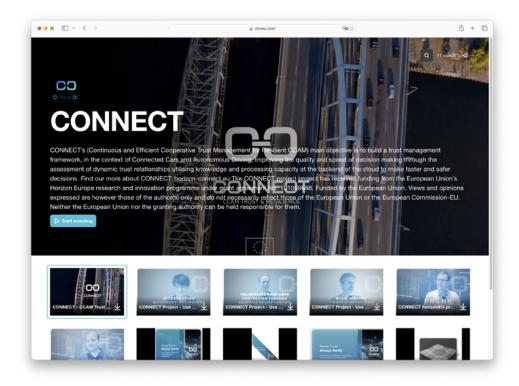
tions and standards related to trust. This is going to be intensified further towards enabling the endmost goal of how V2X communications can be integrated into broader automated vehicle functionalities ensuring safety-critical services and, thus, directly supporting the EU's goal to lead in the digital transition.

Media & Papers

CONNECT Videos:

All project-related videos are now showcased on Vimeo: [**link**]

White papers related to CONNECT

„Cybersecurity for Edge Computing", [**link**]

„Creating Trust in Connected and Automated Vehicles", [**link**]

The CONNECT consortium is formed by a diverse group of stakeholders with a wide range of abilities and expertise, making them well-equipped to address and overcome the challenges at hand.