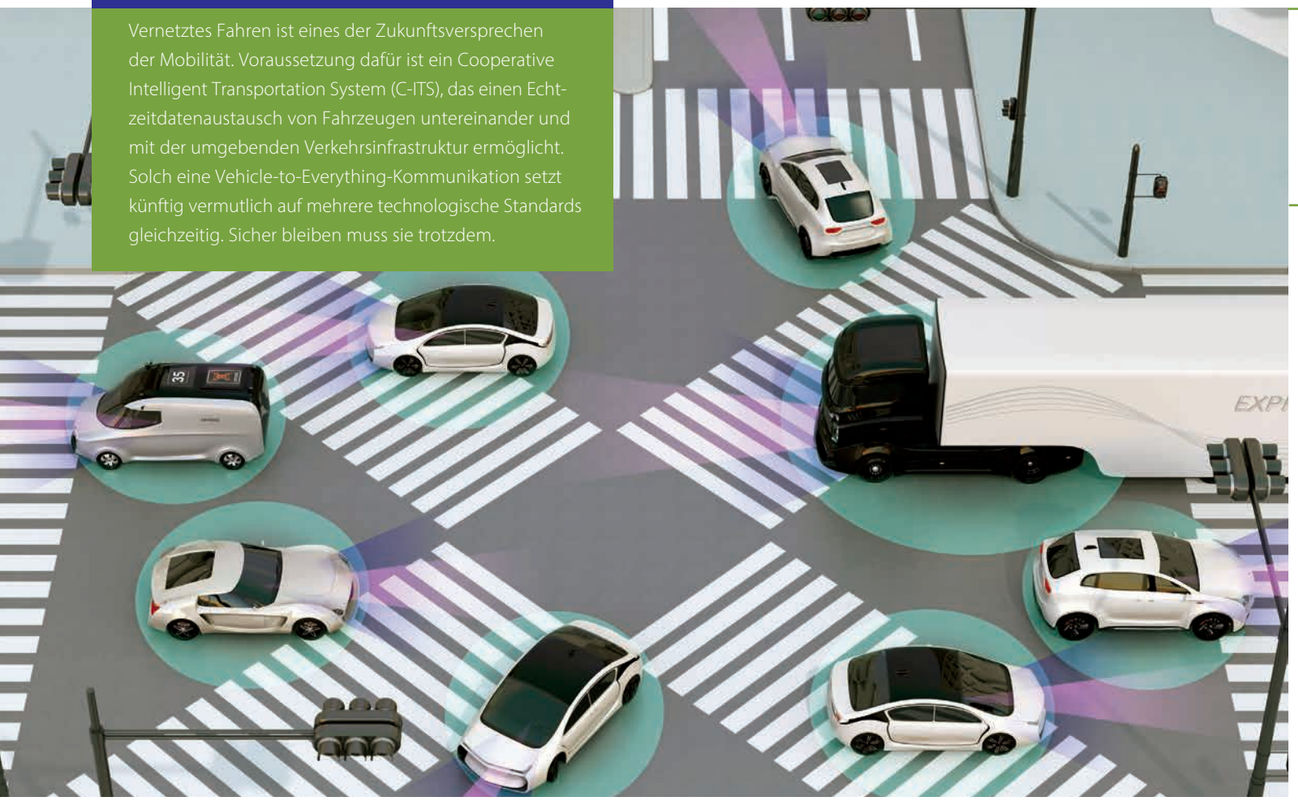
Homogene Sicherheit für hybride V2X-Kommunikation

Einheitliche Lösung sichert vielfältigen Datenaustauch beim vernetzten Fahren

Vernetztes Fahren ist eines der Zukunftsversprechen der Mobilität. Voraussetzung dafür ist ein Cooperative Intelligent Transportation System (C-ITS), das einen Echtzeitdatenaustausch von Fahrzeugen untereinander und mit der umgebenden Verkehrsinfrastruktur ermöglicht. Solch eine Vehicle-to-Everything-Kommunikation setzt künftig vermutlich auf mehrere technologische Standards gleichzeitig. Sicher bleiben muss sie trotzdem.



Bislang basiert direkte V2X-Kommunikation vornehmlich auf dem Dedicated-Short-Range-Communication-(DSRC-)Standard ITS-G5. Der Datenaustausch zwischen Fahrzeugen und Verkehrsanlagen erfolgt dabei quasi in Form einer direkten WLAN-Kommunikation. Doch dabei wird es nicht bleiben. Schon gibt es Bestrebungen, den Mobilfunkstandard LTE-V (heute 4G, alsbald auch 5G) in Zukunft ebenfalls zum V2X-Datenaustausch zu verwenden. Dank neuartiger Mobilfunkchips in den Endgeräten lassen sich so künftig auch andere Verkehrsteilnehmer (z. B. Fußgänger oder Radfahrer) in Form eines direkten Ad-hoc-Datenaustausches (C-V2X Autonomous) zwischen den Endgeräten in die Kommunikation mit einbeziehen. Parallel kommen weitere standardisierte Konzepte hinzu: Mobile Edge Computing (MEC), das Nachrichten über ein zelluläres Netzwerk im Nahbereich verteilt (z. B. für Stauendewarnungen) und der klassische Mobilfunk über Sendemasten zur Kommunikation mit Cloud und Backend-Services (siehe Bild 1).

Einheitliche, intelligente Struktur des Protokoll-Stacks

Höchstwahrscheinlich werden wir es künftig mit einer mannigfaltigen V2X-Kommunikation zu tun haben, die sich je nach Anwendungsfall und Entität verschiedener Kanäle und Standards bedient. Bleibt die Frage: Wie lässt sich eine derart hybride V2X-Kommunikation effizient absichern? Die verschiedenen Übertragungswege nun auch noch mit unterschiedlichen Security-Ansätzen zu belegen, wäre hier genau die falsche Antwort. Stattdessen bedarf es eines Security-Konzepts, das einheitlich über die gesamte V2X-Kommunikation mit ihren vielfältigen Anwendungsfällen hinweg wirkt.

> Wie lässt sich eine derart hybride V2X-Kommunikation effizient absichern?

Die Lösung liegt in einer für alle V2X-Geräte und -Entitäten einheitlichen, intelligenten Struktur des Protokoll-Stacks für die V2X-Kommunikation (siehe Bild 2): Auf Ebene der Anwendung oder des Endgeräts wird die V2X-Nachricht generiert und an die Transport- und Vermittlungsebene weitergereicht. Dort wird über die Schnittstelle zur Security-Komponente der Security Header in die V2X-Nachricht eingebracht. Der Security Header enthält die Signatur der Nachricht sowie das dazugehörige Zertifikat. Falls nötig, wird die Nachricht in einem zweiten Schritt symmetrisch verschlüsselt. Die Informationen zum symmetrischen Schlüssel werden dann dem Header mitgegeben, um den Empfängern der V2X-Nachricht die Entschlüsselung zu ermöglichen. Um zugleich den Datenschutz der kommunizierenden Entitäten im V2X-Netz zu gewährleisten, wird die V2X-Nachricht

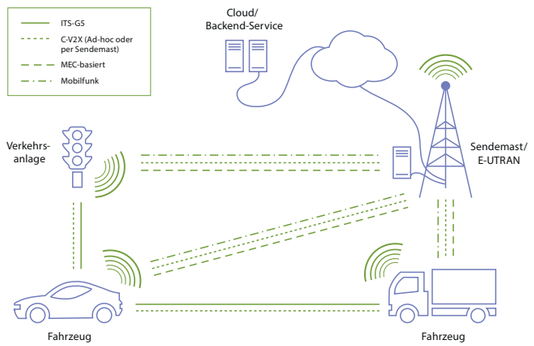


Bild 1: Hybride V2X-Kommunikationsarchitektur

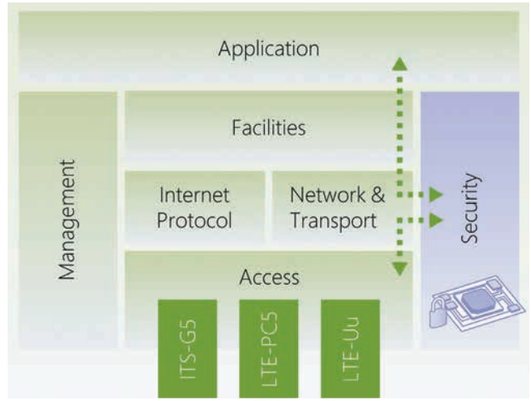


Bild 2: Software-Architektur für einheitliche V2X-Security bei hybrider Kommunikation

zuerst signiert und dann verschlüsselt. Auf diese Weise hält die Absicherung des V2X-Datenaustausches auch in einem hybriden Kommunikationsnetz allen Anforderungen stand: Integrität der Daten, Authentizität des Absenders, Autorisierung des Senders, Replay Detection, Vertraulichkeit, Datenschutz (Privacy Protection), funktionale Zuverlässigkeit (Reliability) und Widerruf von Zertifikaten (Revocation of Trust).

CONCORDA-Projekt als Probelauf

Hybride Fahrzeugkommunikation ist eine sinnvolle und wünschenswerte Weiterentwicklung im Hinblick auf das vernetzte Fahren. Auf diese Art können mehr Endsysteme, Verkehrsteilnehmer und Services am V2X-Datenaustausch teilhaben. Zugleich ist und bleibt IT-Sicherheit eine zwingende und grundlegende Voraussetzung für V2X. Mit einem intelligenten Konzept lässt sich eine homogene und effiziente IT-Security für die V2X-Kommunikation herstellen, die die unterschiedlichen Kommunikationskanäle und Standards überspannt. Ein Probelauf erfolgt im von der Europäischen Union mitfinanzierten und unter anderem von ESCRYPT, der Telekom, Nokia, Bosch und VW begleiteten Projekt CONCORDA (Connected Corridor for Driving Automation) auf Teststrecken in den Niederlanden, Belgien, Deutschland, Frankreich und Spanien. Bis Mitte 2020 wird sich dort erweisen, wie sich ein hybrides V2X-Kommunikationssystem mit ITS-G5 und LTE-Konnektivität sowie einer übergreifenden IT-Sicherheitsarchitektur in der Praxis bewährt. ■

Autoren

Dr. Norbert Bißmeyer ist Project Manager bei **ESCRYPT**.
Jan-Felix van Dam ist Security Engineer bei **ESCRYPT**.