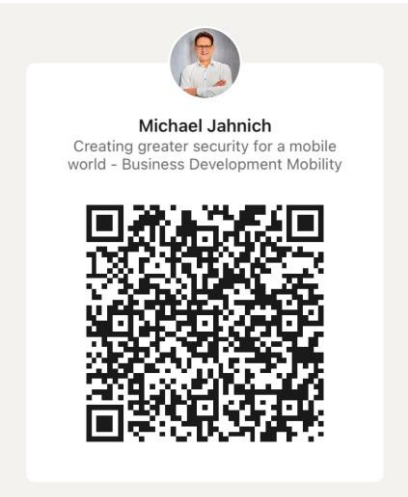
achelos

White Paper

Mobility Connected – How Cyber Security Changes Automotive IT

Abstract

Automotive use cases such as advanced driver assistance and highly autonomous driving push the introduction of V2X communications. But the rapidly increasing connectivity of vehicles and traffic infrastructure offers criminals a growing target for cyberattacks. This white paper provides an overview of current initiatives in the area of automotive cyber security. In particular, it describes the requirements for the development of critical elements of connected vehicles and how **achelos** can support developers to design, implement and test embedded software to achieve a higher level of trust in the security of their products.



1 INTRODUCTION

During the last couple of years, highly autonomous and assisted driving use cases are among the top drivers of automotive industry. They are mile stones on a road to accident free traffic and autonomous vehicles and part of an overall EU strategy to pave the way to a cooperative, connected and automated mobility called CCAM. Instant vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication - in the following, we will call it Vehicle-to-Everything or short V2X communications - is a crucial building block and will further transform the car into a mobile IT data center with many embedded control units (ECU), sensors, monitoring systems, infotainment systems, anti-theft systems and wireless communication modules.

These communication interfaces increase the cyber attack surface of potential hackers or cyber criminals substantially. Cyber attacks on connectivity become scalable and may lead to a large negative impact for car OEMs and their suppliers. The UNECE working party 29 has therefore proposed a regulation on cyber security and software update management which will enter into force early 2021 and which will cause a paradigm shift in the automotive industry in all participating member states. This EU regulation will require vehicle OEMs to provide a cyber security management system (CSMS) to be in place for each new vehicle type. Moreover, it mandates that identified risks must be mitigated and extensive testing must be performed, especially on critical elements.

It is important to notice that this UNECE regulation explicitly mentions embedded high-security modules (eHSM) and the need to use eHSM that have been designed and evaluated according to common security standards. From the current perspective, the critical elements of V2X communications are the eHSM as the secure space for all secret key material and cryptographic operations and the wireless communication module or VCS, as specified in the ETSI standards. In this context, VCS is used as an acronym of acronyms that stands for V2X C-ITS Station (Vehicle-to-Everything Co-operative Intelligent Transport Systems). Both components are closely linked together. They are responsible to provide authenticity, integrity and confidentiality to any message sent or received and thus to enable secure communications.

Today's first eHSM implementations are basically built on embedded secure element technology, which can already be found in smartphones and payment terminals, pay TV smart cards and identification cards. In general, there is a trend towards a more cost-effective integrated secure element technology, e.g. secure elements which are directly integrated into complex system-on-chip designs which leads to new technology challenges. However, the general principles for highly secure development still apply even if they have to be further developed and substantially adapted to automotive requirements. This white paper covers three essential aspects:

- **Security-by-design**. It all starts with risk assessment. Security requirements to mitigate risks must be designed in, implemented and tested as an integral part of the software development in the same way as any other requirement.
- **Cyber Security Testing.** Testing of cyber security functionality becomes vital: strategies and processes for testing embedded security must be defined
- **Evaluation methodologies for critical elements**: Critical elements of the automotive IT must be identified and its evaluation should follow "consensus" standards, Common Criteria is the most likely one.

We will focus on these aspects in the following sections and show why achelos can be a perfect partner to implement and test eHSMs, VCS and other critical embedded software in the automotive space.

2 CURRENT CYBER SECURITY REGULATIONS

2.1 UNECE WP.29 Regulations

In their 181st session in Geneva, the World Forum for Harmonization of Vehicle Regulations, which is WP.29 of the United Nations' Economic Commission for Europe (UNECE), adopted a proposal for two UN regulations: one about Cyber Security Management System (CSMS) and the other one about Software Update Management System (SUMS). Both UN regulations will enter into force beginning of 2021, then they will apply to cars, vans, trucks and buses. In the EU, the UN regulation will become mandatory from July 2022 for all new vehicle types and manufacturers must prove CSMS in place or comparable processes. From July 2024 vehicle manufacturers must demonstrate a CSMS for all vehicles types produced.

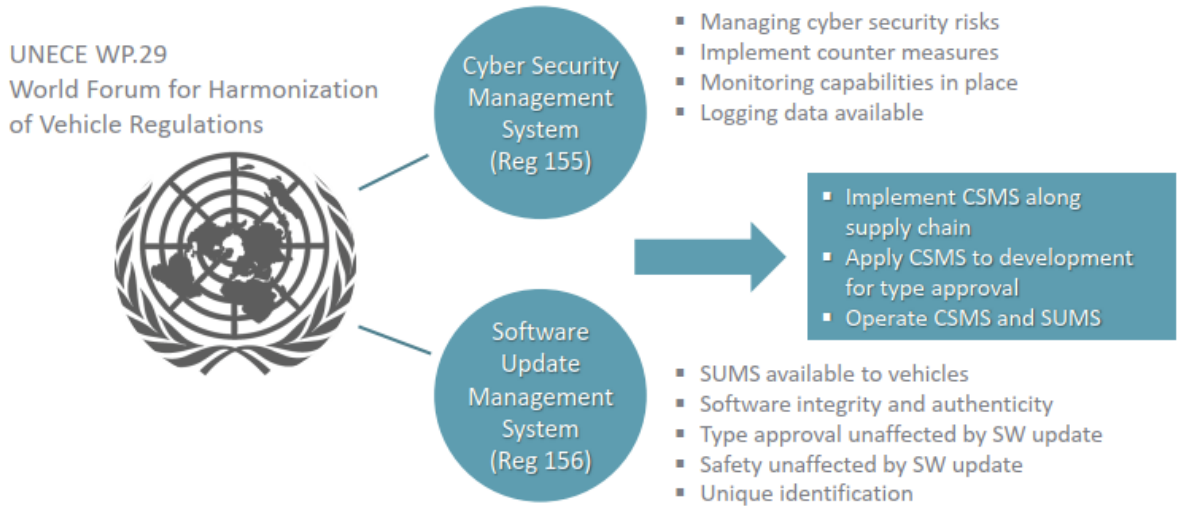


Figure 1 – UNECE regulations

Cyber Security Management System:

The regulation provides a framework of security requirements for new vehicle types and their manufacturers. These requirements will be used by approval authorities and technical services to grant approval for new types of vehicles with respect to cyber security. In particular, the technical services must verify that

- Cyber security risks are identified
- Appropriate countermeasures are designed and implemented in the vehicle type
- Monitoring capabilities are in place to detect and respond to cyber attacks
- Logging data is available for a-posteriori threat analysis (forensic)

Software Update Management System:

The second UN regulation is concerned with the processes and approval of vehicle type with respect to secure software updates and of software update management systems. The main goal here is to ensure that the vehicle's safety is not compromised by insecure software updates and processes. In the near future, technical services will only grant approval for a vehicle type if the following conditions are met:

- Software Update Management System is implemented and available to vehicles on the road
- Update mechanisms ensure integrity and authenticity of the delivered software
- Type approval remains unaffected by software update
- Safety remains unaffected by software update
- Unique identification of software updates
- Software identification must be readable from the vehicle

We would like to point out three particular aspects of this UN regulation:

First of all, with these requirements, **"Security-by-Design"** has become an imperative for the automotive industry, the car makers and their supplying industry. "The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately", states the UN regulation. Car makers or suppliers must start to think of cyber security as an integral part of their product development. They must adapt state-of-the-art practices in design, implementation and testing, as they have been common and field-proven in smart card and embedded security controller developments for decades. The soft- and hardware must implement countermeasures that prove effective before it is subject to verification by the technical services. The situation gets more challenging because security principles need to be rapidly integrated into existing software architectures. On the other hand, the rigid safety requirements that the automotive industry has already established forms a very good quality foundation for the required evolution. However, it is paramount to realize that protecting a system from arbitrary faults exhibits some fundamental differences to protecting a system against malicious attacks of human intelligence.

Secondly, there is much focus on **cyber security testing.** The UN regulation states that "the Approval Authority or Technical Service shall refuse to grant the type approval if the vehicle manufacturer did not perform, prior to the approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented". Without appropriate and sufficient testing, a vehicle OEM will not achieve type approval with respect to cyber security. Therefore, the regulation mandates that "processes used for testing the cyber security of a vehicle type" must be established and that cyber security testing must be performed with an adequate test coverage. Since cyber security testing aims at modelling and proving resistance against malicious attacks, also testing and quality controls face new challenges.

Last but not least, adequate **evaluation methodologies** such as Common Criteria should be applied to the certification of critical elements, such as embedded HSMs. The regulation explicitly mentions embedded HSMs: "if cryptographic modules are used to comply with this requirement, the manufacturer is obliged to use modules that comply with the consensus standards, and if this is not the case, a satisfactory justification should be provided." A consensus standard can be any evaluation methodology used in the cyber security area which has been created in consensus of a participating parties. For high-security components like secure elements, HSMs, or cryptographic modules, the most widespread and used are Common Criteria and FIPS as of today. Further evaluation methodologies may be derived, especially for more complex software systems, but currently, Common Criteria at least is an established and usable way to thoroughly evaluate high-security components as we will see in the following. The more challenging question is how to scale

the traditional approaches up to more complex security relevant systems like the security gateways such as the VCS and the automotive system architecture as a whole.

It is important to mention that the regulation foresees, although the vehicle maker is in the central position when it comes to cyber security, that cyber security has to be handled by the whole supply chain, since the manufacturer has to identify and mitigate risks "through the supply chain so as to demonstrate that supplier-related risks are identified and are managed".

The implementation of the UN's regulation for a CSMS will follow the new ISO/SAE 21434 for cyber security risk management, which is likely to be final beginning of 2021, and further implementation regulations, e.g. ISO PAS 5112 Road vehicles — Guidelines for auditing cyber security engineering. Implementation guidelines for software update management are currently developed in ISO 24089 Road vehicles — Software update engineering.

2.2 Cooperative, connected and automated mobility in Europe

In November 2016 , the European Commission broadened their strategy on Cooperative Intelligent Transport Systems (C-ITS), which was set by the EU directive 2010/22, towards a general cooperative, connected and automated mobility. This strategy is aimed at providing a legal framework for the deployment of C-ITS services, the availability of an EU project funding and the evolution of the C-ITS platform. It includes continuous coordination of initiatives like C-ROADS for the deployment of appropriate infrastructure and the CAR-2-CAR Communication Consortium (C2C-CC).

The C2C-CC is an association of leading European and international vehicle manufacturers, automotive suppliers, development companies and research institutes. It works together on innovative mobility projects and aims to achieve road safety and accident-free mobility by bringing together a diverse range of competencies. To achieve these goals, direct networking between road users, whether vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication, is defined and standardized. Cyber security is the basis for cryptographically secured communication between vehicles based on IEEE 1609 and ETSI standards related to the reference architecture of Co-operative Intelligent Transport Systems (C-ITS). The C2C-CC specifies a Basic System Profile that can be used to develop interoperable collaborative applications.

Current work is mostly related to security. Following the security policy of C-ITS in Europe, C2C-CC has specified a protection profile for the so-called V2X HSM according to Common Criteria. The V2X HSM, which is functionally specified in ETSI TS 102 940, shall be used for secured cryptographic operations, e.g. digital signature generations, and key management. Its cryptographic capabilities are consumed by the vehicle's C-ITS station or VCS. The protection profile is currently updated and is going be certified and published. It defines a high assurance level of EAL4 augmented with ALC_FLR.1 and AVA_VAN.4 to be used as appropriate for a V2X HSM that resists threats with a moderate attack potential.

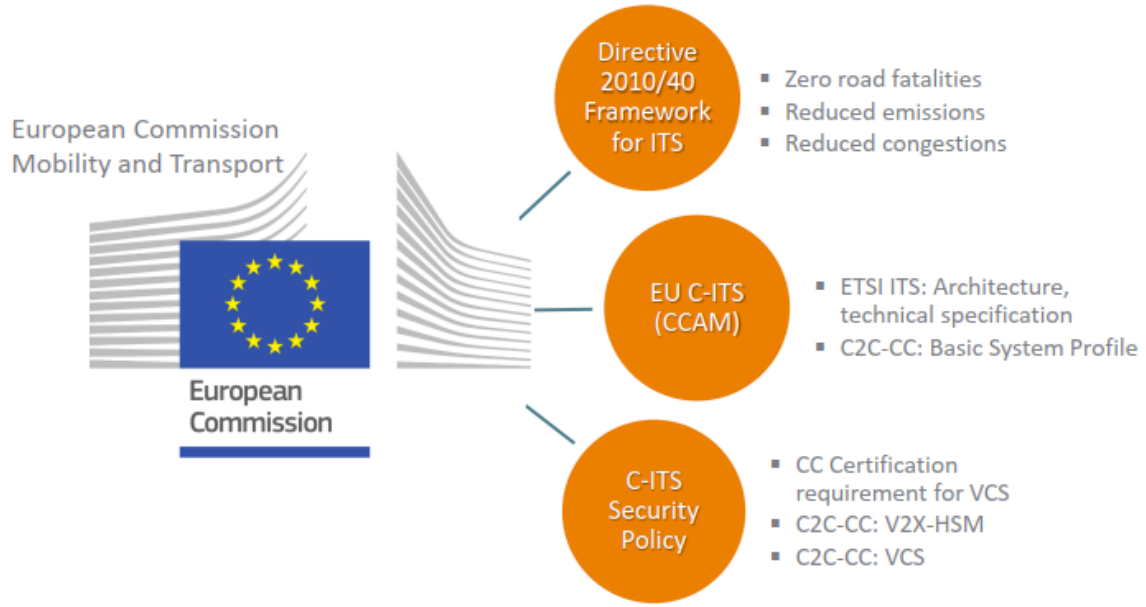


Figure 2 – EU on Cooperative, Collaborative and Automotive Mobility

According to the C-ITS security policy and the delegated act on C-ITS, the VCS shall be assessed and certified using the Common Criteria scheme. For the VCS, the C2C-CC is currently drafting a protection profile. However, a final version is still not in sight and the question arises to what extend the traditional evaluation approaches can cope with both the increasing complexity of the software systems and the increasing complexity of the stakeholder landscape. The latter aspect is still often overlooked by people more used to simple HSMs or secure elements which integrate components of a handful of companies only. Nowadays, the increasing specialization and system complexity leads to system architectures that incorporate a large amount of hardware IPs, firmware, operating system, middle-ware and application components provided by a large variety of companies and integrators. Traditional composition approaches will not able to cope with this evolution unless substantially improved.

It is worth noting that both protection profiles are referenced by implementing regulation (EU) 2019/1213 of 12 July 2019 ensuring the "uniform conditions for the implementation of interoperability and compatibility of on-board weighing equipment" for stage 2.

So basically, the HSM and the VCS can be considered the critical elements of the V2X communication of a vehicle or traffic infrastructure. Their implementation requires the skills mentioned above: security-by-design, cyber security testing and evaluation.

3 SOFTWARE SECURITY ENGINEERING IN THE AUTOMOTIVE SPACE

What becomes an inevitable element of automotive software development with the regulative initiatives, has been a paradigm in the development of smart card and secure elements software for 30 years or even more. It is security-by-design and the complete integration of security into the development process. This knowledge is now moving into the rapidly expanding field of security solutions for more complex systems like mobile phone, cars or industrial IoT devices. But what is the

best way to develop secure systems? The general answer is straight forward and extremely simple. Our experts would respond: "Just treat security requirements like all other requirements for the system, and process them as an integral part of our development life-cycle using the powerful software and hardware engineering techniques that are already at your disposal." Even though the principle is simple, the application requires a lot of security expertise. Let us have a look at some of the security techniques.

3.1 Security-by-design

The UN regulation mandates that risks shall be identified and mitigated by implementing appropriate security functions. Manufacturers shall even apply "excessive risk assessment" to critical components. This first step supplies vital input for the security architects to derive security objects and requirements. And these requirements must be handled like any other requirement. The best situation is created when security and software architects work together right from the start and draft a software architecture that includes an appropriate security architecture. Companies will not succeed putting security onto an insecure software architecture and achieve a secure implementation.

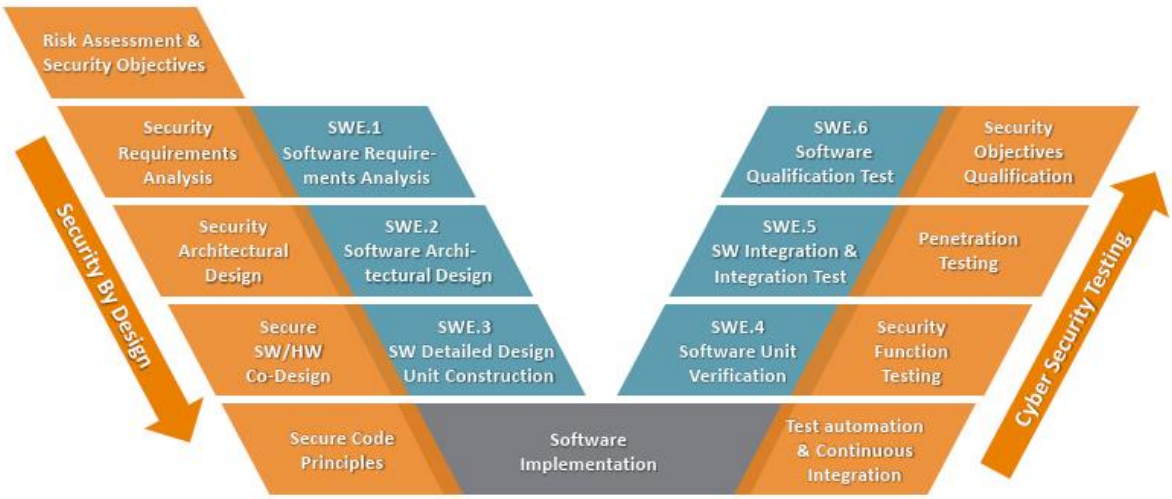


Figure 3 – A-SPICE Software Engineering (SWE) enhanced by Cyber Security Tasks

Obviously, software engineering and testing is in reality way more agile and dynamic as the figure above suggests. Nonetheless, the observation still remains that issues detected during the risk assessment, requirements analysis and the architectural design are easier and more cost effective to fix, than issues detected during development, testing or even in the field. Furthermore, we observe that for automotive security scenarios way higher quality standards apply so that agility has to be used with care.

Designers in particular have to work on a secure co-design of software and hardware because enforcing security properties like side-channel attacks or fault injection resistance require a tight collaboration between the hardware and at least the lower parts of the embedded software stack. Similarly, on higher real-time operating system-level of a software stack the logical attack surface increases drastically which naturally leads to the demand of strong - preferably hardware-backed - exploit mitigation techniques building on top of memory protection units or security enforcing instruction set extensions. Moreover, throughout the whole development process, developers must

follow secure coding principles. Training of those techniques and review of code with respect to these principles are a must.

Additional supportive techniques, like the use of static code analysis, enforcement of security aspects in quality gates, fuzz testing, but also the definition and execution of an incident response plan (as for example advocated in the Security Development Life-Cycle (SDL) of Microsoft) further complement the integration of security into development.

3.2 Cyber Security Testing

Having designed software with appropriate security functions, the UN regulation recommends that software is tested extensively especially with respect to cyber security. The UNECE regulation 155 states that "the vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented".

Testing should comprise functional testing and penetration testing. Functional testing means that the security functions specified are thoroughly checked to verify that controls in place are working properly. Test automation and continuous integration can help developers testing each code to not affect security controls. Functional testing may consist of standards tests that verify if the software complies with public standards to enable interoperability but it can also check that security is implemented properly. For example, a test suite can check that the transport layer security (TLS) is implemented according to the publicly available standards and therefore enables an interoperable secure communication. But the same test suite can also verify that the TLS interface has been configured correctly and that no weak security configurations are used. Automated security functional testing can even go one step further and test for example the absence of obvious timing side-channels.

Here the boundary towards penetration testing is crossed which checks that the implementation is robust to hacking and cyber attacks. Quite a variety of different penetration test categories exist, ranging from black-box style approaches where a security analyst tries to penetrate into a system using similar information gathering, privilege escalation, and exploitation techniques like an attacker, to white-box evaluations, where an in-depth vulnerability analysis of sensitive code parts is conducted upfront and pen-testing is primarily conducted to support and complement the vulnerability assessment. The TLS interface, to reuse the example above, can be checked by test suites that perform an irregular behaviour of the communication partner and thus try and find a weakness in the implementation or configuration of the TLS protocol implemented.

At the end of the day, cyber security testing aims at verifying that the security objectives are fulfilled and the security functions implemented work as intended and cannot be bypassed with reasonable efforts.

Although cyber security testing in the public is often perceived as pen-testing, it is both, functional and penetration testing. Both go hand in hand. And both are recommended to be performed by independent teams.

3.3 Evaluation Methodologies

Many risks in V2X communication can only be mitigated by means of an embedded HSM that serves authenticity, integrity and confidentiality and manages the cryptographic keys needed in a secure storage. The UN regulation requires that cryptographic modules, which are embedded HSMs, shall comply with consensus standards, while European initiatives explicitly require core components to

be certified following the Common Criteria evaluation methodology. For a good reason, Common Criteria already today implies principles such as security-by-design and cyber security testing. It defines an internationally accepted framework for the evaluation and certification of security software and hardware, at least for core components that have a medium system complexity and software will not be updated regularly.

As already outlined, it will become increasingly difficult to create transparent security assessment for a growing complexity of the systems and the stakeholder landscape. While component assessment which consider specific sensors, firewalls, secure elements which act as trust anchors can still be addressed by traditional means, assessing the security of more complex systems like the VCS in connected cars can become harder to manage. The collaboration of security experts from many different fields and building strong partnerships will become more and more a key success factor. In addition, our experts expect that a form of higher level process and integration assessment which aggregates the results of various security assessments of different components into an overarching security statement is needed. It remains open if Common Criteria alone is suitable for this purpose because of its product-centric approach and lack of efficient support for complex composition scenarios, dynamic deployment and update cycles, and differing assurance level requirements for various parts of security systems.

4 CONCLUSION - DEVELOPING CRITICAL ELEMENTS OF AUTOMOTIVE IT

The architecture of a V2X HSM - as we have seen so far - consists of a security controller that supplies the necessary cryptographic operations. On top of the security controller, a native operating system, or alternatively a Java Card operating system, manages the necessary resources and grants access to volatile and non-volatile memory, to security operations and manages the applications loaded into the controller. For the V2X-HSM, these applications basically comprise the management of cryptographic keys, which are used to provide authenticity, integrity and confidentiality of the V2X messages sent and received. Moreover, it provides securely implemented crypto-operations such as generating and verifying digital signatures based on Elliptic Curve Cryptography and key exchange and derivation methods to provide a symmetric session key for message encryption.

The HSM must be integrated into the VCS design by means of a physical connection such as SPI or ISO 7816 or can be part of an integrated solution at the chip design level. Anyway, the security services of the eHSM must be available to the application controller of the VCS and thus provide some kind of integration layer, the Security Services, for the application programmer.

How can we help to create secure systems?

The answer is just as simple: modern cyber security development, testing and certification in the automotive space can benefit substantially from security expertise developed for smart card and other embedded security controllers for ID cards, mobile phones or payment terminals. This has been our excellence for more than a decade. However, this experience needs to adopt and further evolve to cope with increasingly complex systems and therefore an effective partnership between system and security experts is a key success factor.

McKinsey states that they "expect the market to stay in the hands of the incumbent semiconductor companies, but there are also opportunities for OEMs or suppliers to enter the market if hardware security modules become an important differentiating factor." Having an independent development

partner who has the knowledge of and the experience in securely implementing and integrating such a solution could be a real business advantage.

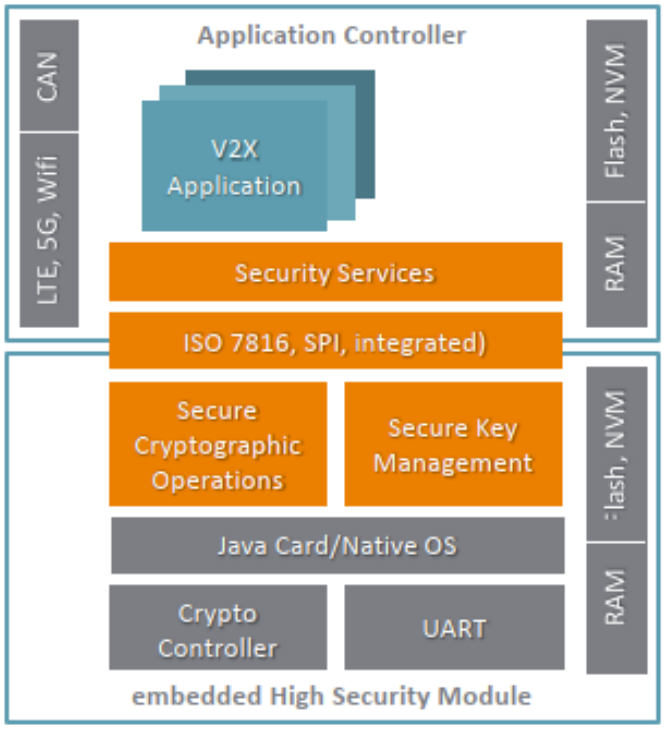


Figure 4 – VCS and V2X-HSM architecture

We are your Security Engineering Partner

With our products and services, we enable you to develop, integrate, roll out, monitor and continuously improve your IT security solutions in the automotive market faster. For many years, we have been working on the certified security of solutions in the automotive market. For example, in the digital tachograph market, we carry out security evaluations according to Common Criteria and offer functional test suites for the onboard unit. We have successfully achieved security certification a lot of times.

Secure software starts with design. With many years of experience in the development and evaluation of secure software, achelos offers a comprehensive consulting service for Security by Design software. By participating in the evaluation of high-security products according to Common Criteria, both on the test center and manufacturer side, you have an excellent partner at your side. Especially in evaluations, our experience saves costs and time and avoids high efforts for a later adaptation.

Based on dedicated requirements management, achelos develops secure applications in an agile way. The software development process is viewed holistically and quality assurance is taken into account as early as the requirements analysis stage. achelos' origins in the development of security-relevant applications and the development of operating systems for health insurance and bank cards, where a very high security standard has had to be maintained for years, form the basis for this.

achelos helps companies in the development process through services. We build and operate complete test environments including all necessary simulations for operating environments.

Through excellent domain knowledge, e.g. in the area of TLS, IKE/IPsec and certificates, we achieve an exceptionally high test coverage in security-relevant areas and the highest quality.

In the area of CC certifications, we take care of the co-ordination between the manufacturers, the BSI (German Federal Office for Information Security) and evaluation labs and prepare all necessary documents for certification as required.

Overall the capability to support development over a broad range of security engineering, security development and security testing activities makes the portfolio of achelos quite unique in the market. In addition to this, we strive to expand further into different security markets and find novel ways to scale our experience to more complex systems and integration scenarios. We are independent of any supplier and we know security by heart.

5 ABOUT ACHELOS IN THE AUTOMOTIVE MARKET

achelos GmbH is an associate member of the Car-2-Car Communication Consortium, an association of leading European and international vehicle manufacturers, automotive suppliers, development companies and research institutes. Through our membership in the Car-2-Car Communication Consortium, our experts contribute to the central application environment of future mobility and further expand this segment for achelos with offers and solutions. From the perspective of connected vehicle communication, achelos works on new standards and procedures for safety.

For many years, achelos has been working on certified security solutions for the automotive market. One example is the digital tachograph. The company has contributed expert knowledge to the European project for security evaluations according to Common Criteria and offers test suites for functional tests of the onboard unit as well as a test system for all card types of the digital tachograph system. Our customers benefit first-hand from the active participation in various working groups of the Car-2-Car Communication consortium. We use this to develop a focused range of products and security services for the mobility market in line with its rapidly growing requirements for cyber security.

If you are interested in further information, do not hesitate to contact us.

6 REFERENCES

1. Burkacky et al.: Cybersecurity in automotive - Mastering the challenge. Mc Kinsey Study, March 2020,
2. UNECE WP.29 GRVA: Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. World Forum for Harmonization of Vehicle Regulations 181st session Geneva, 23-25 June 2020, ECE/TRANS/WP.29/2020/79, June 2020.
3. UNECE WP.29 GRVA: Proposal for amendments to ECE/TRANS/WP.29/2020/79, 181st session Geneva, 23-25 June 2020, ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97, June 2020.
4. UNECE WP.29 GRVA: Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. 181st session Geneva, 23-25 June 2020, ECE/TRANS/WP.29/2020/80, June 2020.
5. EC: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, December 2017.
6. ETSI EN 302 665:Intelligent Transport Systems (ITS); Communications Architecture, V1.1.1, September 2010.
7. ETSI TS 102 940: Intelligent Transport Systems (ITS);Security; ITS communications security architecture and security management, V1.3.1, August 2018.
8. IEEE 1609.2: Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, Draft 2019.
9. Car-2-Car Communication Consortium: Protection Profile V2X Hardware Security Module. Version 1.5.1, July 2020 - under revision.
10. EU Commission: Implementation of interoperability and compatibility of on-board weighing equipment. Commission Implementing Regulation (EU) 2019/1213, 12 July 2019.

achelos GmbH
Vattmannstraße 1
33100 Paderborn

+ 49 5251 14212-0

www.achelos.de