Rethinking automotive cybersecurity
“Automotive cybersecurity is becoming a question of personal safety.”

Dr. Uwe Müller
Vice President Cybersecurity Solutions
ESCRYPT, Bosch Group

Enabling the future of connected mobility

Digital transformation will fundamentally change mobility and the automotive sector. The future of highly automated, connected driving is based on powerful new electrical system architectures and high connectivity. This increases the danger of cyberattacks on vehicles exponentially, with a risk of manipulation, data spying, and unauthorized access to vehicle functions.

At the same time, traffic safety for digitally connected, automated vehicles goes hand in hand with IT security. Automotive cybersecurity is becoming a question of road users’ personal safety. And it will become a critical success factor for all market participants looking to comply with legal requirements and standards, avoid recalls and liability claims, and live up to people’s trust in new technologies.


ESCRYPT is a pioneer and leading provider of IT security solutions in the automotive sector. We have been developing software applications for vehicle protection for over 15 years. Today, ESCRIPT solutions are an integral part of large-scale automotive production in many places and are used in millions of vehicles worldwide.

- A subsidiary of ETAS GmbH, part of the Bosch Group since 2012
- Some 400 associates at 18 locations worldwide
- Security for electrical system communications, attack detection and defense, V2X security, secure vehicle access, key management, secure over-the-air updates, and more
- Consulting, risk analysis, security testing, real-time analysis, as well as incident and emergency response management
- Security services for the Bosch Group’s corporate IT and its products
Implementing automotive security in production

Automotive security must be factored in right from the start: in the connected manufacturing processes used in the automotive industry. Production of vehicles and their individual components must be protected against cyberattacks and data theft. Meanwhile, in ECU production, key material provided by automakers must be distributed as needed among production sites, where it is stored before being introduced into the ECUs during the manufacturing process.

ESCRYPT protects the vehicles’ production environment with classic manufacturing IT security services and ensures that ECUs are fit for an IT-secured data exchange.
Protecting the vehicle with embedded security components

Depending on the degree of connectivity and automation, vehicles must be protected in road traffic across all functional levels. This requires embedded automotive security components that work together according to the respective security approach of the individual vehicle platform – starting with security functions on the ECU processor, this extends from protecting on-board communication and the E/E architecture through to security solutions for V2X communication and vehicle IT infrastructure.

ESCRYPT protects vehicles in the field with a multi-layered security concept in combination with complementary embedded IT security components.

Maintaining security over the entire life cycle

Security-specific backend services are indispensable in maintaining the IT security of vehicles over their entire life cycle. In the Security Operations Center, cyberattacks on the vehicle fleet are aggregated, assessed with self-learning analysis tools, and forensically evaluated before security updates are rolled out. It is also essential to protect the operating backend systems, hosting systems, and data streams for the vehicle’s connected online services or mobility services at all times.

ESCRYPT protects the vehicle fleet by combining automotive security expertise and classic enterprise IT security to form a Security Operations Center (SOC) – with big data analysis systems and security services for vulnerability management and incident response.
Design
Enable
Manage

ESCRYPT offers the suitable solutions for integrated vehicle security – from risk analysis during development to secure over-the-air updates.
Cost-effective state-of-the-art solutions

- Cost-effective security approach for good balance between security risks and implementation costs.
- Automotive security pioneer for technologies: risk-based security engineering, hardware security modules, secure automotive hypervisor, and more.
- Large-scale, reliably backed security management solutions.
- Strong connections to leading research institutions, universities, and worldwide security committees.

Platform security provider

- From deeply embedded to connectivity to backend.
- From early concept to implementation and production to operation and phase-out.
- From prediction and prevention to detection to response.

Reliable & trusted partner

- Successful international automotive security provider for over 15 years.
- Active around the globe and security partner to all OEMs and tier 1 suppliers.
- Strong long-term commercial horizon as an independent company within the Bosch Group.
Design Security
Consulting, Testing, and Training

Strategic Security Consulting
- Strategic Security Development, Security Vision and Roadmap
- Security Standardization, Lobbying, and Strategic Cooperation

Enable Security
Products and Solutions

Managed PKI Service
allows OEMs to maintain internal control over vital aspects of security such as certificate issuance, suspension, and revocation.

Security Operations Center (SOC)
acts as mission control, tracking anomalies and events in any aspect of a vehicle's operation.

Security Trainings
- Security Basics
- Security Risk Analysis
- Secure Product Design
- Secure Connected Products
- Automotive Security

Production Key Server
Crypto server for secure key injection in mass production

CycurHSM
Automotive-qualified security stack for HSM

CycurIDS
Intrusion detection

CycurV2X
Secure V2X communication SDK

CycurGATE
Automotive firewall

ECU Production
Threat Intelligence and Forensics deliver evidence-based knowledge about existing or emerging menaces to induce informed decisions and responses.

Vulnerability Management helps uncover flaws and enables OEMs to implement a proactive threat prevention strategy.

Product Security Consulting
- Security Risk and Threat Analyses, Protection Requirements
- Security Concepts and Design
- Security Roles and Processes
- Custom Consulting

Product Security Engineering
- Security Specifications
- Security Implementations
- Security Integration
- Security Production
- Security Management

Security Testing
- Functional Security Testing
- Vulnerability Scans and Fuzzing
- Penetration Testing
- Code Security Audits
- Security Certifications
- Security Test Management

CycurACCESS Vehicle access and key sharing
CycurTLS Transport Layer Security (TLS) for embedded platforms
CycurLIB Cryptographic library

CycurKEYS Secure management of cryptographic keys and certificates
CycurV2X-SCMS V2X security credential management system
CycurGUARD Intrusion monitoring and analysis
Ready to secure you worldwide

Ann Arbor Bangalore Berlin Bochum Lund Munich Pune Saint-Ouen Seoul Shanghai Stuttgart Sunnyvale Torino Warsaw Waterloo Wolfsburg Yokohama York